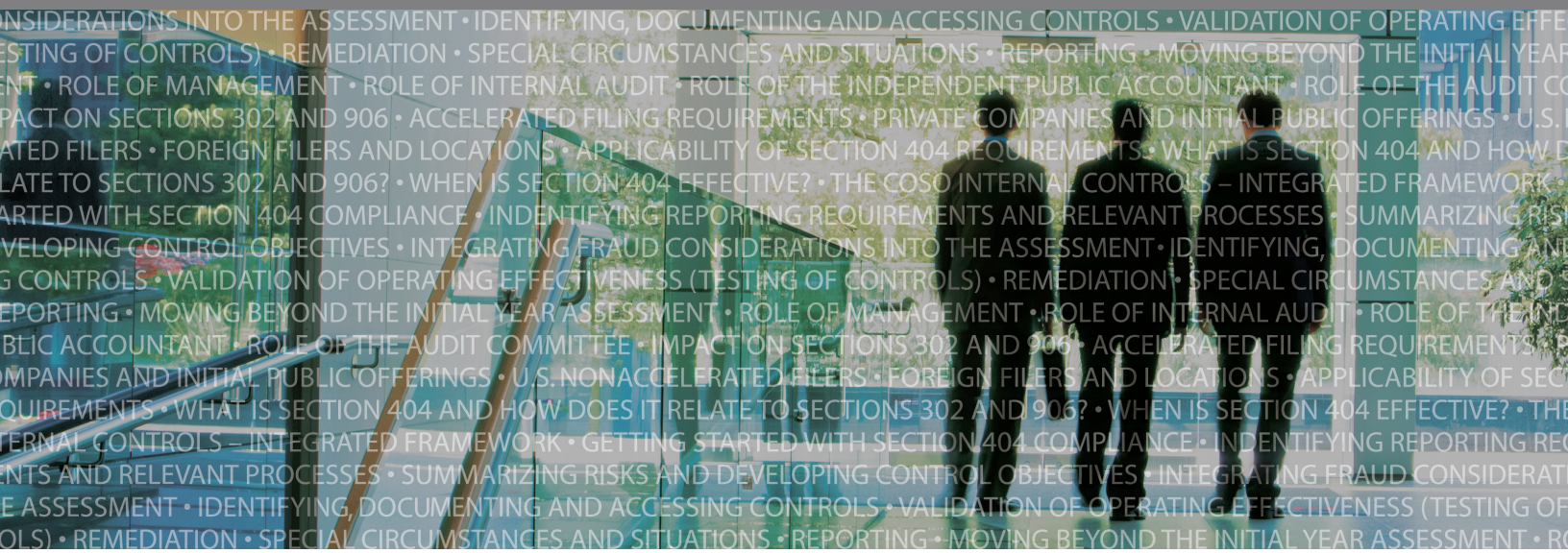
GUIDE TO THE SARBANES-OXLEY ACT:

Internal Control Reporting Requirements



Frequently Asked Questions Regarding Section 404

Fourth Edition

protiviti®
Independent Risk Consulting

Business Risk | Technology Risk | Internal Audit

Table of Contents

Page No.

* Indicates new or substantially revised material (in comparison to the third edition of this resource guide)

Table of Contents *(continued)*

Page No.

* Indicates new or substantially revised material (in comparison to the third edition of this resource guide)

Table of Contents *(continued)*

Page No.

* Indicates new or substantially revised material (in comparison to the third edition of this resource guide)

Table of Contents *(continued)*

Page No.

* Indicates new or substantially revised material (in comparison to the third edition of this resource guide)

Table of Contents *(continued)*

Page No.

* Indicates new or substantially revised material (in comparison to the third edition of this resource guide)

Table of Contents *(continued)*

Page No.

* Indicates new or substantially revised material (in comparison to the third edition of this resource guide)

Table of Contents *(continued)*

Page No.

* Indicates new or substantially revised material (in comparison to the third edition of this resource guide)

Table of Contents *(continued)*

Page No.

* Indicates new or substantially revised material (in comparison to the third edition of this resource guide)

Table of Contents *(continued)*

Page No.

* Indicates new or substantially revised material (in comparison to the third edition of this resource guide)

Table of Contents *(continued)*

Page No.

* Indicates new or substantially revised material (in comparison to the third edition of this resource guide)

Table of Contents *(continued)*

Page No.

* Indicates new or substantially revised material (in comparison to the third edition of this resource guide)

Introduction

Since the third edition of *Frequently Asked Questions Regarding Section 404* of Protiviti's Guide to the Sarbanes-Oxley Act series was released in August of 2004, much has happened. For example:

- The U.S. Securities and Exchange Commission (hereinafter referred to as the "SEC" or the "Commission") has created a "large accelerated filer" category and has adopted different deadlines for initial Section 404 compliance for accelerated foreign private issuer filers and nonaccelerated U.S. domestic issuer and foreign private issuer filers. In addition, the deadline for initial compliance with Section 404(b) requiring an attestation report has been delayed an additional year for accelerated foreign private issuer filers and nonaccelerated U.S. domestic issuer and foreign private issuer filers. As this publication went to print, the SEC Commissioner announced his intention to propose an additional one-year delay for the external auditor's attestation under Section 404(b) related to smaller public companies. Finally, the Commission provided additional time for newly public companies to comply with Section 404.
- There have been two joint roundtables conducted by the SEC and the Public Company Accounting Oversight Board (hereinafter referred to as the "PCAOB" or the "Board") on the implementation of the internal control provisions of The Sarbanes-Oxley Act of 2002 (hereinafter referred to as the "Sarbanes-Oxley Act," the "Act" or "Sarbanes-Oxley").
- The SEC has issued interpretive guidance to management for conducting the assessment process required by Section 404.
- The PCAOB has issued Auditing Standard No. 5 to incorporate guidance the PCAOB staff released in response to the 2005 roundtable and make the attestation process more cost-effective. This new standard superseded the controversial Auditing Standard No. 2.
- The Committee of Sponsoring Organizations of the Treadway Commission (hereinafter referred to as "COSO") has issued further guidance on the use of its Internal Control – Integrated Framework, particularly by smaller companies.
- More questions have arisen on a wide variety of topics.

While the above list does not include everything that has occurred, it certainly is enough to warrant an updated fourth edition of this publication.

This publication is designed to help answer your questions about the sections of Sarbanes-Oxley pertaining to public reporting without your having to wade through material you already know. This information will assist Section 404 project sponsors, leaders and team members within your organization. For readers of prior editions of this publication, new and substantially revised questions have been flagged. The questions listed in this publication are ones that have arisen in our discussions with clients, attorneys, auditors and others in the marketplace who are dealing with these requirements. We have provided responses and points of view based on our experience that we hope will assist companies as they document, evaluate and improve their internal control over financial reporting, and as they continue to enhance their executive certification process. We have also held discussions from time to time with the SEC and PCAOB staffs to understand their views on key points and confirm our interpretations in certain areas.

This fourth edition considers the SEC's interpretive guidance to management and incorporates the PCAOB's major revisions to Auditing Standard No. 2. It includes questions directed to foreign filers and U.S. domestic nonaccelerated filers and is updated for lessons learned since publication of the third edition. It also incorporates responses to frequently asked questions the SEC and PCAOB staffs have published through the date this book was released to print.

Other Protiviti publications in our Sarbanes-Oxley Frequently Asked Questions series addressing questions germane to Section 404 compliance are also available. These publications include *Guide to Internal Audit: Frequently Asked Questions About the NYSE Requirements and Developing an Effective Internal Audit Function*, *Guide to the Sarbanes-Oxley Act: IT Risks and Controls* and *Guide to the Sarbanes-Oxley Act: Managing Application Risks and Controls*. These and other publications are available at **www.protiviti.com**.

This publication is not intended to be a legal analysis. Nor is it intended to be a detailed "cookbook." Accordingly, companies should seek legal counsel and appropriate risk advisors for advice on specific questions as they relate to their unique circumstances. Companies should also seek input from their independent auditors on appropriate issues. They should also expect some of the issues addressed in this publication to continue evolving. Companies can obtain a copy of the SEC's final Section 404 rules and interpretive guidance to management, as well as the SEC staff's responses to frequently asked questions at **www.sec.gov**. Companies can also obtain a copy of the PCAOB's Auditing Standard No. 5 and the PCAOB staff's responses to frequently asked questions at **www.pcaobus.org**.

Protiviti Inc.
December 2007

Applicability of Section 404 Requirements

1. Which companies are subject to the requirements of Section 404?

Section 404 of the Sarbanes-Oxley Act states that the internal control report requirement applies to companies filing annual reports with the SEC under either Section 13(a) or 15(d) of the Securities Exchange Act of 1934 (the "Exchange Act"). These companies include banks, savings associations, small-business issuers and non-U.S. companies (i.e., foreign private issuers).

Sarbanes-Oxley defines an "issuer" as an entity that has a class of securities registered under Section 12 of the Exchange Act or that is "required to file reports under Section 15(d) [of the Securities Exchange Act of 1934] or one that files or has filed a registration statement that has not yet become effective under the Securities Act of 1933 and that it has not withdrawn." The internal control report requirement under Section 404 of Sarbanes-Oxley applies to all "issuers" because they are required to report under the securities laws.

We have received questions as to whether nonpublic subsidiaries of public companies must comply with Section 404. Although the subsidiary has no obligation to file a separate report with the SEC, the subsidiary's issuer parent will need to evaluate the subsidiary's controls and procedures if the subsidiary or any part of it is deemed to be significant to an understanding of the issuer parent's overall internal control structure.

2. Are foreign companies subject to the requirements of Section 404?

Yes, foreign issuers (including Canadian issuers) must comply. However, compliance varies for "foreign private issuers" (e.g., non-U.S. companies that file annual reports on Form 20-F or, for Canadian companies, Form 40-F) based on their accelerated filing status. Large accelerated foreign filers must comply fully with Section 404 in their annual reports for fiscal years ended on or after July 15, 2006. Accelerated foreign filers must file an internal control report in accordance with Section 404 in their annual reports for fiscal years ended on or after July 15, 2006; they must also comply with the Section 404 attestation requirements in the annual report filed for the following year. Finally, nonaccelerated foreign filers must file an internal control report in accordance with Section 404 in their annual reports for fiscal years ended on or after December 15, 2007; they must likewise comply with the Section 404 attestation requirements in the annual report filed for the following year.[1]

The Section 404 rules also require foreign private issuers to evaluate and disclose their conclusions regarding the effectiveness of their internal control over financial reporting and disclosure controls and procedures only in their annual report and not on a quarterly basis. These issuers are not subject to the quarterly reporting requirements under the Exchange Act.

3. Does Section 404 apply to small business issuers?

Yes. The final rules apply to all companies that file Exchange Act periodic reports, regardless of their size (except registered investment companies and asset-backed issuers). The SEC recognized, however, that many smaller companies might require more time to evaluate their internal control over financial reporting because they lack the formality or structure in their internal control systems that larger companies have. Thus, companies meeting the requirements of a nonaccelerated filer (among other things, these companies must have a market cap of less than $75 million) may wait to comply with the provisions of Section 404(a) requiring a management internal control report until their fiscal years ended on or after December 15, 2007. In addition, these companies may defer compliance with Section 404(b) requiring an attestation report from their independent public accountant until their fiscal years ended on or after December 15, 2008.[2]

[1] Just before this publication went to print, the SEC Commissioner announced his intention to propose an additional one-year delay for the external auditor's attestation related to smaller public companies under Section 404(b).

[2] Ibid.

4. Are unlisted companies with public debt required to comply with Section 404?

Unlisted companies with public debt must comply with the SEC's reporting requirements, including the executive certification and internal control reporting requirements, in the fiscal year the registration statement(s) for such debt is declared effective. Following that period, if at the end of any fiscal year there are fewer than 300 record holders of the debt outstanding, the company may elect to discontinue filing periodic reports with the SEC or may continue to file reports voluntarily. Many of these companies continue to report voluntarily to retain access to the capital markets or because of indenture covenants that require that periodic reports be filed with the SEC. If they do elect to report voluntarily, they must issue periodic 10-Qs and 10-Ks, and will be required to comply with the Section 302 executive certification and Section 404 internal control assessment requirements because the SEC has made those requirements an integral part of Forms 10-Q and 10-K (and the accompanying exhibits). However, because these companies are unlisted, they are considered nonaccelerated filers. Therefore, and as discussed in Question 3, they are not required to file an internal control report until their fiscal years ended on or after December 15, 2007. They also do not have to file an attestation report until their fiscal years ended on or after December 15, 2008. (Note: As this publication went to print, the SEC Commissioner announced his intention to propose an additional one-year delay for this requirement.) After the nonaccelerated filer transition period is completed, when a company voluntarily files Forms 10-Q and 10-K, it must file the entire form and comply with the related SEC rules, including providing the required Section 302 certifications and internal control report. However, Section 906 certifications are not required of voluntary filers.

Section 15(d) of the Exchange Act applies to entities that have had a registration statement declared effective under the Securities Act. There are a number of types of securities that are exempt from the registration requirements of the Securities Act, and accordingly the issuers of these securities are exempt from the filing requirements of Section 404, including issuers of certain government and municipal securities (see Question 5). However, this is a question that must be addressed case by case based upon the specific facts.

Notwithstanding the above commentary, due to the complexities involved, companies having public debt with no listed stock should consult with their legal advisors to determine their specific reporting responsibilities under Sarbanes-Oxley.

5. Are municipal utilities or universities that sell bonds required to comply with Section 404?

A good rule of thumb is if an entity must file a Form 10-K or 10-Q, it is subject to Sections 302 and 404. Under state law, municipalities are generally permitted to issue tax-exempt bonds, which are not registered with the SEC but are sold through the tax-exempt markets. That is also the case with most university debt, especially public institutions allowed under state law to issue tax-exempt General Receipt Bonds (a form of a revenue bond). The university sells the bonds through underwriters based on an official statement offering. The institution typically has indenture requirements to file the financial statements and any communications on significant events into a repository of disclosures that all tax-exempt organizations use. While municipalities and other not-for-profits are generally not subject to Sarbanes-Oxley, they should periodically take a fresh look at how they can improve their internal controls and governance processes and meet the needs of their constituencies and stakeholders.

6. Do insured depository institutions (e.g., banks and savings associations) that are already complying with the requirements of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) have to comply with Section 404?

Under regulations adopted by the FDIC implementing Section 36 of the Federal Deposit Insurance Act, insured depository institutions are required to prepare an annual management report that contains, among other things:

(1) A statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting;

(2) Management's assessment of the effectiveness of the institution's internal control structure and procedures for financial reporting as of the end of the fiscal year; and

(3) An attestation report prepared by the institution's independent accountant.

Although bank and thrift holding companies are not required under the FDIC's regulations to prepare these internal control reports, many of these holding companies do so under a provision of the FDIC's regulations that permits an insured depository institution that is the subsidiary of a holding company to satisfy its internal control report requirements with an internal control report of the consolidated holding company's management under certain circumstances. The SEC rules assert that, regardless of whether an insured depository institution is subject to the FDIC's requirements, such institutions or holding companies that are required to file periodic reports under Section 13(a) or 15(d) of the Exchange Act must comply with the SEC's internal control reporting requirements.

After consultation with the staffs of other federal agencies, the SEC decided to provide flexibility in satisfying both sets of requirements to insured depository institutions subject to Part 363 of the FDIC's regulations (as well as holding companies permitted to file an internal control report on behalf of their insured depository institution subsidiaries in satisfaction of these regulations), and also subject to the final rules implementing Section 404. Therefore, these institutions can choose either of the following two options:

- They can prepare two separate management reports to satisfy the FDIC's requirements and the SEC's new requirements; or
- They can prepare a single management report that satisfies both the FDIC's requirements and the SEC's new requirements.

If an insured depository institution or its holding company chooses to prepare a single report to satisfy both sets of requirements, the report of management on the institution's or holding company's internal control over financial reporting must contain all of the required statements under the SEC's new rules. For purposes of management's report and the attestation report of the independent public accountant, financial reporting must encompass both financial statements prepared in accordance with GAAP and those prepared for regulatory reporting purposes.

7. What is the distinction between the requirements of FDICIA and the requirements of Section 404?

Although the Commission's rules are similar to the FDIC's existing internal control reporting requirements, they differ in several respects. For example, the SEC's rules do not require a statement of compliance with designated laws and regulations relating to safety and soundness, whereas the FDIC's rules do require such a statement. However, if a compliance issue arose, it would clearly have disclosure implications. Conversely, the following provisions in the Section 404 rules are not addressed by the FDIC's regulations:

- The requirement that the report include a statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting
- The requirement that management disclose any material weakness it has identified in the company's internal control over financial reporting, as well as the attestation report prepared by the independent accountant
- The reporting standard that management may not conclude the company's internal control over financial reporting is effective if there are one or more material weaknesses
- The requirement that the company disclose that the independent accountant who audited the financial statements included in the annual report has also issued an attestation report on the effectiveness of the company's internal control over financial reporting

8. Does Section 404 apply to registered investment companies?

No. Investment companies, including mutual funds, subject to filings under the Investment Act are exempt from the provisions of Section 404, even though they must comply with Section 302 of Sarbanes-Oxley. However, the

Commission made several technical changes to the rules and forms covering investment companies in order, in part, to conform them to some of the changes adopted for operating companies. These changes include, among other things, the following:

- Defining "internal controls and procedures for financial reporting" in the same manner as for operating companies
- Requiring disclosure in Form N-SAR or Form N-CSR of any significant changes to internal controls and procedures made during the period covered by the report
- Requiring the signing officers to state that they are responsible for establishing and maintaining internal control over financial reporting, and that they have disclosed to the investment company's auditors and audit committee all significant deficiencies in the design and operation of internal control over financial reporting that could adversely affect the investment company's ability to record, process, summarize and report financial information required to be disclosed in the reports that it files or submits under the Exchange Act and the Investment Company Act

The SEC does not require the evaluation by an investment company's management of the effectiveness of its disclosure controls and procedures to be as of the end of the period covered by each report on Form N-CSR, similar to an operating company. Thus, these companies are required to evaluate their disclosure controls within 90 days prior to the filing date of the report. Investment companies having funds with staggered fiscal year-ends would have to perform evaluations of their disclosure controls and procedures as many as 12 times per year if they were to apply the same rules as operating companies. The certification rules the SEC adopted only require an investment company to perform at most four evaluations per year.

9. Does Section 404 apply to U.S. divisions or units of foreign-based companies?

Only companies filing annual reports with the SEC under either Section 13(a) or 15(d) of the Exchange Act must comply with Section 404. Thus if the foreign-based company does not file such annual reports, Section 404 does not apply either to it or to its U.S. divisions or units.

10. Does Section 404 apply to not-for-profit entities?

No. However, not-for-profit entities benefit from effective internal control over financial reporting. To the extent that they provide financial reports to trustees, donors, governmental agencies and other stakeholders, or are otherwise accountable to these stakeholders, these entities have a responsibility for effective governance and fair reporting. Furthermore, at least one state (New York) is considering legislation that would impose on not-for-profit entities obligations similar to those under Sarbanes-Oxley, including internal control evaluations. (See also Question 4 for applicability to unlisted companies with public debt.)

11. Does Section 404 apply to asset-backed issuers?

No. Issuers of asset-backed securities are not required to implement Section 404. Because of their unique nature, asset-backed issuers are subject to substantially different reporting requirements. For example, they generally are not required to file the types of financial statements that other companies must file and are typically passive pools of assets, without a board of directors or persons acting in a similar capacity. Notwithstanding these differences, the SEC does require that asset-backed issuers file special certifications to comply with Section 302.

12. Does Section 404 apply to forward-looking financial information?

No. Section 404 is focused on the historical financial statements (which, by definition, include the footnotes). With respect to the disclosure of financial projections and similar forward-looking information on analyst calls and in other public venues such as shareholder meetings, such disclosures must be consistent with information

provided in public reports. For example, the SEC has said disclosures of financial information for a completed fiscal period in a presentation that is made orally, telephonically, by webcast, by broadcast or by similar means will not be required to be filed, if (1) the presentation occurs within 48 hours of a related release or announcement that is filed on Form 8-K; (2) the presentation is broadly accessible to the public; and (3) the information in the webcast is posted on the company's website. The information in these various venues must be consistent with the information included in financial and public reports.

13. Does Section 404 apply to the MD&A disclosures?

The Management's Discussion and Analysis (MD&A) is not a part of the financial statements, which are the primary focus of Section 404. The processes that facilitate preparation of the MD&A, therefore, are not subject to an audit of internal control over financial reporting. The PCAOB staff has reaffirmed this point of view. However, auditing standards require the auditor to review unaudited information to satisfy him/herself that there are no material inconsistencies with the information presented in the audited financial statements. As "unaudited information," the MD&A falls under the scope of those standards, and much of the information in the MD&A comes directly from the financial statements. From management's perspective, the MD&A is covered by the disclosure controls and procedures addressed by the Section 302 executive certification. The significance of keeping MD&A within the bounds of Section 302 is that the external auditor is not required to audit the controls over the preparation of MD&A.

What Is Section 404 and How Does It Relate to Sections 302 and 906?

14. What does Section 404 require companies to do annually?

Section 404 of Sarbanes-Oxley mandates the SEC to adopt rules requiring each issuer, other than a registered investment company, to include an internal control report that contains management's assertions regarding the effectiveness of the company's internal control structure and procedures over financial reporting. Section 404 also requires the company's independent auditor to attest to the effectiveness of the company's internal control over financial reporting in accordance with standards established by the PCAOB.

Pursuant to the SEC's rules on Section 404, the internal control report must articulate the following:

- Management's responsibilities to establish and maintain adequate internal control over financial reporting for the company
- The framework used by management to provide criteria for evaluators to assess the effectiveness of the company's internal control over financial reporting
- Management's assessment as to the effectiveness of the company's internal control over financial reporting based on management's evaluation of it, at year-end (i.e., a point-in-time assessment), including disclosure of any material weakness in the company's internal control over financial reporting identified by management

Management's report also must state that the company's independent public accountant who audited the financial statements included in the annual report has attested to and reported on management's evaluation of internal control over financial reporting.

The SEC's rules provide a threshold for concluding that a company's internal control over financial reporting is effective by providing that management is not permitted to reach such a conclusion if there are one or more material weaknesses in internal controls. Thus, an assertion that internal control over financial reporting is effective both in design and in operation is also an assertion by management that there are no material weaknesses in such internal control. The SEC's rules require disclosure to the public of any material weaknesses identified by management during the assessment.

To further clarify management's responsibilities, the SEC has issued principles-based interpretive guidance. This guidance is organized around two important principles:

Principle	Implications to Management
Management should evaluate the design of the controls that it has implemented to determine whether there is a reasonable possibility that a material misstatement in the financial statements would not be prevented or detected in a timely manner	Management applies a top-down, risk-based approach that promotes efficiency by focusing only on those "key controls" that are needed to prevent or detect material misstatement in the financial statements
Management should gather and analyze evidence about the operation of the controls being evaluated based on its assessment of the risk associated with those controls	Management aligns the nature and extent of the evaluation procedures with those areas of financial reporting that pose the greatest risk of control failure

In essence, the SEC guidance explains that "risk" includes both the risk of material error or fraud and the risk of control failure. These two components of risk are referred to as "ICFR risk."

15. What does Section 404 require companies to do quarterly?

With regard to internal control over financial reporting, the SEC decided not to require quarterly evaluations that are as extensive as the annual evaluation. The Commission is of the view that management should perform an evaluation of the design and operation of the company's entire system of internal control over financial reporting over a period of time that is adequate to permit management to determine whether, as of the end of the company's fiscal year, the design and operation of the company's internal control over financial reporting are effective.

However, management is required to disclose any change in controls that occurred during a fiscal quarter that has materially affected, or is reasonably likely to materially affect, the company's internal control over financial reporting. Although the final rules do not explicitly require the company to disclose the reasons for any change that occurred during a fiscal quarter (including the fourth quarter), or to otherwise elaborate about the change, a company will have to determine, on a facts and circumstances basis, whether the reasons for the change, or other information about the circumstances surrounding the change, constitute material information necessary to make the disclosure about the change not misleading to investors.

The quarterly certification requirement under the Section 302 rules also requires management to disclose in a timely manner significant deficiencies and material weaknesses to the audit committee and to the independent accountant. The SEC expects that if a certifying officer becomes aware of a significant deficiency, material weakness or fraud requiring disclosure outside of the formal evaluation process or after management's most recent evaluation of internal control over financial reporting, he or she will disclose it to the company's auditors and audit committee.

With respect to disclosure controls and procedures, the SEC's rules under Section 302 require an evaluation as of the end of the period covered by the quarterly or annual report (however, see comments in Question 8 regarding registered investment companies). For purposes of evaluating the effectiveness of disclosure controls and procedures on a quarterly basis, disclosure in quarterly reports may make appropriate reference to disclosures in the most recent annual report (and, where appropriate, intervening quarterly reports) and, as required, disclose subsequent developments in the quarterly report. For example, disclosure in an annual report that continues to be accurate and current need not be repeated.

16. How often must management assess internal control over financial reporting?

The SEC's rules for compliance with Section 404 require management to make an annual assessment of the company's internal control over financial reporting and to evaluate quarterly the impact of changes on such

controls. These evaluations are accomplished in conjunction with each filing of a quarterly report and with the filing of the annual report (in which an internal control report must be included).

17. Is Section 404 limited to public reports for which executive certification requirements are required?

Yes. The requirements of both Section 302 (quarterly executive certifications) and Section 404 (annual evaluation of internal controls) are triggered when companies file quarterly reports and, with respect to the internal control report and auditor attestation report required by Section 404, when companies file annual reports with the SEC under either Section 13(a) or 15(d) of the Exchange Act.

18. What does Section 302 of the Sarbanes-Oxley Act require companies to do?

Section 302 applies to companies filing quarterly and annual reports with the SEC under either Section 13(a) or 15(d) of the Exchange Act. Section 302 requires a company's principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, to certify each quarterly or annual report. For most companies, the certifying officers are the CEO and CFO. While companies have the flexibility to have others sign the certification in addition to the CEO and CFO if they determine it is appropriate to do so because of the extent of their involvement in the financial reporting and disclosure process, we have rarely seen this happen.

Section 302 has two primary requirements. First, the certifying officers must issue a certification. Second, their companies must make certain disclosures. These requirements are discussed below and apply to any periodic filings due on or after August 14, 2003.

Executive Certification – The SEC's rules specify the form of the certification in detail. Generally, the SEC rules require the certifying officers to state the following:

- They have reviewed the report.
- Based on their knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which they were made, not misleading with respect to the reporting period.
- Based on their knowledge, the financial statements and other financial information in the report fairly present in all material respects the financial condition, results of operations and cash flows of the company as of, and for, the periods presented in the report.
- They are responsible for establishing and maintaining "disclosure controls and procedures" and "internal control over financial reporting" for the issuer and have:
  - Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under their supervision, to ensure that material information is made known to them, particularly during the period in which the periodic report is being prepared
  - Designed internal control over financial reporting, or caused such internal control over financial reporting to be designed under their supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles
  - Evaluated the effectiveness of the issuer's disclosure controls and procedures as of the end of the period covered by the report, and have presented in the report their conclusions about the effectiveness of the disclosure controls and procedures based on their evaluation
  - Disclosed in the report any change in the issuer's internal control over financial reporting that occurred during the issuer's most recent fiscal quarter (the "fourth fiscal quarter" in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the issuer's internal control over financial reporting

- They have disclosed, based on their most recent evaluation of internal control over financial reporting, to the auditors and to the audit committee:
  - All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting that are reasonably likely to adversely affect the company's ability to record, process, summarize and report financial information; and
  - Any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal control over financial reporting.

Based upon current SEC rules, the certification format is the same, whether the report is "clean" or not, because Section 302 of Sarbanes-Oxley prescribed the wording. While the SEC modified the language of Sarbanes-Oxley slightly, it did so based on the premise of congressional intent. The SEC makes it clear that the wording of the required certification may not be changed, and will allow only minor exceptions, such as (i) changing the reference to the "other certifying officers" from the plural form to the singular form, and (ii) adding an officer's title under his or her signature. For example, the certifying officers cannot include a modifier or limitation stating that the work to support the report was done at a point in time and that controls could change after that date. Nor is management permitted to issue a report with a scope limitation for outsourced processes when (a) the issuer is unable to obtain the requisite SAS 70 letter from the service organization and assess the underlying controls, and (b) sufficient compensating controls are not in place. The SEC has not accepted certifications of companies that did not follow verbatim the prescribed wording (however, see Question 236).

For newly public companies and other companies that are not yet subject to Section 404, the SEC has advised that officers should delete portions of the text related to internal control over financial reporting in the certification because these portions of the required certifications do not become effective until after management files the first Section 404 internal control report. Specifically, the first reference to "internal control over financial reporting" in the fourth paragraph of the certification and the entire second subpoint regarding the design of such controls in the fourth paragraph should be deleted until a certification is filed for the first interim period following the year in which the company becomes Section 404 compliant. Question 31 discusses this important point further.

Make Certain Disclosures – Item 307 of Regulation S-K requires the company to disclose the conclusions of its principal executive and principal financial officers (or persons performing similar functions) regarding the effectiveness of the company's disclosure controls and procedures as of the end of the period covered by the report. This disclosure is pursuant to the requirements of Item 4 in Form 10-Q and Item 9B in Form 10-K.

19. What does Section 906 of the Sarbanes-Oxley Act require companies to do?

Section 906 requires a separate certification from the one required by Section 302. The Section 906 certification requirement differs from Section 302 in at least three respects:

- Section 906 expressly imposes criminal penalties, whereas Section 302 relies on the general criminal penalty provision that applies to all violations of the Exchange Act.
- The Section 906 certification is a shorter representation basically stating that the periodic report containing the financial statements fully complies with the requirements of Section 13(a) or 15(d) of the Exchange Act, and that the information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer.
- Unlike the Section 302 certifications, the Section 906 certifications are required only in periodic reports that contain financial statements.

The two sets of certification requirements under Sections 302 and 906 surfaced from different facets of the legislative process. Both are required even though they overlap significantly. A fraudulent Section 302 certification is subject to civil enforcement by the Commission, and a fraudulent Section 906 certification carries criminal penalties enforceable by the Department of Justice. The comprehensive evaluations and assessments required of the certifying officers under Section 302 also should enable these officers to sign the certification required by Section 906.

20. How are the requirements under Section 404 and the requirements under Sections 302 and 906 of the Sarbanes-Oxley Act related?

Sections 302 and 906 contain two certification requirements that lay a foundation for restoring investor confidence in the integrity of public reporting. Section 404 builds on this foundation. These three sections, along with Section 409 (which deals with "real-time disclosures") and other provisions in Title IV of Sarbanes-Oxley, are inextricably linked and comprise the public reporting aspects of the Act. They are summarized below:

Comparison of Sections 302, 404 and 906

	Section 302	Section 404	Section 906
When is it effective?	August 29, 2002	Fiscal years ended on or after: • November 15, 2004, for U.S. accelerated filers* • July 15, 2006, for foreign accelerated filers* • December 15, 2007, for others	July 30, 2002
Who signs off?	• CEO • CFO	• Management • Independent accountant	• CEO • CFO
What's it about?	• Executive certification issued quarterly	• Internal control report annually • Independent accountant attests to annual report • Quarterly review for change	• Abbreviated certification issued quarterly • Criminal penalties
How often are the evaluations?	• Quarterly evaluation	• Annual assessment • Quarterly review for change	• Quarterly evaluation

* See Questions 23 and 242 for a discussion of large accelerated filers and accelerated filers, as well as differentiation of effective dates for management and attestation reports.

Sections 302, 404 and 906 (along with other sections of Title IV) are related in at least two important ways:

- First, internal control over financial reporting (addressed by Section 404) generally is a subset of disclosure controls and procedures (addressed by Section 302). The SEC has issued rules that require issuers to maintain, and regularly evaluate the effectiveness of, disclosure controls and procedures designed to ensure the information required in reports filed under the Exchange Act is recorded, processed, summarized and reported on a timely basis.

  As defined by the Commission, "disclosure controls and procedures" applies to material financial and nonfinancial information required to be included in public reports so that investors are fully informed. This definition is broader than the scope of internal control over financial reporting. To the extent that internal control over financial reporting impacts disclosure, a company's disclosure controls and procedures are clearly inclusive of such internal controls because disclosure controls apply to all material financial and nonfinancial information to be included in public reports, both within and outside the financial statements. In this context, materiality applies to the information investors need in order to make informed judgments. Thus, the delineation between what is material and what is not material applies to nonfinancial as well as financial information.

- Second, the primary message underlying the public reporting provisions of Sarbanes-Oxley and the rules and interpretive guidance issued by the SEC is that ad hoc reporting and disclosure activities are substandard. Financial reporting processes and the related internal controls that are in place to produce reliable financial statements must be consistently performed, clearly defined and effectively managed. The processes for generating nonfinancial information presented outside the financial statements are expected to become more formalized, consistent with a process-based approach.

For a comparison of disclosure controls and procedures and internal control over financial reporting, see Question 37.

When certifying officers sign their certifications, they are representing that they possess or have access to the collective knowledge of the company regarding any and all information that is material to investors. They are or should be, in effect, certifying management's internal processes. Therefore, the evaluation of internal control over financial reporting is integral to the certification process.

21. How does the Section 404 assessment enhance the Section 302 executive certification process?

Section 404 documentation and assessments, by definition, enhance the Section 302 executive certification process because, as noted in Question 20, there is a substantial overlap between internal control over financial reporting (covered by Section 404) and disclosure controls and procedures (covered by Section 302). Section 404 compliance results in, among other things, a top-down, risk-based approach focused on control-related policies, activities, personnel, reports, methodologies and systems. It also establishes process owner accountability. Both of these outcomes enhance the quality of the Section 302 executive certification process.

The SEC's rule on Section 302 recommends a disclosure committee. Many companies also have formed a Section 404 project management organization (PMO) or steering committee. Question 201 provides commentary as to the interrelationships between these two committees as they address common issues of mutual interest, e.g., formatting the internal control report, establishing criteria for identifying and reporting significant deficiencies and material weaknesses, evaluating internal control-related disclosures, etc.

Once the Section 404 process is completed, much knowledge is gained regarding the key controls and the owners of those controls. That knowledge can be used to organize an ongoing self-assessment process supporting both Section 302 and Section 404 compliance going forward. An effective self-assessment process, enabled by the information gained by Section 404 compliance, frees up the certifying officers to focus on the impact of change on the internal control structure. Significant deficiencies and material weaknesses identified by the Section 404 assessment must be disclosed to the audit committee and the external auditor as soon as practicable, consistent with the requirements of Section 302. Note that the executive certification specifically represents that management has disclosed such deficiencies in a timely manner.

These are some of the ways the Section 404 assessment process enhances the Section 302 executive certification process. See Questions 186 through 197 for a discussion of alternative structures for complying with Sections 302 and 404, after the first internal control report is filed.

22. Is there a value proposition from a controls assessment process beyond compliance with Section 404?

Yes, there is. In responding to this question, there are two related points. First, what is accomplished by complying with Section 404? Second, can a controls assessment do more than merely comply with Section 404?

The reduction of regulatory risk (i.e., the risk of noncompliance with Sarbanes-Oxley and the SEC's regulations) is accomplished through applying in good faith the SEC's interpretive guidance to document in reasonable detail the relevant risks, the key controls, the appropriate test plan and the execution of that test plan in a manner that *provides a credible body of evidence* that the certifying officers have established effective internal control over financial reporting. Risk reduction is also accomplished through identification of key risk areas and control points that enable the certifying officers *to better manage the critical processes and controls* and *drive accountability throughout the organization*.

A controls assessment can – and over time should – go beyond regulatory compliance. For example, management can have its processes and procedures reviewed to *reduce the risk of financial reporting restatements and fraud.* To illustrate, AuditAnalytics™ published a study in February 2007 reporting a decline in the rate of restatements among accelerated filers after these companies had experienced two cycles of Section 404 compliance. The reported rate of decline for restatements was from 16.1 percent to 13.3 percent of all accelerated filers. Conversely, restatements associated with nonaccelerated filers increased significantly during the same period. The message is that Section 404 compliance reduces restatement risk. This point is important

because a reduction of restatement risk decreases a company's exposure to the market cap declines that inevitably result from these events (see commentary regarding a 2006 Lord & Benoit study in Question 181). Recognizing its continuing reporting obligations, management also should extend the emphasis on the initial annual assessment of controls to *create a sustainable monitoring process* for continued compliance over time.

Management can also evaluate the effectiveness of internal controls against other objectives to *identify improvements in process effectiveness and efficiency to reduce costs*, e.g., reduce closing process cycle time, simplify and eliminate redundant and inefficient controls, improve effectiveness of controls design, and reduce the level of external audit fees. Finally, management can focus the assessment of processes to improve management of the business, e.g., satisfy customers faster, better and at lower cost. In summary, a cost-effective and sustainable compliance process also can facilitate improving the quality of the internal control structure and the upstream business processes impacting financial reporting.

When Is Section 404 Effective for Different Companies?

23. When do companies have to comply with the Section 404 requirements?

The initial implementation of Section 404 was based on a transitional period tied to a company's classification under the SEC's accelerated filer rules. The idea was to require the larger issuers to comply first. The specific timing requirements in the final rules were initially defined for two groups, the first one consisting of companies meeting the definition of an "accelerated filer" in Exchange Act Rule 12b-2. Generally, an "accelerated filer" is a company that (i) has equity market capitalization over $75 million, (ii) has been subject to the requirements of Section 13(a) or 15(d) of the Exchange Act for at least 12 months, (iii) has filed an annual report with the Commission, and (iv) is not eligible to use Forms 10-KSB or 10-QSB for its annual and quarterly reports. These companies are required to comply with the Commission's accelerated filing requirements for 10-Ks and 10-Qs; therefore, they have the distinction of being "accelerated filers." The U.S. domestic accelerated filers were required to file a management report on internal control over financial reporting beginning in fiscal years ending on or after November 15, 2004. Large foreign private issuers classified as accelerated filers were to comply with the Section 404 reporting requirements for their first fiscal year ending on or after July 15, 2006.

During the last quarter of 2006, the SEC modified its requirements around this first group of companies by creating a new classification under the accelerated filer rules – the so-called "large accelerated filer" with a market capitalization of $700 million or more. Thus, the first group of companies now consists of large accelerated filers and accelerated filers. For U.S. companies, this change had no effect because such companies already were to have complied with Section 404. For foreign private issuers, however, the accelerated filers (companies with an equity market capitalization of more than $75 million, but less than $700 million) were given an additional year (i.e., fiscal years ending on or after July 15, 2007) to comply with Section 404(b), the provision requiring an attestation report.

The second group of companies consists of all other issuers, including small-business issuers and foreign private issuers qualifying as nonaccelerated filers. For these companies, whether domestic or foreign, compliance with Section 404(a), which requires management to issue an internal control report, is required for fiscal years ending on or after December 15, 2007. Furthermore, compliance with Section 404(b) was further delayed for an additional year (i.e., fiscal years ending on or after December 15, 2008), with an additional year delay expected to be proposed as this publication went to print. To illustrate, calendar-year reporting companies are required to file their first internal control report with the Form 10-K for calendar year 2007, which would be filed no later than March 2008. If the SEC delays the deadline for another year, as expected, the independent auditor's attestation report would not be required until the Form 10-K for calendar year 2009, which would be filed no later than March 2010.

The following table summarizes the previous discussion:

		Revised Compliance Dates and Final Rules Regarding the ICFR Requirements	
	Accelerated Filer Status	**Management's Report**	**Auditor's Attestation**
U.S. Issuer	Large Accelerated Filer ***or*** Accelerated Filer ($75 million or more)	Already complying	Already complying
	Nonaccelerated Filer (less than $75 million)	Annual reports for fiscal years ending on or after December 15, 2007	Annual reports for fiscal years ending on or after December 15, 2009
Foreign Issuer	Large Accelerated Filer ($700 million or more)	Annual reports for fiscal years ending on or after July 15, 2006	Annual reports for fiscal years ending on or after July 15, 2006
	Accelerated Filer ($75 million or more but less than $700 million)	Annual reports for fiscal years ending on or after July 15, 2006	Annual reports for fiscal years ending on or after July 15, 2007
	Nonaccelerated Filer (less than $75 million)	Annual reports for fiscal years ending on or after December 15, 2007	Annual reports for fiscal years ending on or after December 15, 2009

Note that the dollar amounts in the table refer to the worldwide market value of outstanding voting and nonvoting common equity held by nonaffiliates.

As this publication went to print, the SEC Commissioner announced his intention to propose an additional one-year delay for the external auditor's attestation related to smaller public companies under Section 404(b). The above table reflects this intent.

These transition rules apply to companies other than registered investment companies. Registered investment companies were required to comply with the rule and form amendments applicable to them beginning August 14, 2003, except as follows: Registered investment companies were required to comply with the amendments to Exchange Act Rules 13a-15(a) and 15d-15(a) and Investment Company Act Rule 30a-3(a) that require them to maintain internal control over financial reporting with respect to fiscal years ending on or after November 15, 2004.

Once the transition rules expire and all public companies, regardless of their status as accelerated or nonaccelerated filers, are required to be Section 404-compliant, the question arises as to when a newly public company must comply. See Question 26.

24. Why did the SEC defer the effective date of Section 404 compliance?

The Commission has deferred the effective compliance date several times. These delays have had several purposes:

- First, the Commission provided companies an opportunity to complete the preparatory work that is needed to comply.
- Second, the auditors needed time to gear up for these new requirements.
- Third, the PCAOB needed time to develop its rules on the independent auditor's attestation process and to consider whether additional standards or guidance are appropriate.
- Finally, the Commission sought to provide smaller U.S. public companies and foreign private issuers, as well as their auditors, more time to address the requirements.

Thus, the Commission staff wanted to provide companies more time to do a thorough job. For example, the activities of documenting processes and controls, evaluating control design effectiveness, validating control operating effectiveness and remediating control deficiencies to close gaps could be accomplished over a longer period of time, provided that companies took advantage of the additional time. The longer transition period was

appropriate in light of both the substantial time and resources needed by companies to properly implement the rules, and the corresponding benefit to investors that would result from companies' proper implementation of the new requirements. With respect to the most recent deferral, both the SEC and PCAOB have collaborated to make the Section 404 compliance process and the attestation process more cost-effective and scalable to reduce the disproportionate compliance cost burden on smaller companies.

25. What happens if an issuer that is currently not an accelerated filer qualifies as an accelerated filer because of an increase in market capitalization? When does the issuer have to file an internal control report?

The significance of this question to Section 404 compliance is that the transition period for initial compliance varies depending on whether a company is an "accelerated filer." The requirements for this determination are discussed in Questions 244 and 245. Market capitalization is relevant to determining whether a company is an accelerated filer: The threshold is $75 million and, for a given fiscal year, the determination is made as of the end of the most recent second quarter. Smaller companies will have to ask themselves, "Was my public common float $75 million or greater at the end of my most recent second quarter?" If the answer is "yes" and the company also meets the other criteria of an accelerated filer as described in Questions 23 and 245, then the company must file an internal control report for that year.

Smaller companies "on the bubble" during the transition period discussed in Question 23 must pay close attention to this determination. For example, depending upon their current market capitalization, business plans and the market in general, smaller companies that are dynamic, growing, acquisitive and/or planning to tap the equity markets need to be careful about deferring compliance with Section 404 because they could find themselves in crisis mode to comply.

26. Assume Company A, which reports on a calendar year, plans to go public this year and is expecting a capitalization below the $75 million accelerated filer threshold. When must it comply with Section 404?

All newly public companies, regardless of size, have a transition period granted them by the SEC that enables them to elect not to comply with the Section 404 requirements until after the first annual report that they file after becoming an Exchange Act reporting company. This transition period applies to a company that has become public through an initial public offering (whether equity or debt) or a registered exchange offer or that otherwise has become subject to the Exchange Act reporting requirements. It also includes a foreign private issuer that is listed on a U.S. exchange for the first time. The transition period is intended to permit newly public companies to concentrate on their initial securities offerings and to prepare for their first annual report without the additional burden of having to comply with the Section 404 requirements at the same time.

With respect to reverse mergers (the acquisition of an operating company by an empty public shell corporation with the operating company being the surviving entity), the SEC staff has indicated they will not approve the "newly public company" designation for these entities for purposes of deferring Sarbanes-Oxley compliance.

27. When is the internal control report due?

The report is due when the Form 10-K is filed for the year Section 404 is effective.

28. Does the independent accounting firm express an opinion on management's assertions regarding internal control over financial reporting?

No, the independent auditor is not required to attest to and report on management's assessment process. An audit of internal control over financial reporting is limited to an evaluation of whether, in the auditor's opinion, the company's internal control over financial reporting is effective, and does not include an opinion on the

adequacy of management's assessment process. However, the auditor is expected to obtain an understanding of management's process as a starting point to understand the company's internal control, assess risk and determine the extent to which he or she will use the work of others. The quality of management's assessment process is inversely related to the amount of work the auditor will need to do to complete an audit of internal control over financial reporting. The higher the quality of management's assessment process, the less work the auditor will need to perform.

29. As of what date is management's annual assessment conducted?

Management's annual assessment of internal control over financial reporting is a point-in-time assessment as of the end of the company's fiscal year. Management may test and evaluate the controls over a period of time during the year, but the assessment must be made at a single point in time (i.e., did the necessary controls exist at the end of the financial reporting period and were they operating effectively at that time?). However, to support this assessment, it is necessary to demonstrate operating effectiveness over a sufficient period of time (see Questions 130 and 158).

30. Is a quarterly assessment required of internal control over financial reporting?

A company's management (including its CEO and CFO) must evaluate any change in the company's internal control over financial reporting that occurred during a fiscal quarter that has materially affected, or is reasonably likely to materially affect, the company's internal control over financial reporting. This requirement begins with the first periodic report due after the first annual report required to include a management report on internal control over financial reporting. Thus, companies required to file an internal control report for calendar year 2006 are required to begin their quarterly evaluation of changes made during the first quarter of calendar year 2007. See also Question 15.

31. If management is not required to assess internal control over financial reporting until the first internal control report is issued, what about the references to such internal controls in the quarterly executive certifications required by Section 302?

As noted in Question 18, the executive certification makes references to internal control over financial reporting. The SEC's rules on Section 404 have allowed the company's certifying officers to temporarily modify the content of their Section 302 certifications to eliminate certain references to internal control over financial reporting. For example, under the new rules, the certifying officers must state that they "are responsible for establishing and maintaining … internal control over financial reporting" and "designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under [their] supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles." The new rules allow the certifying officers to modify, during the transition period discussed in Question 23, the content of their Section 302 certifications to eliminate these references until the first 10-K in which the company is required to issue an internal control report.

While this transition period allows companies to exclude the language introduced in the previous paragraph from their certifications for the duration of that period, it does not in any way affect the provisions of the SEC's other rules and regulations regarding internal controls that are already in effect. For example, the certifying officers are still required to certify that they have informed the company's auditors and audit committee about significant deficiencies and material weaknesses in internal control, as well as any fraud involving employees who have a significant role in internal control.

What Is Meant by "Internal Control Over Financial Reporting" and "Disclosure Controls and Procedures"?

32. What is "internal control over financial reporting"?

The SEC rules define the term "internal control over financial reporting" to mean the following:

> A process designed by, or under the supervision of, the issuer's principal executive and principal financial officers, or persons performing similar functions, and effected by the issuer's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:
>
> - Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;
> - Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and
> - Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements.

While the above definition is consistent with the COSO framework, it also incorporates language from Sarbanes-Oxley by placing the ultimate responsibility with the company's certifying officers. It also refers to safeguarding of assets, addressing COSO's supplement to the Integrated Framework after it was originally released.

The SEC's definition of internal control over financial reporting does not encompass the effectiveness and efficiency of a company's operations and a company'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. The definition is consistent with the description of internal accounting controls in Exchange Act Section 13(b)(2)(B).

33. What are "disclosure controls and procedures," a key component of the certification requirements under Section 302?

The SEC introduced "disclosure controls and procedures" as a new term in its initial August 29, 2002, release following the enactment of Sarbanes-Oxley. Disclosure controls and procedures are controls and other procedures designed to ensure that information required to be disclosed by the company in its Exchange Act reports is recorded, processed, summarized and reported within the time periods specified in the Commission's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by the company in its Exchange Act reports is accumulated and communicated to the company's management (including its principal executive and financial officers) for timely assessment and disclosure pursuant to the SEC's rules and regulations. The SEC intended to make it explicit that the controls contemplated by Sarbanes-Oxley should embody controls and procedures addressing the quality and timeliness of disclosure in public reports.

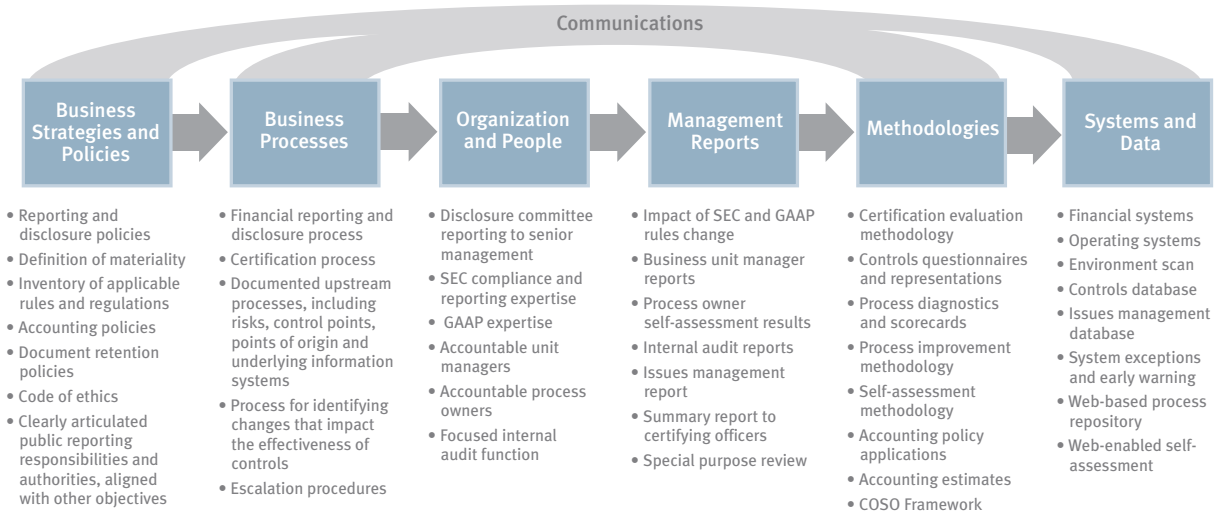
With respect to these rules, the SEC states the following:

> The certification statement regarding fair presentation of financial statements and other financial information is not limited to a representation that the financial statements and other financial information have been presented in accordance with generally accepted accounting principles (GAAP) and is not otherwise limited by reference to GAAP. We believe that Congress intended this statement to provide assurances

that the financial information disclosed in a report, viewed in its entirety, meets a standard of overall material accuracy and completeness that is broader than financial reporting requirements under GAAP. A "fair presentation" of an issuer's financial condition, results of operations and cash flows encompasses the selection of appropriate accounting policies, proper application of appropriate accounting policies, disclosure of financial information that is informative and reasonably reflects the underlying transactions and events, and the inclusion of any additional disclosure necessary to provide investors with a materially accurate and complete picture of an issuer's financial condition, results of operations and cash flows.

In summary, disclosure controls and procedures are the activities in place that ensure material financial and non-financial information required to be disclosed is identified and communicated in a timely manner to appropriate management, including the certifying officers, so that decisions can be made regarding disclosure.

Effectively designed and operating disclosure controls and procedures require an infrastructure of policies, processes, people, reports and systems. The following summary illustrates examples of key components of the disclosure infrastructure. These components are consistent with how many managers view and run a business.



Examples of disclosure controls and procedures are further discussed in Questions 34, 35 and 36.

34. What are examples of disclosure controls and procedures that generate required disclosures?

Following are examples of disclosure controls and procedures that generate disclosures required to be filed in public reports:

- ***Form a disclosure committee to organize and oversee the disclosure process.*** Many companies have adopted some form of a disclosure committee. For example, based on a study published in September 2003, Protiviti found that almost 75 percent of companies with more than $500 million in annual revenues had formed a disclosure committee. This committee considers the materiality of information, determines disclosure requirements on a timely basis, identifies relevant disclosure issues, and coordinates the development of the appropriate infrastructure to ensure that material information is elevated in a timely manner to the appropriate level of management for potential action and disclosure. If a company forms a disclosure committee, it is important that the committee discharges its assigned functions and activities as articulated in its charter. It doesn't help to form a disclosure committee and define its tasks only to have it fail in execution. However, if a disclosure committee isn't in place, the company's certifying officers must address how they will achieve the specified tasks a committee is intended to achieve. See Question 198 for further discussion.

- ***Use a standard reporting package or process to engage the appropriate unit managers and process owners, and funnel the required information upward.*** This upward communication is vital to effective disclosure controls and processes. While a standard reporting package is a common practice followed by many companies, we see companies enhancing their reporting packages to facilitate upward communications of material information from unit managers and process owners and making them an integral part of the disclosure process. For example, one company developed a standard monthly reporting package for all operating units that included, among other things, a representation letter, an analysis of variations and fluctuations in operations, an internal control evaluation, a risk assessment relating to changes in operations (e.g., changes in personnel, changes in systems, changes in business practices, etc.), a summary of related parties, and the financial statements. The company's disclosure committee reviews each reporting package, follows up on questions and significant unresolved issues, and documents the results of that follow-up. The reporting packages are subject to review by internal audit and the independent public accountant. This process funnels upward information about new risks, changes and issues to management and, ultimately, to the certifying officers.
- ***Inventory the reporting requirements and maintain a current inventory.*** Regulation S-K, Regulation S-X, up-to-date GAAP checklists and other checklists provide a basis for determining the universe of reporting requirements. Management or the disclosure committee should use these checklists to determine the applicable requirements and ensure the requisite policies, activities and subject matter expertise are brought to bear so that an effective infrastructure is in place to identify, record, process, summarize and report the required information.
- ***Design and implement a process to address each required disclosure.*** Once the disclosure requirements are identified, management should understand and, if appropriate, document the disclosure creation process, communicate it to responsible individuals, and clarify their roles, responsibilities and authorities for generating the required disclosures. The organization's critical disclosure controls and procedures should be documented by the disclosure committee, or an equivalent group of executives, and approved by appropriate management, including the certifying officers. Accountability for executing these controls and procedures should be established by submitting the written documentation to the personnel responsible and requiring them to acknowledge their understanding in writing. Staffing and training requirements should be evaluated to ensure everyone understands what is expected.
- ***Conduct a financial reporting risk profile.*** When the controls related to the significant financial reporting elements are subject to the risk of management override, involve significant judgment or are complex, they should generally be assessed as having higher financial reporting risk. The underlying premise of a financial reporting risk profile is to answer the question, "Do management and the audit committee know where the soft spots are with respect to the company's financial reporting?" The pitfalls associated with consistently achieving accurate and reliable financial statements are too numerous not to take a fresh look from time to time. An effective financial reporting risk profile focuses on six areas: (1) accounting principle selection and application, (2) estimation processes, (3) related party transactions, (4) business transaction and data variability, (5) sensitivity analysis, and (6) measurement and monitoring. The objective of a financial reporting risk profile is to identify the areas where there is a reasonable possibility of potential misstatements so that the appropriate oversight and control can be established to reduce financial reporting risk to an acceptable level. The profile can provide a powerful source of input into the Section 404 risk assessment process.
- ***Establish a tracking system for routine disclosures.*** Management should assign responsibility to specific individuals or groups for generating the required disclosures, as noted by the reporting requirements inventory, and define specific timetables to allow for timely preparation, assembly and review. Progress in relation to established timetables must be monitored.
- ***Source material information components in public reports back to upstream processes and points of origin, and identify the critical processes that generate them.*** As we've seen in practice, an effective solution often focuses on evaluating the financial reporting process and the infrastructure that ensure effective disclosure controls and procedures. The critical upstream processes that feed the financial reporting and public

disclosure process should then be reviewed, with the appropriate process owners assuming responsibility for that review. Management can identify these critical processes by decomposing the critical information in the public reports into appropriate segments, assigning segments by responsible function (e.g., operations, HR, GC, treasury, insurance, investor relations, etc.) and working backwards to identify the relevant processes that record, process, summarize and report that information. These processes should be ranked according to criticality using appropriate criteria, such as pervasiveness of importance to the company's operations, impact on public reports, susceptibility to change, potential for material errors, etc.

Every company must decide the level of granularity that is appropriate for their circumstances. Following are some points to consider:

- *The owner of the period-end financial reporting process manages the accumulation of the necessary data and information through a disclosure control used to monitor completion, much like a project management organization (PMO) (see Question 47).* As noted earlier, an up-to-date disclosure checklist is useful for reviewing submitted drafts for completeness.
- *For items that are relatively simple and straightforward, the appropriate disclosure control might be to focus on using the disclosure checklist and reporting timeline, assigning the relevant segment by function and the date due.* Often, there is a presumption that the requisite information and data within a given disclosure segment would be provided consistent with the prior year. Take the description of facilities, for example. Does the company need to document the process that the real estate function uses to generate the list of facilities or is the responsibility for the disclosure assigned to the real estate function with a firm deadline? If the facilities are relatively stable year-to-year and can even be reviewed for reasonableness by financial statement preparers who are knowledgeable of the business, it probably is adequate to include the item on the disclosure checklist with responsibility assigned to the real estate function. On the other hand, if there are numerous acquisitions and divestitures during the year and such activity is expected in future years, it may be appropriate to understand and document the process to ensure that it is designed effectively.
- *When a particular disclosure segment has multiple data sources to generate, it may be necessary to understand and document the process by which the required data is obtained, compiled and organized. The supplementary schedules might be an example of this situation.* The MD&A might require specific calculations, but many of those can be referenced to the financial statements. Operating data comes from operating information, and the source of that information and its reliability should be understood due to the criticality of ensuring the MD&A disclosures are reliable. A good portion of the MD&A is variance explanation from operations. Accordingly, the MD&A should be supported by operating reports and have direct input and review by operating management.

- ***Decide how the company's collective knowledge will be captured and summarized for certifying officers to ensure timely action and disclosure.*** At least initially, a simple process should be in place to facilitate the flow of material information. This could be nothing more than formalizing existing disclosure processes. For the company requiring monthly reporting packages, as illustrated earlier, the disclosure committee forwards each unit's package to the CEO and CFO – the certifying officers – who review them as part of their ongoing evaluation process. Some companies use regular conference calls with business-unit managers to identify new risks and emerging issues requiring attention.

The purpose of providing the above examples is to illustrate what the SEC has in mind when referring to disclosure controls and procedures. In providing these examples, we acknowledge that many of them are not new.

35. How should management design the disclosure controls and procedures so that the disclosure process will not become simply a ritual?

During the initial filings, the disclosure process is likely to receive significant attention by everyone involved. However, over time, priorities change. The business undergoes change. The managers and key employees involved in the disclosure process change.

Processes are needed to monitor change and assess risk to continuously improve the disclosure process and keep it fresh. The disclosure committee should determine that such processes are in place and are operating effectively. Following are examples of steps management should take:

- ***Monitor change, both externally and internally.*** Changes in the environment and in the company's operations require special emphasis to evaluate their impact on the business, the financial statements and the required disclosures. Examples of changes requiring evaluation include mergers and acquisitions, divestitures, new innovative business practices, new systems, changes in personnel, significant market declines, and changes in laws and regulations. The disclosure committee, or an equivalent group of executives, should be designated with the responsibility to monitor change for purposes of identifying material information requiring disclosure. As noted in Questions 187, 195 and 196, a change-recognition process is a critical element of an ongoing Section 404 compliance structure.
- ***Identify the primary business risks associated with company operations and the critical information essential for measuring, monitoring and reporting on each risk; in view of such risks, evaluate current disclosures to determine whether additional information is needed.*** Senior management and the board should concur as to the company's primary business risks, the appetite or tolerance for such risks, and the plans for managing and monitoring the company's exposure to losses and potential for profits from such risks. As management recommends to the board specific strategies and plans for action, they should articulate the risks inherent in such strategies and plans, and evaluate the consistency of their recommendations with their expressed risk tolerance. The board, in turn, must understand and agree with management's assessment of and tolerance for risk and the impact of their recommendations on the organization's risk profile. An explicit understanding of the organization's risks and the uncertainties inherent in its performance goals will assist management in identifying material information for disclosure in public reports. Management's assessment of business risk and the related impact on disclosure in public reports should be continuously updated over time. Our point of view is that an enterprise risk management capability would facilitate an organization's disclosure process and risk management.
- ***Design a process to identify operating and other changes that impact the effectiveness of established controls.*** Change is inevitable. For example, operational risks, new related party transactions, new litigation and other contingencies, strategic risks, regulatory developments, credit and market risks, and risks to reputation and brand image can emerge that present issues requiring disclosure. Changes in the external environment (e.g., changes in the economy, in interest rates, etc.) can affect the determination of estimates and assumptions inherent in the financial statements. Management should put in place an infrastructure that on a timely basis identifies issues requiring action and possible disclosure. Management should satisfy itself that the company's disclosure controls and procedures are effective in addressing new issues and developments as they arise. See Question 187 for a discussion of the key elements of an ongoing Section 404 compliance structure, which enhances the quality of a company's disclosure controls and procedures.

36. What should the certifying officers do when evaluating disclosure controls and procedures on a quarterly basis?

When the SEC released its rules on Section 302 in 2002, it required quarterly evaluations of disclosure controls and procedures and disclosure of the conclusions regarding the effectiveness of those controls and procedures.

These rules have remained unchanged since they were issued. Thus, the evaluation and disclosure requirements applicable to disclosure controls and procedures continue to remain in force, including the elements of internal control over financial reporting that are "subsumed" within disclosure controls and procedures.

With respect to evaluations of disclosure controls and procedures, companies must evaluate the effectiveness of those controls and procedures on a quarterly basis. The SEC points out:

> While the evaluation is of effectiveness overall, a company's management has the ability to make judgments (and it is responsible for its judgments) that evaluations, particularly quarterly evaluations, should focus on developments since the most recent evaluation, areas of weakness, or continuing concern or other aspects of disclosure controls and procedures that merit attention.

The SEC's message is one of flexibility in approach whereby management may choose to design the quarterly evaluation process in a manner that focuses on identifying control deficiencies, the impact of changes from prior periods and other areas of concern representing changes from previously issued annual or quarterly reports. Thus, management may decide that a complete evaluation is not needed every quarter to satisfy the spirit of the certification requirements and that the certification process should focus on change. Even though there is an expectation that an evaluation of overall effectiveness is conducted each quarter, the emphasis should be on the impact of changes in controls and procedures and in their performance.

Disclosure controls and procedures are the means by which the certifying officers assume responsibility to ensure they (or someone they designate) receive in a timely manner the reliable material financial and nonfinancial information needed to enable them to certify to the fairness of public reports. We believe that disclosure controls and procedures should evolve over time until a process-based "chain of accountability" is in place. This begins with understanding and documenting key disclosure processes, risks and controls. *Efforts to comply with Section 404 facilitate this understanding and documentation because such efforts must focus on the underlying financial reporting processes and controls.*

Under the direction of the certifying officers, the company should:

- ***Identify critical disclosure processes that require immediate evaluation to ensure the underlying controls are adequately designed and operating effectively.*** Based on a risk assessment, management should identify critical disclosure areas requiring attention. For example, the processes for stock option grants and exercises might warrant attention, given experiences in 2006 and 2007. The processes for accumulating the expanded executive compensation disclosures – including the participation of executives, directors, significant shareholders and other related persons in financial transactions and relationships with the company – may warrant attention because of the SEC's new disclosure rules. Greater attention is being paid to these disclosures by investors, media and regulators. Areas of known weakness might also receive appropriate attention. For each of the critical processes selected by management as requiring immediate assessment, a diagnostic should be performed of the controls and procedures to ensure they are adequately designed, effectively operating and sufficiently documented to satisfy compliance with the rules. For example, the financial reporting process might be reviewed because of the nonroutine activities that take place in that process.
- ***Document the critical disclosure processes, including risks and control points.*** Identify gaps and action plans to close the gaps. The inputs, outputs, activities, policies, systems and metrics of the key disclosure processes should be documented over time, depending on management's assessment of criticality. As each critical process is documented, the risks and key control points are identified. These control points provide the basis for conducting an evaluation of controls.
- ***Remedy control deficiencies.*** Any control deficiencies should be considered for disclosure and certification purposes, and addressed as soon as possible.
- ***Align the organization with the objective of fair reporting.*** The disclosure controls and procedures infrastructure should consider the organization's performance expectations, incentive compensation programs and other behavior-influencing practices that may impact fair reporting. Reporting needs to be an integral part of

every manager's job. For some organizations, this will require a change in mindset. The disclosure committee could assume the responsibility of determining whether there are any aspects of the company's culture that could frustrate the goal of fair reporting. For example, if a significant component of the CFO's and accounting management's compensation is linked to profits, that approach should be examined to ensure there is adequate balance given to quality reporting.

- ***Align process owner monitoring and internal audit plans with evaluation requirements.*** Identified control points provide the basis for developing appropriate metrics and for focusing process-owner monitoring. They also provide a business context for focusing internal audit plans. The results of process owner monitoring and internal audits should be reported to the disclosure committee for review.
- ***Document the evaluation process.*** In connection with its internal control rules, the SEC points out that each registrant should maintain evidential matter in reasonable detail, including documentation, to provide a basis for management's conclusions. It is appropriate that the evaluation of disclosure controls and procedures should generate similar documentation, all of which should be maintained for subsequent review.

The certifying officers should create a checklist summarizing the key steps that must be taken each quarter. The steps on the checklist should include actions that need to be completed before the designated officers sign the certification. For example, do the certifying officers:

- Carefully read the report and ask relevant questions to understand its contents?
- Evaluate the internal control over financial reporting to ensure financial disclosures are complete and accurate?
- Evaluate the internal processes used to prepare periodic public reports, including the related disclosures?
- Discuss with key personnel involved in the process whether there are any unresolved issues with respect to disclosures or financial reporting?
- Take a close look at areas where there is a reasonable possibility for material errors or omissions, e.g., past problem areas, revenue recognition, significant accounting estimates, asset impairments, loss contingencies, related party issues, significant industry problem areas and off-balance sheet issues? For example, approximately half of the SEC's enforcement actions involve revenue-recognition issues.
- Keep a close eye on areas where potential control deficiencies may exist? For example, certain types of control deficiencies occur most frequently, based on disclosures by public companies. These deficiencies include such areas as inadequate financial personnel, revenue recognition, account reconciliations, segregation of duties and review, monitoring and analysis.
- Discuss with the independent public accountants whether they have any concerns that could increase the company's compliance risks?
- Discuss the company's disclosure controls and procedures with the audit committee to confirm it is satisfied with them?
- Follow up on open areas, e.g., disagreements with the independent public accountants, prior SEC comments, concerns of the audit committee, violations of the code of conduct, significant audit or other adjustments, issues raised by whistleblowers, instances or allegations of fraud, questions from analysts, and unresolved issues in the internal audit report?

37. How is internal control over financial reporting distinguished from disclosure controls and procedures?

Disclosure controls and procedures will include those components of internal control over financial reporting that provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles. Thus, for the most part, internal control over financial reporting is a subset of disclosure controls and procedures. In its final rules on Section 404, the SEC states there is "significant overlap" between these two types of controls and procedures. The SEC

differentiates disclosure controls and procedures from internal control over financial reporting based on its interpretation of congressional intent: to have senior officers certify that required material nonfinancial information, as well as financial information, is included in an issuer's quarterly and annual reports. The SEC intends for the concept of disclosure controls and procedures to cover a broader range of nonfinancial information than is covered by an issuer's internal control over financial reporting. Likewise, the concept of internal control over financial reporting covers items that do not directly relate to disclosure (e.g., reasonable assurance that receipts and expenditures are made only in accordance with management and board authorization).

The following summary contrasts internal control over financial reporting with disclosure controls and procedures:

	Required by:	
Management Must	**Section 404** Internal Control over Financial Reporting	**Section 302** Disclosure Controls and Procedures
Conclude as to integrity of public information	Financial statements	All material financial and nonfinancial information included in public reports, including F/S
Timely assess controls and procedures	Annually	Quarterly
Conduct review as of	Year-end	Quarter- or year-end
Document evaluations for auditor to attest	Annually	None
Evaluate impact of change	Quarterly	Quarterly
Comply with Sections 404 and 302 through common and interfacing processes	Subset of disclosure controls and procedures	Includes internal control over financial reporting
Report to the public	Internal control report	Officers' certification

38. Are there examples of internal control over financial reporting that fall outside the realm of disclosure controls and procedures?

To the extent that internal control over financial reporting impacts public disclosure, a company's disclosure controls and procedures are clearly inclusive of such internal controls because disclosure controls apply to all material information to be included in public reports, both within and outside the financial statements. Given the SEC's broad view of disclosure, as articulated in its August 29, 2002, release, it is difficult to identify any internal control over financial reporting that would not be viewed as a subset of disclosure controls and procedures so long as such controls are relevant to the production of financial statements, which are a part of public reports. In our view, when the scope of internal controls and procedures is limited to objectives relating to reliability of financial reporting (i.e., they do NOT apply to objectives relating to operational efficiency and effectiveness or to compliance with other applicable laws and regulations), such controls and procedures are generally viewed as a subset of disclosure controls and procedures.

In designing their disclosure controls and procedures, companies can be expected to make judgments regarding the processes on which they will rely to meet applicable requirements. Thus, some companies might design their disclosure controls and procedures so that certain components of internal control over financial reporting pertaining to the safeguarding of assets are not included. For example, a company might have developed internal control over financial reporting that includes, as a component of safeguarding of assets, dual signature requirements or limitations on signature authority on checks. That company could nonetheless determine that this component is not part of its disclosure controls and procedures.

The COSO Internal Control — Integrated Framework

39. What is COSO?

The SEC ruled that the criteria on which management's evaluation is based must be derived from a suitable, recognized control framework that is established by a body or group that has followed due process procedures, including the broad distribution of the framework for public comment. As defined in the Commission's rules, a "suitable framework" must: be free from bias; permit reasonably consistent qualitative and quantitative measurements of a company's internal control; be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal controls are not omitted; and be relevant to an evaluation of internal control over financial reporting. The SEC points out in its rules that the COSO Internal Control – Integrated Framework satisfies this requirement. It acknowledges that frameworks other than COSO that satisfy the intent of the statute without diminishing the benefits to investors may be developed within the United States in the future. Other frameworks in other countries may also meet this requirement, e.g., CoCo, Turnbull, King or other country-specific authoritative frameworks.

COSO stands for "Committee of Sponsoring Organizations" and is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance. COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative often referred to as the Treadway Commission. The Commission studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

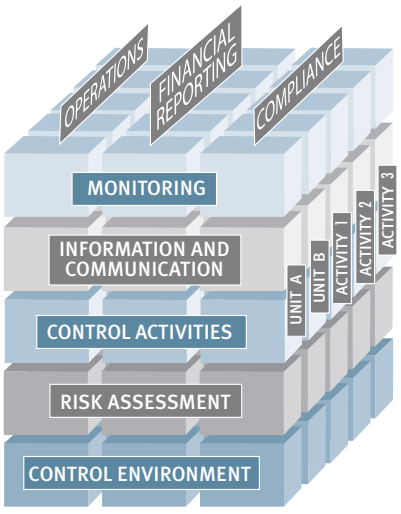
The sponsoring organizations are the American Institute of Certified Public Accountants (AICPA), The Institute of Internal Auditors (IIA), Financial Executives International (FEI), Institute of Management Accountants (IMA) and American Accounting Association (AAA). COSO so far has produced four documents, one in 1992 on the Internal Control – Integrated Framework, one in the mid-1990s on derivatives, one in 2004 on the Enterprise Risk Management – Integrated Framework and the most recent in 2005, which provides guidance to smaller public companies applying the integrated internal controls framework to report on internal control over financial reporting.

40. What is the Internal Control – Integrated Framework?

The COSO Internal Control – Integrated Framework defines internal control as a "process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations." The Integrated Framework uses three dimensions, illustrated in the adjacent cube, that provide management with criteria by which to evaluate internal controls.

The first dimension is objectives. Internal controls are designed to provide reasonable assurance that objectives are achieved in the following categories: effectiveness and efficiency of operations (including safeguarding of assets), reliability of financial reporting, and compliance with applicable laws and regulations (left to right, across the top of the cube).

Three Dimensions of COSO Integrated Framework



Source: COSO Internal Control – Integrated Framework

The second dimension required by COSO is an entity-level focus and an activity-level focus (front to back, across the right side of the cube). Internal controls must be evaluated at two levels: at the entity level, and at the activity or process level.

The third dimension includes the five components of internal controls (bottom to top, on the face of the cube):

(1) ***Control environment*** – Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

(2) ***Risk assessment*** – This component is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks should be managed.

(3) ***Control activities*** – Includes the policies and procedures that help ensure management directives are carried out.

(4) ***Information and communication*** – This component consists of processes and systems that support the identification, capture and exchange of information in a form and time frame that enable people to carry out their responsibilities.

(5) ***Monitoring*** – Consists of the processes that assess the quality of internal control performance over time.

These five components provide the framework for effective internal control over financial reporting and, in similar fashion, provide a framework more generally for disclosure controls and procedures. They provide the context for evaluating internal control over financial reporting.

These three dimensions represent the Integrated Framework. The framework works in the following manner: For any given objective, such as reliability of financial reporting, management must evaluate the five components of internal control at both the entity level and at the activity (or process) level.

Management must decide on a control framework on which to base its assertions regarding – and its evaluation of – the effectiveness of internal control. We recommend the COSO framework. It meets the test of an authoritative framework as it is widely accepted and reasonably intuitive. The SEC's rules and interpretive guidance for Section 404 refer to the COSO framework and define "internal control over financial reporting" consistently with the framework. The U.S. professional auditing literature historically has embraced the COSO framework since it was issued. When the PCAOB issued, and subsequently revised, its auditing standard for an audit of the effectiveness of internal control over financial reporting, the Board reaffirmed the COSO report as providing "a suitable and available framework for purposes of management's assessment" in accordance with Section 404. Banks complying with FDICIA (see Questions 6 and 7) have also used COSO.

If management decides not to use COSO, an alternative framework must be selected. Any framework management chooses to use must meet the SEC's criteria. If a company chooses to use a non-COSO framework, we suggest that management "map" the framework to COSO to demonstrate coverage of the key COSO components for the benefit of the external auditor and other parties who may challenge the use of the framework. For example, in its interpretive guidance to management, the SEC states the following:

> [B]oth the COSO framework and the Turnbull Report state that determining whether a system of internal control is effective is a subjective judgment resulting from an assessment of whether the five components [as discussed above] … are present and functioning effectively. Although CoCo states that an assessment of effectiveness should be made against twenty specific criteria, it acknowledges that the criteria can be regrouped into the five-component structure of COSO.

41. How is the COSO framework applied at the entity level during the Section 404 assessment process?

COSO is applied at two levels – the entity level and the activity or process level. At the entity level, each of the five components is broken down into attributes to support the assessment. "Attributes" define the nature of a component. For example, as illustrated in the accompanying graphic, the control environment component is

further defined using seven attributes. For each attribute, COSO provides appropriate "points of focus" representing some of the more important issues relevant to the attribute. Not all points of focus are necessarily relevant to every entity. Additional points of focus may be relevant to some entities. COSO recommends that, for purposes of a controls evaluation, every organization should tailor the points of focus to fit the organization's facts and circumstances; e.g., smaller companies with management closer to the front lines and more knowledgeable of business realities will often have a different approach than larger companies with several layers of management and multiple operating units.

Both the SEC and PCAOB refer to these controls as "entity-level controls." These are the controls that management relies on to establish the appropriate "tone at the top" relative to financial reporting. They often have a pervasive or indirect impact on the effectiveness of controls at the process, transaction or application level. At the entity level, management must address the various attributes COSO provides for each component. The following illustration shows the various attributes provided for each of the five components and illustrates points of focus for one attribute – human resource policies and procedures:

Illustrating COSO at the Entity Level

COSO Components	Attributes
Risk Assessment	• Entitywide objectives • Activity-level objectives • Risk identification and assessment • Managing change
Control Environment	• Integrity and ethical values • Commitment to competence • Board of directors or audit committee • Management's philosophy and operating style • Assignment of authority and responsibility • *HUMAN RESOURCE POLICIES AND PRACTICES* →
Information and Communication	• External and internal information is identified, captured, processed and reported • Effective communication down, across and up the organization
Control Activities	• Policies, procedures and actions to address risks to achievement of stated objectives
Monitoring	• Ongoing monitoring • Separate evaluations • Reporting deficiencies

Points of Focus

- Are there policies, procedures and effective processes for hiring, compensating, promoting, training and terminating employees?
- Are employees made aware of their roles, responsibilities, authorities and performance expectations?
- Are everyone's control-related responsibilities clearly articulated?
- Are employees accountable for results and are performance expectations reinforced with appropriate performance measures?
- Are employee retention and promotion criteria clearly defined, and is the performance evaluation process effective?
- Does management take appropriate remedial action in response to departures from approved policies and procedures?
- Is the established code of conduct reinforced and disciplinary action taken when warranted?
- Are the background and experience of prospective employees checked and references obtained?

To continue with this illustration, human resource policies and procedures are designed to recruit and retain competent people who can achieve the entity's stated objectives and execute its strategies successfully. The points of focus provided above for "human resource policies and practices" are illustrative and are not intended as a comprehensive list. As noted earlier, management may tailor them to the organization; i.e., management may add, delete and modify points of focus. Management may also add more specific granular questions or issues addressing each point of focus. For example, the first illustrative point of focus above is, "Are there policies, procedures and effective processes for hiring, compensating, promoting, training and terminating employees?" For this point of focus, more granular criteria (not intended as all-inclusive) might include:

- Personnel policies are effectively communicated for (a) recruiting or developing competent people with integrity, and (b) encouraging and incenting them to support an effective system of internal controls.
- Existing personnel procedures and processes for recruiting or developing competent people with integrity are in accordance with stated policies and are effectively executed.
- Existing personnel procedures and processes for encouraging and incenting people to support an effective system of internal controls are in accordance with stated policies and are effectively executed.

- The emphasis on recruiting the right people and training them to do the right things is appropriate.
- Management periodically communicates expectations about the desired characteristics of the people targeted for hiring.
- Personnel policies are effectively communicated for counseling people who are experiencing difficulty on the job and for terminating and exit-conferencing people who are not performing to standards.
- Existing procedures and processes for counseling people who are experiencing difficulty on the job and for terminating and exit-conferencing people are in accordance with stated policies and are effectively executed.

To summarize the previous illustration as to how the COSO framework is applied at the entity level:

- For each of the five components, COSO provides several attributes.
- For each attribute, COSO provides points of focus.
- For each point of focus, more granular criteria may be developed to support the assessment.

With respect to conducting the assessment at the entity level, there are several points to keep in mind:

- COSO recommends the following:
  - Responses should be documented for each point of focus rather than for the more granular criteria. Responses should be based on management's conclusion that the stated policies, processes, competent people, reports, methodologies and systems actually exist and are effectively functioning.
  - A response should generally not be a "yes" or a "no" answer, but rather should address specifically what the entity does to address the point of focus.
- Management should conclude as to the effectiveness of internal controls with respect to each attribute supporting a given component of internal control. The responses providing information with respect to the points of focus, as described on the previous page, support management's conclusions on the attributes. To illustrate, management should conclude on each of the seven attributes of the control environment, including human resource policies and practices.
- An overall conclusion should be reached with respect to each COSO component. This overall conclusion is supported by the collective weight of the individual conclusions on each of the relevant attributes. Thus, management formulates a conclusion as to the effectiveness of the control environment. This conclusion is supported by a conclusion on each of the seven attributes of the control environment.
- A response of "ineffective" or "requires improvement" for a given attribute does not necessarily warrant a conclusion that the related component is ineffective at the entity level. There may be compensating controls in other areas (see Question 107).
- A response of "ineffective" or "requires improvement" for a given attribute should lead management to evaluate whether improvements are needed in internal controls and to take appropriate action to close any gaps. If management believes there is an absence of one or more key controls that, if not compensated for in other areas, increases the likelihood that there are significant control risks (meaning an increased risk of control failure), action should be taken quickly. Further, such conditions are very likely significant deficiencies that should be communicated to the audit committee and independent public accountant.

Depending on how the reporting entity (the "issuer" for SEC reporting purposes) divides into control units (see Questions 54 and 55), the stated attributes and points of focus may apply to one unit but not to another. *All assessments of the control environment for the various control units must be taken into account for management to reach an overall enterprisewide conclusion with respect to the control environment.*

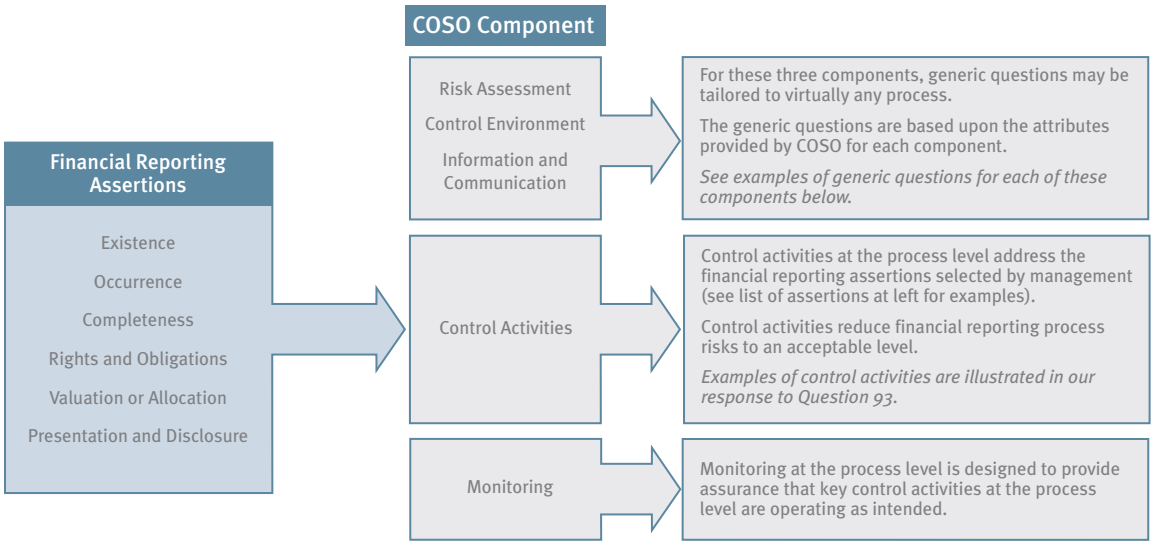
For example, consider a reporting entity with several highly autonomous operating units included in its consolidated statements. Assume that each of the operating units represents a control unit along with the reporting entity. For purposes of assessing the control environment:

- The reporting entity may set the tone at the top with a corporatewide code of ethics, and oversee the various compliance and enforcement activities (e.g., the "integrity and ethical values" attribute). The board of directors and audit committee meet at the reporting entity level (another separate attribute of the control environment). The reporting entity establishes the organizational structure (another separate attribute), provides overall HR policies (part of the "human resource policies and practices" attribute), etc.
- The various operating units functioning as control units address other attributes of the control environment, such as commitment to competence, management's operating style, assignment of authority and responsibility, etc.
- The assessments for all of these units are taken into account in formulating a conclusion for the entity as a whole. The overall assessment summarizes the impact of the various entity-level assessments.

In summary, the extent of top management's control over the consolidated reporting entity, the diversity in the nature and types of operations and business units, the unique risks inherent in those operations and business units, and other factors impact the project team's approach to assessing the entity-level controls.

42. How is the COSO framework applied at the activity or process level during the Section 404 assessment process?

Just as it is applied at the entity level, the COSO framework is also applied at the activity or process level. When assessing the "design effectiveness" of process-level controls over financial reporting and documenting that assessment, the five COSO components are considered, as shown in the following illustration:



From a practical standpoint, when performing a review of internal control over financial reporting, most of the attention at the process level focuses on control activities and the monitoring of those activities. Once the assertions related to reliability of financial reporting are generally understood and documented (see Questions 71 and 72 for two illustrative groups of financial reporting assertions), control activities most directly address those assertions. Monitoring provides assurances that the control activities are performing as intended.

- ***Control Activities*** are an integral part of making business processes work. Embedded within the processes, they provide assurance that the processes are preventing and detecting on a timely basis errors and fraud as close as possible to the source, providing assurance that relevant assertions are met. Control activities at the

process level are the internal controls that specifically address the financial reporting assertions or risks (see Questions 71 and 72 for examples). Control activities should be in place within the process to reduce "financial reporting assertion risks" to an acceptable level. The financial reporting assertions and the risks ("what can go wrong") to achieving those assertions provide a context for evaluating the design effectiveness of control activities at the process level.

- ***Monitoring*** includes the activities focused on evaluating the performance of control activities and the results of the process to ensure they are in accordance with the entity's objectives and established performance criteria for the process. Monitoring consists of both ongoing monitoring and separate evaluations.

Control Activities

The control activities in place should provide reasonable assurance that management's financial reporting objectives or assertions are met. It is important to note that the SEC's interpretive guidance states that, through a top-down, risk-based approach, management focuses on those controls that are needed to prevent or detect a material misstatement in the financial statements. In this regard, management may identify controls for a financial reporting element that are preventive, detective or a combination of both. Management is not required to identify the entire population of controls, just those controls that adequately address the risk of a material misstatement. To illustrate, if a particular risk is addressed by an entity-level control or by a few controls within a process, the SEC's interpretive guidance states that management is not required to identify and document all controls within the process.

The SEC states that "[e]ntity-level controls may be designed to operate at the process, application, transaction or account level and at a level of precision that would adequately prevent or detect on a timely basis misstatements in one or more financial reporting elements that could result in a material misstatement of the financial statements." The Commission also states that other entity-level controls comprise the control environment (e.g., the "tone at the top" and entitywide programs, such as codes of conduct and fraud prevention) and "have an important, but indirect, effect on the likelihood that a misstatement will be prevented or detected on a timely basis." Therefore, the so-called direct entity-level controls may be considered a "control activity" because they operate at a sufficient level of precision to support a conclusion that they are effective in preventing or detecting material misstatements and reduce financial reporting assertion risk to an acceptable level. The so-called indirect controls – those with an indirect effect on the likelihood a misstatement will be detected or prevented – are also important, because their absence increases the risk of a control failure. The existence of direct entity-level controls, along with controls that monitor the effectiveness of other controls, allow the evaluator to reduce the scope of testing process-level controls.

The distinction between direct and indirect entity-level controls is important from the standpoint of testing process-level controls. An entity-level control to monitor the results of operations may be designed to detect potential misstatements and investigate whether a breakdown in lower-level controls occurred. In these instances the SEC states: "If the amount of potential misstatement that could exist before being detected by the monitoring control is too high, then the control may not adequately address the financial reporting risks of a financial reporting element." Therefore, the control is indirect in nature.

Once the key control activities are identified, management must evaluate their design and operational effectiveness:

- The assessment of design effectiveness addresses whether the control activities, as designed, provide reasonable assurance that identified risks are mitigated and the stated financial reporting assertions are achieved.
- The validation of operational effectiveness addresses whether the control activities are functioning as intended (i.e., are they performing as designed?).

There are many examples of control activities applied at the process level. Illustrative examples of control activities are provided in our response to Question 93.

Monitoring Activities

At the process level, monitoring activities address the effectiveness of the key control activities built into the process, as well as the effectiveness of the control environment, risk assessment and information/communication components. Monitoring activities consist of both ongoing monitoring and separate evaluations. Ongoing monitoring arises from regular management and supervisory activities, comparisons, reconciliations, and other formal and informal mechanisms in the ordinary course of business that provide continuous feedback as to the effectiveness of internal controls. Examples of ongoing monitoring activities include:

- Day-to-day monitoring by supervisors and process owners
- Formal processes for following up on information received from external sources to improve internal processes, e.g., customer complaints about billings result in correction of deficiencies in the billing system
- Comparisons of physical assets with recorded balances, e.g., physical inventories result in book-to-physical adjustments
- Active follow-up on feedback received through planning meetings, employee suggestions systems, training sessions, etc.
- Periodic reports, e.g., exception and "near misses" reports, audit reports, limit violation reports and status of improvement initiatives reports
- Analytics built into financial systems to handle data correctly or "kick out" data failing to meet selected criteria

Senior and unit management, process owners and internal audit periodically take a fresh look at the components of internal controls (including the ongoing monitoring procedures) to evaluate their effectiveness. These initiatives are called "separate evaluations." Internal audit reviews are a common example.

Monitoring requires protocols and processes for capturing, reporting and following up on deficiencies to ensure all significant deficiencies, or deficiencies that could eventually become significant, are considered and resolved in a timely manner.

The preceding discussion has focused on the two COSO components that are most prevalent at the activity or process level – control activities and monitoring. With respect to the risk assessment, control environment and information/communication COSO components, generic questions may be developed for application at the activity or process level to facilitate evaluation of those components at that level. To illustrate, following are examples of generic questions applicable to each of these three components that may be customized to virtually any significant process.

Risk Assessment

Business processes are exposed to risk from external and internal sources. These risks must be assessed in terms of their impact on the achievement of process objectives. Process owners must either establish a process or be part of an established process to effectively identify and evaluate the risks in the external and internal environment that present threats to the achievement of process objectives.

Following are appropriate questions pertaining to the risk assessment component at the activity or process level:

- Has the process owner established process objectives that are consistent with the overall objectives established by the reporting entity or unit management?
- Do the process objectives provide clarity and sufficient granularity as to what the process is designed to achieve? Are the objectives consistent (and not in conflict) with the objectives of other processes? Has management been involved in setting the process objectives, particularly those that are critical to the success of the reporting entity or unit?
- Does the process owner have adequate resources to achieve the stated objectives?

- Does the process owner have an effective process to: (a) identify significant risks arising from external and internal sources to the achievement of key process objectives; (b) assess the significance of the risks and the likelihood of occurrence; and (c) evaluate alternative actions for reducing those risks to an acceptable level?
- Does the process owner continuously anticipate, identify and react to routine events and changing circumstances and conditions that could affect the achievement of process objectives?
- Are process activities dependent on the integrity and availability of information identified, captured, processed and reported? If so, has the process owner evaluated the risks related to the security, integrity and availability of that information?

Control Environment

Process owners must establish an effective control environment to provide discipline, structure and a strong foundation for control within the process. The control environment consists of the control owners and other personnel responsible for executing the process and the environment in which they operate. It sets the tone for the effective functioning of the process, influencing the control consciousness of everyone involved in making the process work. It is the foundation for all other components of internal control within the process.

Following are appropriate questions pertaining to the control environment at the activity or process level:

- Does the process owner have an effective and understandable structure that (a) effectively facilitates monitoring, and (b) enables the vertical and horizontal communication and information flows necessary to achieve process objectives?
- Are the process owner's approaches for articulating and clarifying roles, responsibilities, authorities and accountabilities in accordance with the established policies of the entity or unit? Is there effective communication of appropriate policies, performance expectations and established accountability to each individual responsible for important process activities?
- Are the process owner's policies and practices for recruiting and retaining competent people and developing competence clearly defined, in support of process objectives and in accordance with the established human resource policies of the entity or unit?
- Does the process owner maintain a positive operating style in terms of accepting risks, facilitating interaction among managers and employees, and demonstrating a supportive attitude (as evidenced by appropriate action) toward financial reporting consistent with the tone set by senior management?
- Has the process owner conveyed a clear message to employees, through his or her actions and communications, that the integrity and ethical values established by the organization are an integral part of the manner in which the process is executed, and cannot be compromised?
- Has the process owner documented and communicated policies and procedures regarding information technology managed by control owners and other employees in areas including the following:
  - Control over access to sensitive and critical applications and data files supporting the process (including practices to minimize the potential for introducing computer viruses into systems supporting the process)?
  - Authorization, documentation, testing and controlled implementation of new applications and application changes affecting the process?
  - Appropriate backup and recovery procedures for all critical application programs and data files supporting the process?

Information/Communication

Relevant and reliable information is essential to understanding what is really happening in the external environment and in the entity's business processes. The right performance measures and effective communication processes are essential to ensure that important messages relating to internal control are communicated and managed within a process.

Following are appropriate questions pertaining to the information/communication component at the activity or process level:

- Is the process owner committed to the development of the necessary information systems to ensure all pertinent information is captured as close as possible to the source, accurately recorded and processed, and reported in a timely manner for analysis, evaluation and use in financial reporting?
- Is the process owner able to obtain adequate information – with support from executive management – from relevant external sources to assess the impact of environmental changes on the process, its performance and the information about that performance? For example, is there information about customer needs and wants; the competitive, technological and regulatory environments; and general economic and industry trends and conditions?
- Does the process owner have access to information gathered by the organization on changing conditions and trends affecting the performance of the process?
- Does the process owner determine that relevant and timely information is provided to control owners and other process personnel in sufficient detail to enable them to effectively discharge their responsibilities?
- Does the process owner effectively (a) communicate process objectives to control owners and other process personnel, (b) facilitate communication within the process and with personnel representing other entity and unit processes and functions, and (c) support a process for control owners and other process personnel to communicate upward issues regarding process performance and control?

43. Must the Section 404 compliance team address each of the five COSO elements in each critical process affecting a significant financial reporting element?

At the process level, most of the controls will consist of control activities and monitoring. The remaining three COSO components – control environment, risk assessment and information/communication – can be addressed by tailoring relevant questions listed in Question 42 to the appropriate processes. There are a variety of ways these three components can be documented at the process level. Some auditors have insisted that all five components be addressed for each critical process. Others point out that the risk assessment component is generally applied at the entity and business-unit levels. Elements of the control environment and information/communication clearly apply to the processes because process owners set the tone for their subordinates, and must have information with which to manage the process and communicate with others on important topics. Monitoring at the process level often includes ongoing supervisory activities by process owners, including review and follow-up on exceptions and issues identified through reports, reconciliations, comparisons, confirmations and other sources of process performance information (see Question 42 for other examples). Monitoring also includes separate evaluations by internal auditors and others.

44. Since the COSO framework includes internal controls over operational effectiveness and efficiency and over compliance with applicable laws and regulations, to what extent must management evaluate these controls to support the internal control report?

Section 404 does not require management to evaluate internal controls over operations, except to the extent that such controls may overlap with financial controls (see illustration). For example, defining processes, documenting procedures, analyzing root causes and supervising activities are examples of operational controls that may also be relevant to financial reporting activities.

Some Control Processes Address Multiple Objectives

There are potentially strong sources of value extending beyond mere compliance with Section 404. Sections 302 and 404 of Sarbanes-Oxley provide the "launching pad" to improve processes and the internal control structure and enhance entity-level and process-level monitoring of financial reporting processes. Because Sarbanes-Oxley forces public companies to assess weaknesses in their business processes, including their controls over processing information, the line between reliable financial reporting and operational effectiveness and efficiency can be a blurry one. Financial reporting processes for many companies are often dependent on people and manually intensive detective controls and are sometimes inadequately defined. Because this dependency leads to a focus on detecting and correcting errors leading to costly rework, it provides a significant opportunity to "build in" (versus "inspect in") quality, optimize costs and compress time within the organization's processes while simultaneously reducing its financial reporting risks. Compressing time in the close process can be especially important due to the accelerated SEC filing deadlines for Forms 10-K and 10-Q of large accelerated filers and accelerated filers (see Question 242). In today's environment, it is impossible to improve cost, quality and time process performance without also automating controls and improving the balance of preventive and detective controls.

With respect to compliance with laws and regulations, financial reports issued to the public are governed by SEC rules and regulations with which companies must comply. Thus, some compliance controls may be germane to financial reporting, e.g., monitor the SEC regulatory environment, assess impact of changes, clearly articulate company reporting policies and communicate such policies throughout the organization. In the final Section 404 rule, the SEC said that Section 404, in general, does not cover compliance with laws and regulations. Notwithstanding the SEC's statement, if a company is NOT complying with specific laws and regulations, the question arises as to whether that noncompliance must be identified and assessed by the company's disclosure controls to determine whether there is a possible impact on the financial statements or on other disclosures in the company's current or periodic public reports.

Management always has the option to expand the review of its processes, risks and controls to other categories of objectives, e.g., operational effectiveness and efficiency, and compliance with applicable laws and regulations. If management chooses to do so, however, that action is a business decision and not a Sarbanes-Oxley-driven initiative. (See Question 22.)

45. If a company already uses the COSO framework, is there anything more it needs to do to comply with Section 404?

The COSO framework has been available for companies to use since the early 1990s. Many internal audit departments use it in organizing and documenting assessments of internal controls. However, just because the framework has been used by internal auditors or by anyone else does not mean a company is prepared to demonstrate compliance with Section 404. Use of the COSO framework in the past does mean that the documentation available will be more useful and comprehensive for purposes of preparing Section 404 documentation.

46. Will the COSO framework on enterprise risk management affect the Section 404 assessment?

No. When COSO released the Enterprise Risk Management Conceptual Framework and the accompanying Application Techniques in September 2004, it made clear that this framework would not replace the Internal Control – Integrated Framework. The Integrated Framework will continue as a viable and authoritative framework for companies to use when evaluating the effectiveness of internal controls.

Getting Started With Section 404 Compliance

47. How does management get started?

The process of preparing for Section 404 compliance is a significant undertaking for many companies and should be managed as a formal project. Because the project may require improvements in internal controls before the independent public accountant conducts its annual audit, it is imperative to begin soon. Following are three important areas for management to consider when setting the foundation.

Organize the project – In organizing the project, management should identify the appropriate project sponsor. The sponsor should be a senior executive who can assume responsibility for providing overall direction to the project team and for communicating the project to the organization with credibility. One of the certifying officers should fulfill this role, i.e., the CEO or CFO. In addition to the sponsor, management should identify the project team members, their roles and responsibilities, the resources required and the source and funding of those resources, both internal and external. A team leader, such as the chief accounting officer or corporate controller, should also be appointed. Reference is also made to Questions 198 and 200 for discussions of the role of the disclosure committee and the role of the Section 404 compliance project steering committee.

Develop project plan – The project plan results from defining objectives, establishing a critical path, setting key success factors, defining milestones and checkpoints, and identifying external advisors. The project timeline should be considered carefully to ensure there is adequate time to perform all project tasks, and provide sufficient time for process owners to close any control gaps and for the independent auditor to perform the attestation work. The more complex the company, the more time the auditor will need to complete the attestation process. For many accelerated filers, the plan called for the auditor to begin the audit by sometime during the third quarter. For example, the auditors have requested management to complete the documentation, assessment and validation of controls by six months prior to year-end. In instances involving larger and more complex companies, the auditor requested an even earlier deadline to begin reviewing the controls documentation and assessment of controls design effectiveness. Regardless of the specific deadline agreed to with the auditor, management must back up from that date for planning purposes and allow for sufficient time and resources to complete the project. Due to the scarcity of resources, management will want to do everything possible to avoid missing the deadline because audit firms may have limited capacity to access and organize resources to accommodate significant delays. The project plan must allow for such tasks as sizing up the current

state, scoping the controls assessment, preparing documentation, assessing controls design, validating controls operation and closing control gaps.

Agree on project approach and reporting requirements – Obtaining agreement up front from management and the external and internal auditor on the approach and the reporting requirements is critical to the project's success. For example:

- Agree on a common language of financial reporting risks or assertions to provide a context for evaluating internal controls. (See Questions 71 and 72 for examples of common language of risks or assertions.)
- Decide on a useful schematic as a basis for decomposing the business into its core and supporting processes. We have found a process classification scheme to be a useful tool. Define other useful frameworks to support the project. (See Questions 66 and 67 for discussion about selecting relevant processes.)
- Set criteria for making important scope decisions, e.g., key financial reporting elements, the type and depth of process documentation, and the depth of management's assessment of controls design and operating effectiveness. (See Question 51.)
- Identify documentation and assessment methodology to support management's assertions on internal control, and provide a basis for the independent public accountant to review and test so they can use the work in lieu of performing it themselves. (See Questions 57, 58 and 59.)
- Define the control units by which to break down the organization for purposes of evaluating entity-level and process-level controls. (See Questions 54 and 55.)
- Identify the tools and technology that are needed to support management's controls evaluation process. The methods, tools and technology should be robust enough to ensure consistency across the organization. When evaluating the technology solution, management must consider the collaboration required in the approach, the level of coordination expected and the extent of accessibility of information desired by different individuals. (See Question 60.)
- Agree on the control framework by which management will evaluate effectiveness. (See Question 40.)
- Validate approach and requirements with the independent public accountant to ensure everyone is in agreement. (See Questions 64 and 214.)
- Define the internal communication plan for management to execute during the project. (See Question 56.)

For many large organizations, the Section 404 compliance project requires a project management organization (PMO). The coordination required of multiple tasks by multiple people and teams for multiple locations and units involving multiple processes in which multiple controls are embedded and for which there are multiple action steps to identify, document, assess, test and remediate controls can become too difficult a task for even the most talented and best-intentioned individuals. For that reason, we recommend that companies view initial Section 404 compliance as they would any major project, and dedicate sufficient resources and project management discipline to hold the appropriate personnel accountable and bring the project to successful completion on time and on budget.

48. How is the project team formed?

When forming the project team, management should consider such factors as the extent of controls documentation and the availability of internal resources. If process and controls documentation is already available, the project will take less time and the independent public accountant can begin the attestation process sooner. If internal resources are not available and a substantial amount of work is required to complete the project, it will be necessary to arrange for assistance from an outside party.

Management should organize a balanced project team including (1) a project leader (the corporate controller or chief accounting officer, for example); (2) operating, accounting and auditing representatives from the

company's major business units and foreign operations; (3) corporate executives, such as the chief information officer and chief audit executive; (4) appropriate subject matter experts (e.g., experts in risk and control evaluations for IT, derivatives, reserve estimation and other areas requiring specialized knowledge); and (5) others needed to make key decisions. If a significant amount of work is expected, management should establish a PMO (see Question 47) and support it with a dedicated core of full-time staff. The project team should establish ties to human resources and to the general counsel to obtain timely assistance, advice and input when it is needed. The team will also want to consult with the independent public accountant at periodic checkpoints during the project.

In the initial annual assessment, consideration should be given to forming a steering committee consisting of the certifying officers, operating unit heads or representatives, and leaders of appropriate functions, including the general counsel, human resources, IT and internal audit. This committee evaluates and approves the project plan, approves scoping decisions, reviews major findings and approves the internal control report. The project sponsor, as discussed in Question 199, may chair this committee. The project leader reports to this committee.

49. How should management articulate roles and responsibilities?

Roles and responsibilities must be defined for and acknowledged by the team leader and all team members, whether they are internal or external resources. For example:

- Who makes the key decisions? For example, who makes the decisions in determining the key controls comprising the internal control structure? See Questions 50, 51, 52 and 55 for examples of important matters requiring decision-making.
- Who designs the approach?
- Who builds the supporting tools?
- Who executes the approach?
- Who monitors execution?

Management should assign responsibilities for managing the project, documenting the processes, assessing risks and controls, and facilitating the overall conclusions by management. Roles and responsibilities may be communicated by senior management to the organization, in the project plan, on the company website and in other ways.

50. What should management consider when developing a project plan?

The project plan results from several activities, e.g., defining objectives, establishing a critical path, setting key success factors, defining milestones and checkpoints and identifying external advisors. These activities are discussed further below.

Define objectives – Start by understanding the expectations of key constituencies, e.g., the project sponsor, executive management and the audit committee. Decide whether to limit the controls evaluation to financial reporting or to expand it to other areas, such as operational efficiency and effectiveness, compliance with applicable laws and regulations, risk management objectives or more granular information systems objectives.

Establish critical path – Define key activities needed to accomplish project objectives. Develop a detailed work plan including project activities, tasks, sequencing, scheduling and timeline. The project timeline should be carefully considered to ensure there is adequate time to perform all project tasks, including sufficient time for process owners to correct any control gaps. Finally, there must be sufficient time for the independent public accountant to perform the attestation work. To provide a basis for "blocking and tackling," the project plan must be sufficiently granular so that progress may be reported against schedule on a periodic basis.

Set key success factors – Define key performance indicators and critical success factors and incorporate them into the project plan. Obtain agreement from the project sponsor and executive management. Examples of performance indicators include fulfillment of executive management expectations, completion of designated milestones, completion of work at designated locations, participation of unit managers, participation of process owners, completion of the internal audit plan relating to financial reporting controls, minimal rework of documentation, completion of the project by the date agreed upon with the independent public accountant and timely completion of the attestation process.

Define milestones and checkpoints – Define critical project milestones and assign appropriate checkpoints along the project timeline by which to periodically gauge project progress. Identify the responsible parties with whom to conduct checkpoints, e.g., project sponsor, executive management, the audit committee and the independent public accountant. Use the checkpoints for obtaining review and sign-off, and for obtaining concurrence with the responsible parties.

Identify external advisors – Identify internal resources and capacity for completing the project in accordance with the plan. If internal capacity is insufficient, identify key advisors and define clear expectations of their contributions to the success of the project and beyond.

51. When planning the project, what key scoping decisions should be evaluated, and what criteria should management consider when making these decisions?

The project team must decide on several important scope issues during the project. For example, which financial reporting elements (i.e., the financial statement accounts and disclosures) should the project team review? How much documentation is enough? How much validation and testing are needed? Management must set the criteria for addressing these scoping decisions. In its interpretive guidance, the SEC states that "the extent to which a financial reporting element (1) involves judgment in determining the recorded amounts, (2) is susceptible to fraud, (3) has complex accounting requirements, (4) experiences change in the nature or volume of the underlying transactions, or (5) is sensitive to environmental factors, such as technological and/or economic developments, would generally affect management's judgment of whether a misstatement risk is higher or lower." Other factors to consider when determining key financial reporting elements are summarized below:

- Nature of the financial reporting element and underlying transactions
  - Size and composition of an account or group of related accounts (e.g., revenue and receivables)
  - Volume, size, complexity and homogeneity of the individual transactions processed through a given account or group of related accounts
  - The existence, nature and effect of related party transactions
  - The existence of an ERP system (e.g., SAP, Oracle, PeopleSoft, J.D. Edwards, etc.) or other application system that affects the entire organization or significant parts of the organization
  - The extent of reliance on third parties, including specialists and service organizations
- Potential for material inadvertent or intentional errors
  - Nature and types of errors and omissions that could occur (i.e., "what can go wrong"), including the materiality and significance to investors of possible errors and omissions (see Question 53)
  - Problem areas from prior years that may require attention during the assessment
  - Changes in account characteristics since the prior year
- Other factors
  - Extent of a change in the business and its expected effect

- Risks extending beyond potential material errors or omissions in the financial statements, e.g., illegal acts, conflicts of interest, unauthorized management use of company assets, exposure to losses and likelihood of significant contingent liabilities arising from activities affecting the financial reporting element
- Desire by management to document those processes affecting key accounts that may not be susceptible to a material misstatement and are reasonably predictable. For example, payroll is reasonably predictable for most companies, but it is a significant component of cost of sales and selling, and general and administrative expenses. Management may desire to document the payroll-related processes and controls because of sensitivity to the need to manage and control payroll activities and to ensure compliance with applicable laws and regulations.
- The independent public accountant's expectations and requirements impacting the scope of the external audit

When planning the documentation and assessment methodology, it helps to define the deliverables and design the reports to be issued (i.e., what is the project team's objective?). When planning the assessment, the scoping considerations should include the approach at the entity level and at the process level, the locations at which to conduct assessments, and the relevant systems and components of the IT infrastructure.

With respect to documenting the major transaction flows and processes affecting the key financial reporting elements, the project team must decide the level of process documentation. There are different approaches, including high-level flowcharts, interfunctional process analyses, and procedural and process narratives.

52. How does a company decide the "significant areas" to review for purposes of documenting and evaluating its internal control over financial reporting?

Using the criteria selected and approved by management (see Question 51), the project team prioritizes the financial reporting elements. These elements include the individual accounts or groups of related accounts (e.g., receivables and sales) and footnote disclosures included in the financial statements. Prior to the release of the SEC interpretive guidance to management and the PCAOB's Auditing Standard No. 5, many auditors had articulated the point of view that there is a presumption that ALL line items and captions and ALL footnote disclosures included in published financial statements are significant. Furthermore, when decomposing financial statement line items and captions (as well as disclosures) into specific account balances and components, many auditors also required the use of a quantitative materiality measure (see Question 53) to set a minimum planning threshold. All account balances and components exceeding the defined quantitative threshold (sometimes referred to as "planning materiality") were included within the scope of the audit. In practice, decomposition also has considered accounts or components that are affected by different transaction streams subject to different risks and controls.

Therefore, when applying the now superseded Auditing Standard No. 2, many auditors took the approach that materiality is first applied quantitatively to identify the significant financial reporting elements, and then qualitative factors are applied to identify the elements falling below the quantitative threshold that should also be included in the scope of the audit. Applied in this manner, qualitative considerations add, but do not take away, financial reporting elements within the auditor's scope.

With the release of the SEC's interpretive guidance to management and the PCAOB's Auditing Standard No. 5, it is now clear that qualitative factors can be as important as quantitative thresholds (see Question 51) when determining significant financial reporting elements. In its interpretive guidance, the SEC asserted:

- ***Risk should be assessed based on the standard of providing "reasonable assurance" regarding the reliability of financial reporting*** – "Reasonable assurance" is not "absolute assurance." The SEC uses the "prudent official" test to define "reasonable assurance" and "reasonable detail." (See Question 113.)
- ***Financial reporting elements should be selected based on whether there is a reasonable possibility a material weakness exists*** – According to the SEC, the characteristics of a financial reporting element that management

considers include both the materiality of the financial reporting element and the susceptibility of the underlying account balances, transactions or other supporting information to a material misstatement. This is an inherent risk assessment; i.e., the risk is considered without regard to the effect of controls currently in place. The assessed risk of a financial reporting element generally increases when the given element: (1) involves judgment in determining the recorded amounts; (2) is susceptible to fraud; (3) has complex accounting requirements; (4) experiences significant change; or (5) is subject to environmental factors, such as technological and/or economic developments.

- ***Management should consider the source and likelihood of material misstatements*** – The SEC states that "management [should use] its knowledge and understanding of the business, and its organization, operations, and processes, to consider the sources and potential likelihood of misstatements in financial reporting elements." Thus, the evaluation team should source the risks that could result in a *material* misstatement to the financial statements. Financial reporting risks may arise from such sources as the initiation, authorization, processing and recording of transactions and other adjustments that are reflected in financial reporting elements.
- ***The risk of fraud should be explicitly considered*** – Misstatements include both errors and omissions, whether inadvertent or intentional. Accordingly, management's evaluation of financial reporting risks should consider the vulnerability of the entity to fraud, and whether the fraud risk might result in a *material* misstatement of the financial statements.

Consistent with a risk-based approach, the prioritization of financial reporting elements is based on the above principles. Following the selection of priority financial reporting elements, the evaluation team must next identify the assertions applicable to each element. Examples of assertions are illustrated in our response to Questions 71 and 72. Once the applicable assertions are identified, they must be rated according to risk using the *same* methodology applied when selecting the priority financial reporting elements; i.e., considering the same quantitative considerations and qualitative factors. *In effect, the risk ranking of assertions is the same methodology applied to evaluating the risk of financial reporting elements, but is applied at a more granular level – i.e., the assertion level.*

The risk-rated financial reporting assertions are then used to determine the emphasis in (a) understanding the critical upstream and period-end processes affecting the priority financial reporting elements (to which the assertions apply), (b) selecting the entity-level controls and other key controls embedded within the critical processes, and (c) determining the nature, timing and extent of controls testing. For example, the more risky an assertion, the greater the need to document the underlying processes and identify the key controls that reduce the assertion risk to an acceptable level. High risk assertions ordinarily require a strong understanding of the underlying processes and key controls, beginning with a top-down approach. Low risk assertions may warrant no further work, because a conclusion that an assertion is "low risk" is an intuitive assumption by knowledgeable persons that there is relatively little risk of a material misstatement to the financial statements. Note that the "what can go wrong" question is explicitly considered when evaluating the relative riskiness of the assertions. The evaluation team's response to this question helps the team determine whether or not there is a risk of a material misstatement.

In Auditing Standard No. 5, the PCAOB defines an account or disclosure as a significant account if "there is a reasonable possibility that the account or disclosure could contain a misstatement that, individually or when aggregated with others, has a material effect on the financial statements, considering the risks of both overstatement and understatement … without regard to the effect of controls." The PCAOB also summarized the risk factors relevant to identifying significant financial reporting elements. The Board's summary of risk factors is similar in substance to the factors we provide in our response to Question 51.

The Board also has asserted that the significant accounts identified in the audit of internal control over financial reporting should be the same as the significant accounts identified in the financial statement audit. The Board's focus on a "reasonable possibility" suggests the need to consider qualitative factors when selecting significant financial reporting elements. This approach should lead to the identification of the areas of greatest risk for material financial misstatements or untimely disclosure, e.g., revenue recognition, loss contingencies, capital

expenditures, income tax reporting, etc. Input on this assessment should also be obtained from management and the audit committee, with management approving the results.

It is important to note that the results of the scoping exercise should be validated with the independent public accountant. Practice has indicated that "scoping dialogues" with the auditors often result in the company scoping in additional accounts. This iterative "give and take" is often due to the judgmental nature of scope setting and caption decomposition to specific accounts.

53. How does a company assess materiality when prioritizing financial reporting elements?

As companies identify the primary financial reporting elements, select the key processes affecting those elements and evaluate the design and operating effectiveness of their internal control over financial reporting, questions regarding materiality often arise. We often receive questions regarding the available "rules of thumb." In the commentary below, we outline the authoritative view of regulatory bodies and standard setters. Due to the judgmental nature of materiality, we believe management should formulate its views on materiality and discuss its views with the external auditors.

The PCAOB clarified the consideration of materiality in Auditing Standard No. 5 by stating that the auditor should plan and perform the audit of internal control over financial reporting using the same materiality measures used to plan and perform the audit of the annual financial statements. In addition, the PCAOB clarified in its revised standard that interim materiality is only used when assessing whether a deficiency materially impacts quarterly financial statements (i.e., interim materiality is not used for purposes of planning the audit of internal accounting control).

The PCAOB has avoided making explicit suggestions with respect to quantitative guidelines. This is not surprising. The Financial Accounting Standards Board (FASB) has long emphasized that materiality cannot be reduced to a numerical formula. In its Concepts Statement 2, the FASB noted that some had urged it to promulgate quantitative materiality guides for use in a variety of situations. The FASB rejected such an approach as representing only a "minority view," stating that the predominant view is that only those who have all the facts can properly make materiality judgments. The FASB stated its "present position is that no general standards of materiality could be formulated to take into account all the considerations that enter into an experienced human judgment."

The SEC's point of view on materiality is found in Reg. § 210.1-02(o) of Regulation S-X. That rule states "the term 'material,' when used to qualify a requirement for the furnishing of information as to any subject, limits the information required to those matters about which an average prudent investor ought reasonably to be informed." In a Staff Accounting Bulletin, the SEC staff addresses the question, "... may a registrant or the auditor of its financial statements assume the immateriality of items that fall below a percentage threshold set by management or the auditor to determine whether amounts and items are material to the financial statements?" The staff's answer follows:

> No. The staff is aware that certain registrants, over time, have developed quantitative thresholds as "rules of thumb" to assist in the preparation of their financial statements, and that auditors also have used these thresholds in their evaluation of whether items might be considered material to users of a registrant's financial statements. One rule of thumb in particular suggests that the misstatement or omission of an item that falls under a 5% threshold is not material in the absence of particularly egregious circumstances, such as self-dealing or misappropriation by senior management. The staff reminds registrants and the auditors of their financial statements that exclusive reliance on this or any percentage or numerical threshold has no basis in the accounting literature or the law.
>
> The use of a percentage as a numerical threshold, such as 5%, may provide the basis for a preliminary assumption that – without considering all relevant circumstances – a deviation of less than the specified percentage with respect to a particular item on the registrant's financial statements is unlikely to be

material. The staff has no objection to such a "rule of thumb" as an initial step in assessing materiality. But quantifying, in percentage terms, the magnitude of a misstatement is only the beginning of an analysis of materiality; it cannot appropriately be used as a substitute for a full analysis of all relevant considerations. Materiality concerns the significance of an item to users of a registrant's financial statements. A matter is "material" if there is a substantial likelihood that a reasonable person would consider it important.

There are many qualitative factors when evaluating materiality of an item that may appear to fall below management's quantitative thresholds. For example, the SEC staff lists the following considerations as factors that may well render material a quantitatively small misstatement of a financial statement item:

- Whether the misstatement arises from an item capable of precise measurement
- Whether the misstatement arises from an estimate and, if so, the degree of imprecision inherent in the estimate
- Whether the misstatement masks a change in earnings or other trends
- Whether the misstatement hides a failure to meet analysts' consensus expectations for the enterprise
- Whether the misstatement changes a loss into income or vice versa
- Whether the misstatement concerns a portion of the issuer's business that has been identified as playing a significant role in operations or profitability
- Whether the misstatement affects the registrant's compliance with regulatory requirements
- Whether the misstatement affects the registrant's compliance with loan covenants or other contractual requirements
- Whether the misstatement has the effect of increasing management's compensation
- Whether the misstatement involves concealment of an unlawful transaction

The SEC staff makes it clear that the above list is not intended as an exhaustive one of the circumstances that may affect the materiality of a quantitatively small misstatement. For example, the demonstrated volatility of the price of an issuer's securities in response to certain types of disclosures may provide guidance as to whether investors regard quantitatively small misstatements as material. The SEC staff states that when "management or the independent auditor expects (based, for example, on a pattern of market performance) that a known misstatement may result in a significant positive or negative market reaction, that expected reaction should be taken into account when considering whether a misstatement is material."

In summary, *professional judgment will be a significant factor when applying materiality in conjunction with an audit of internal control over financial reporting*. The weight of the authoritative guidance makes it clear that there are no "hard and fast" rules regarding materiality. In effect, the only individuals positioned to make judgments about materiality are those who possess all of the facts. The SEC staff has said, "… an assessment of materiality requires that one views the facts in the context of the 'surrounding circumstances,' as the accounting literature puts it, or the 'total mix' of information, in the words of the Supreme Court. … The shorthand in the accounting and auditing literature for this analysis is that financial management and the auditor must consider both 'quantitative' and 'qualitative' factors in assessing an item's materiality. Court decisions, Commission rules and enforcement actions, and accounting and auditing literature have all considered 'qualitative' factors in various contexts."

54. What are "control units," and why are they important?

A "control unit" is a business unit, division, subsidiary or common operational area that is relatively autonomous in terms of setting business objectives and managing operations on a day-to-day basis. Control environments in different units may vary due to differences in risk profiles, the nature of the business and management's preferences, value judgments, operating styles and transaction flows. Autonomy often results in unit management having a span of control in which their actions and inactions at the entity level may impact the performance of the unit's internal controls at the process level.

Many companies have common processes and shared services operations in which the competencies and systems for managing key functions (e.g., IT, payroll and accounts payable) reside. The nature and breadth of shared-service operations and near-term plans to expand them should be considered because these operations often constitute separate control units.

Many companies also outsource significant processes and functions, particularly in the IT area. The SEC and PCAOB have both made it clear that the use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting. In this context, it is important to remember that control units outsource processes and functions.

The choice of control units is an important decision and requires careful thought and judgment in considering how management structures, runs and controls the organization. It requires an understanding of the extent of common processes and IT platforms and the degree of centralization versus decentralization. Depending on the results of the risk assessment, different control units – such as significant, autonomous domestic and foreign subsidiaries – may warrant separate assessments of controls at either the entity level or process level, or at both levels. The organization's control units impact the financial statements of the reporting entity that consolidates them and their relative risk must be considered when planning the controls assessment.

55. How does management select the control units and locations to review?

In its interpretive guidance to management, the SEC states that "management's consideration of financial reporting risks generally includes all of its locations or business units." The top-down, risk-based approach to selecting units and locations for inclusion in the scope of an assessment of internal control over financial reporting is based on management's assessed risk of a material misstatement to the financial statements. Once the organization is broken down into separate control units, the relative risk of the various units and locations should be evaluated to determine those units and locations that should be included in the scope of the controls assessment.

It is not necessary to assess the controls at every control unit. It is also not necessary under a risk-based approach to evaluate controls at each location of the company. Entity-level controls may also provide sufficient evidence in certain circumstances. For example, the SEC states: "Management may determine that financial reporting risks are adequately addressed by controls which operate centrally." In such instances, the evaluation approach is similar to that of a business with a single location or business unit. For example, some units and locations would ordinarily be included in the Section 404 assessment scope because they include controls that are applied either entitywide or regionally (e.g., taxes, treasury and procurement). Other units might be excluded from the Section 404 assessment scope because their processes and controls have relatively little impact on reported financial results or are relatively low risk. However, those units and locations excluded from the assessment scope, both individually and in the aggregate, should either be clearly immaterial or present relatively low risk of a material misstatement to the financial statements.

When the controls necessary to address financial reporting risks operate at more than one location or business unit, management would generally evaluate evidence of the operation of the controls at the individual locations or business units. Under the SEC interpretive guidance, management must base the selection of appropriate locations and units on the two components of "ICFR risk" – the risk of material misstatement and the risk of control failure. Under a risk-based approach, the following principles apply:

- The business units or locations that contribute significantly to the financial results and operations of the company are typically included in scope because they generally include the critical processes that impact the higher risk financial reporting elements. These units or locations might include:
  - The core operating divisions or units that drive the segment results disclosed in the financial statements – these divisions or units may include multiple locations for which there are centralized accounting records and systems affecting one or more priority financial reporting elements.

- Units and locations with shared services operations that converge and centralize the operations, transaction processing and control structure affecting one or more priority financial reporting elements.
- Units and locations for which there are multiple standardized processes and controls over transactions affecting a significant account or group of related accounts (e.g., receivables and sales) that provide consistency in operations and controls.

For these business units and locations, the SEC states that "management should generally consider the risk characteristics of the controls for each financial reporting element, rather than making a single judgment for all accounts at [a particular] location when deciding whether the nature and extent of evidence is sufficient." Effective entity-level monitoring controls and analytics may exist that are entitywide in scope and provide the reporting entity's management with sufficient transparency as to whether key controls are operating effectively at multiple locations and units and whether financial information reported is consistent with economic reality. If these entity-level controls operate effectively at a sufficient level of precision in detecting a material error on a timely basis, they may be relied upon for purposes of addressing relevant financial reporting assertions in lieu of relying on process-level controls at the applicable units or locations.

- Although a location or unit is not individually important from a financial reporting standpoint, it may present specific risks that by themselves could create a reasonable possibility of a material misstatement of the consolidated entity's financial statements. The SEC states:

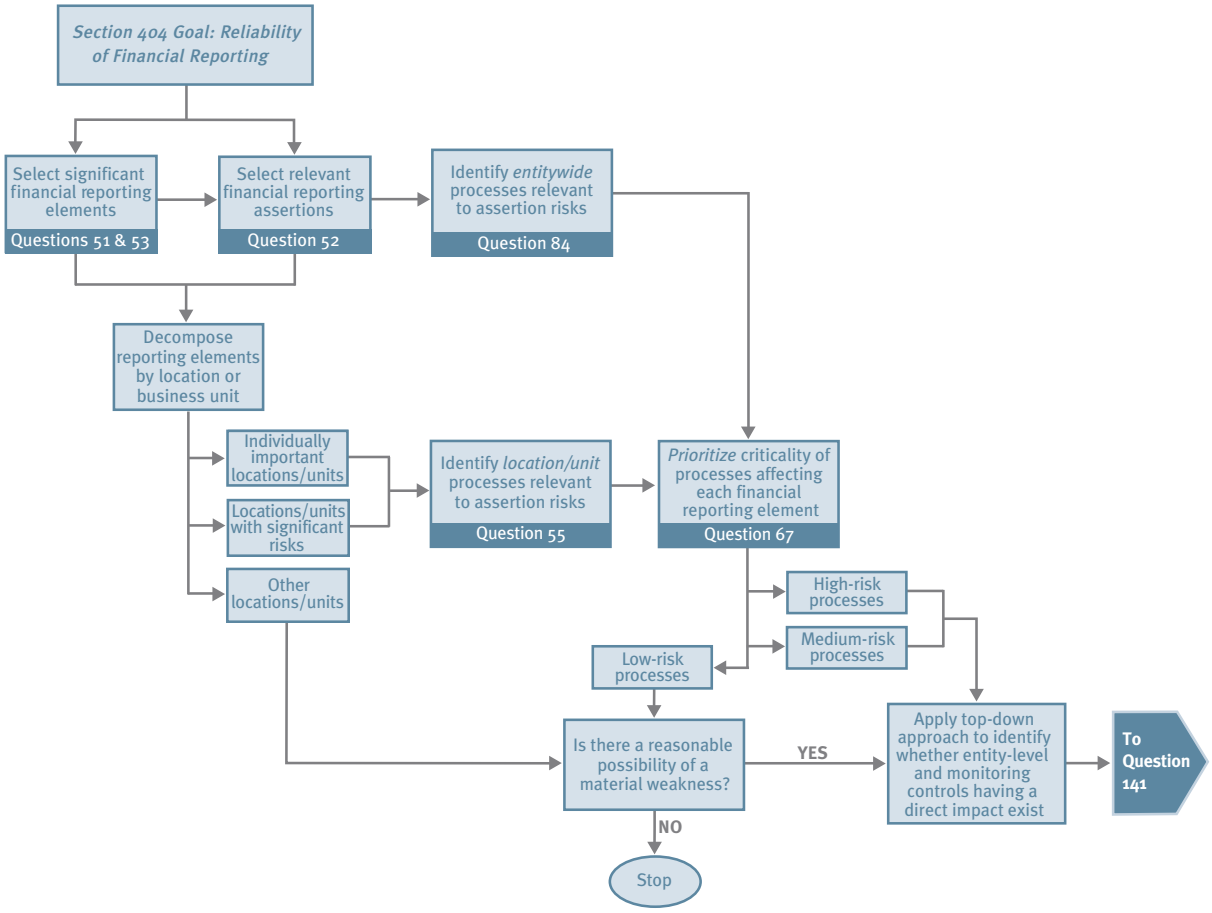
  When performing its evaluation of the risk characteristics of the controls identified, management should consider whether there are location-specific risks that might impact the risk that a control might fail to operate effectively. Additionally, there may be pervasive risk factors that exist at a location that cause all controls, or a majority of controls, at that location to be considered higher risk.

  For example:

  - A global trading unit managing currency, commodity and other financial risks for the enterprise as a whole may present unique and volatile risks not found in the operating units.
  - The decision-making authority of a given unit or location can result in creation of obligations on behalf of the reporting entity or encumber significant assets of the reporting entity.
  - There is a potential for surprise at a unit that may be immaterial based on traditional financial measures, but through its actions or inaction can have a huge impact on the organization, such as exposure to high-profile catastrophic environmental disasters or significant litigation that could have financial reporting impact.
  - There is exposure to material unrecognized obligations or contingent liabilities at a given location or unit (e.g., loss reserves).
  - Due to the environment in the country in which it does business, a particular unit or location is exposed to fraud, sensitive payments or other factors impacting the reporting company's reputation. (Note that these situations might require unit-specific entity-level control assessments to understand "tone at the top" as well as a controls evaluation at the unit itself.)
  - A unit that previously has reported significant control deficiencies may continue to present key risks, and should ordinarily be included in scope.
  - An otherwise insignificant location or unit includes a material account balance (e.g., inventory or fixed assets) that warrants attention because of inadequate coverage of the account balance at other locations on a consolidated basis. (Note that in these situations only the processes and controls affecting the material account need be included in scope.)

  In most of the above examples, what is on the books is not as important as what is not on the books.

Simply stated, coverage is not the goal; the focus is on risk. Following is a schematic illustrating the thought process:



In many cases, application of the above thought process to "individually important locations and units" and "locations and units with significant risks" should result in selecting enough locations and units that will enable management to complete an adequate review of areas where there is a reasonable possibility of a material weakness. While the consideration of entity-level controls was often an afterthought under Auditing Standard No. 2, these controls should be considered first when applying the top-down approach, as outlined by the SEC's interpretive guidance. For example, the SEC states that when ICFR risk is low at individual locations or business units, "management may determine that evidence gathered through self-assessment routines or other ongoing monitoring activities, when combined with the evidence derived from a centralized control that monitors the results of operations at individual locations, constitutes sufficient evidence."

The message is that *companies with numerous locations and units should have effectively operating entity-level controls.* If there is an absence of these controls, or if established entity-level controls are not operating effectively, management may be required to expand the evaluation of controls at the location and business unit level because management is unable to rely on the operation of monitoring, oversight and other appropriate entity-level controls. In addition, there could also be an impact on the work of the external auditor. Ineffective entity-level controls will generally result in an increase in scope in terms of the nature, timing and extent of testing at the process level, resulting in increased audit fees.

As illustrated in the preceding discussion, the process for selecting units and locations for inclusion in the scope of an evaluation of internal control over financial reporting involves considerable judgment because it is risk-based. Once the units and locations are selected, management should document the supporting rationale and

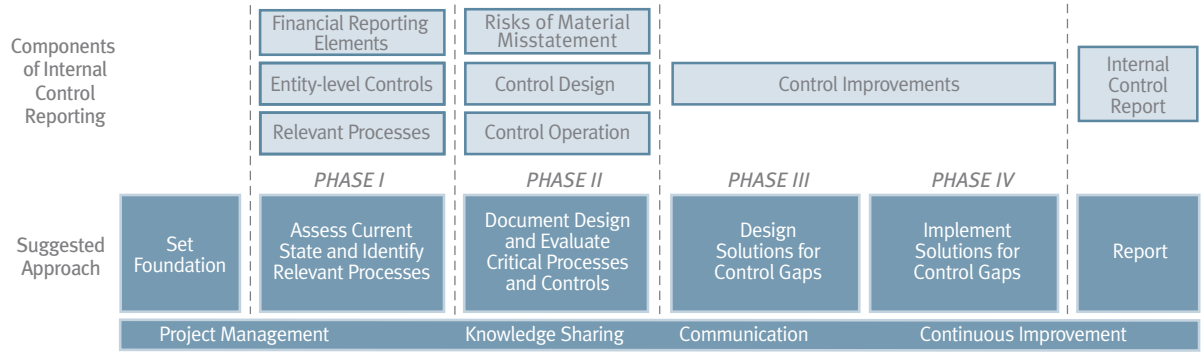
obtain concurrence of the independent public accountant. For large and complex companies with dispersed assets and operations, management should expect the auditors to offer a point of view that will likely result in further refinements to the company's articulation of multilocation coverage.

56. How should management communicate the project effort to the organization?

The project team should work with the project sponsor to develop a communications plan. This plan should outline how the sponsor and the team communicate with executive management, the audit committee, unit management, process owners, the disclosure committee and the independent public accountant throughout the duration of the project. When designing and implementing an internal communications plan, keep in mind that the objective is to build stakeholder commitment, particularly with unit managers and process owners. The sponsor and team leader should articulate the purpose and importance of the project, the sponsorship of the project, the project timing and approach, and everyone who is primarily responsible for critical internal controls, including what is expected of them now, what is expected of them during the project and what is expected after completion of the project.

57. What steps should be included in the project plan?

The project plan should be a phased approach, as shown in the following illustration:



Set foundation – Includes steps for organizing the project, developing the project plan, and agreeing on project approach and reporting requirements.

Phase I (assess current state and identify relevant processes) – Identifies priority financial reporting elements, assesses current state of critical processes and points of origin for satisfying public report requirements, inventories available internal controls documentation, documents the financial close process and develops a critical process scorecard (see Question 58 for explanation).

Phase II (document design and evaluate targeted critical processes and controls) – Identifies risks and assertions for key financial reporting elements, documents the critical processes affecting those elements, assesses the effectiveness of control design, validates and tests effectiveness of control operation, summarizes results, and develops action plan for improvements and remediation.

Phase III (design solutions for control caps) – Designs process improvements to facilitate management reporting and issues management, aligns objectives with corporate governance guidelines, and identifies changes that impact and reflect upon existing controls. In this phase, the project team designs the revisions needed to improve and remediate internal controls, including the related policies, processes, controls, reports and systems.

Phase IV (implement solutions for control gaps) – Facilitates the testing and rollout of improvements and development of training guidelines and documentation.

Report – Communicates the results of the Section 404 evaluation to the appropriate stakeholders.

The project plan should be supported with project management, communication and knowledge-sharing activities, and a commitment to continuous improvement.

Any project plan must recognize that Section 404 requires an ongoing assessment. Our suggested approach should address both the initial annual assessment and the ongoing assessment. Management must continue to evaluate internal control over financial reporting on an annual basis in the years following the initial assessment. The approach and supporting technology should provide the foundation for process-owner self-assessments of control operational effectiveness at any point in time, e.g., as of year-end or quarter-end. With process-owner feedback and an iterative process, management will be positioned to focus on evaluating the effects of change each quarter, e.g., changes in processes, systems, operations and other factors. See Questions 186 through 197 for considerations in moving beyond the initial year assessment.

58. To what extent can companies rely on prior controls documentation?

If controls documentation exists from prior years, it should be used if it is current and complete. The SEC has indicated that documentation may consist of paper documents, electronic or other media, and it can be presented through the use of policy manuals, job descriptions and internal documents, memorandums and forms. Once the critical processes are selected for each significant control unit, the project team inventories the formal documentation of policies, processes and procedures that already exists at the process level. Potential sources of internal controls documentation include policy and procedure manuals and job descriptions, process-owner documentation (process models and flowcharts), internal audit working papers and reports, prior years' independent public accountants' documentation, and documentation of the disclosure controls and procedures supporting the existing certification process. A scorecard that gauges whether the critical processes are fully documented, partially documented or undocumented is a useful project-management tool for summarizing the inventory. The scorecard should note whether the documentation is complete, current and relevant for each type of document desired, e.g., procedures, policies, maps and risks.

59. How should companies document and validate their assessments of internal controls?

There are many different methods for documenting and validating internal control assessments. The most important thing is to adopt a format that addresses the right questions, including:

- What are the key controls?
- What risks do they address?
- Who owns them?
- How are they rated as to design effectiveness? Are the controls adequate in mitigating the financial reporting assertion risks they are intended to address?
- How are they rated in relation to operational effectiveness? When tested, do the controls work and operate as intended?

Ultimately, validation occurs when controls are tested to verify they are operating as designed. However, it is imperative to get the design documented correctly. A walkthrough of the process using the relevant documents is an effective method of ascertaining the procedures and controls as they really function. (See Questions 121 through 155 for guidance with respect to validating operating effectiveness of internal controls.)

60. What tools and technologies are used to implement controls repositories, document process maps, facilitate the assessment process and manage overall Section 404 compliance?

Technology is a key enabler for Sarbanes-Oxley compliance. There is a wide range of software tools available in the marketplace, with no less than 70 tools claiming to enable Sarbanes-Oxley compliance. These tools can be segmented into either "point solutions" or "platform solutions." Point solutions are applications designed specifically for Sarbanes-Oxley compliance. Platform solutions are integrated software applications designed for governance, risk management and compliance (GRC) or software infrastructure designed for another purpose, such as business process automation, document management or financial management, and adapted for Sarbanes-Oxley compliance and/or GRC. Point solutions typically support deeper analysis and reporting requirements for Sarbanes-Oxley compliance, while platform solutions provide extended capabilities and could serve as infrastructure for broader GRC activities over time.

Sarbanes-Oxley software has made significant strides from the first generation software releases. These applications had limited functionality and often included nothing more than a library of controls, best practices and benchmarks. Others were simply content management and financial reporting solutions dressed up to look like they were specifically designed to address the demands of Sarbanes-Oxley compliance. However, realizing the true market potential, many software vendors have invested significantly into vastly improved second- and third-generation releases. Many of these releases are now capable of mapping business processes, cataloging best practices, providing version control, managing documentation of policies and procedures, flagging internal transactions, storing key internal controls and building user interfaces that allow executives to concurrently drive compliance controls and performance management capabilities. As these vendors race to be the first to provide an end-to-end compliance solution, a very competitive and fragmented landscape has emerged. The "total" solution for governance, risk management and broader compliance does not currently exist, and will likely emerge over time through integration of several applications and platforms and as companies evolve toward enterprise risk management.

Platform solutions can be further broken down into four categories – ERP (enterprise resource planning), ECM (enterprise content management), BPM (business process management) and purpose-built GRC platforms. These categories are discussed further below:

- ***ERP Platforms:*** The ERP vendors typically integrate new capabilities with their own financial applications, which provide a significant advantage by leveraging chart of account structures, organizational structures, security profiles and access privileges. However, their initial "bolt-on" compliance solutions did not compare well to their more nimble competitors in functionality, and mainly focused on ensuring that ERP financial reporting tools met the Sarbanes-Oxley requirements. Several of these solutions experienced integration difficulties with existing third-party content management systems and disparate enterprise applications, and only worked successfully in strict, homogenous technical environments. Several ERP vendors, primarily Oracle and SAP, have recently made significant investments both in product development and acquisition of complementary components toward an integrated GRC reference architecture.
- ***ECM Platforms:*** The ECM vendors provide both Sarbanes-Oxley applications and general compliance frameworks. The strengths of products in this segment are document management, workflow and records management. Several ECM vendors, primarily IBM and Stellent (which has been acquired by Oracle), attempt to integrate workflows and Sarbanes-Oxley templates within their core product to consolidate various evidence gathering activities, and provide strong capabilities around document management, versioning and archiving. These vendors also attempt to leverage their large entrenched install base and historical expertise with group collaboration. However, these solutions tend to be weak in several areas, particularly process automation, risk management and support for the COSO Internal Control – Integrated Framework.
- ***BPM Platforms:*** The BPM vendors, primarily BWise and Movaris, are using their business process management toolkits to build compliance specific templates that map out new business processes, allowing executives to model, simulate and analyze various compliance control processes before implementing them. This is

a unique approach. Instead of building specific applications designed to address compliance pain points or building software programs that bolt on to existing enterprise applications, BPM solutions focus on the core business processes and remap and automate them at an enterprise level, ensuring transparency, accountability and financial control across disparate platforms and applications. By initiating the compliance process at an enterprisewide level, companies are able to prevent significant compliance initiatives from becoming fragmented and redundant "silo activities." Adoption of BPM software has been slow as companies continue to look for hard evidence of return on their investment (ROI). As a result, BPM vendors have been leaning toward quick-hitting specialized Sarbanes-Oxley solutions or first generation GRC platform solutions, instead of process-centric BPM solutions requiring fundamental business changes. Many BPM companies are actively looking to build, partner or acquire compliance point application or broader GRC capabilities.

- ***Purpose-Built GRC Platforms:*** The purpose-built compliance software players rely on strong go-to-market messages around such things as subject matter expertise, client experiences and vertical applications for GRC that are integrated on a shared platform. Most GRC platforms, primarily Axentis, Open Pages, Paisley, and Protiviti, provide applications that drill into specific compliance "pain points," such as financial statement certification, internal controls monitoring, risk assessment and automated process support for regulatory filings. Now in their second or third releases, purpose-built solutions are typically more affordable, mature and provide a high ROI. Many so-called purpose-built platform vendors are attempting to build out an end-to-end GRC solution and establish additional traction in the marketplace.

It is very important for companies to define their technology requirements toward the end of the planning process, after obtaining a greater understanding of the project work plan, scope and requirements. Companies also must consider whether they should take a "compliance-driven" (short-term) or "value-driven" (long-term) approach to their Sarbanes-Oxley compliance initiative, as this approach has implications for whether they should consider a point solution for Year One and beyond, or alternatively choose a platform solution. Technology needs will vary and are dependent upon several factors, such as the organization's size, complexity and geographies; the level of IT sophistication; the total number, location and connectivity of individuals involved with the compliance effort; the needs around security and workflow; the existing investments in ERP, content management, process management or compliance software; the budget and time available; and whether supporting technology is a tactical or strategic investment.

61. Is there a way to estimate the effort and cost of complying with Section 404 in Year One?

Estimates are hard to come by without some analysis. Ultimately, the effort and cost are a function of many factors, including the number and relative size of locations and units, the extent of centralization of transaction processing and the number of processes reviewed. We believe the best way to estimate efforts and costs is to base the estimate on a project plan developed after (a) finalizing scoping decisions with respect to the appropriate control units, priority financial reporting elements, critical processes, key locations, and IT systems and infrastructure; (b) determining the sufficiency of useful policies and procedures, the availability of quality process and control documentation and the extent of IT controls documentation; and (c) determining the nature of the gaps that exist in controls design and must be corrected. Once resource requirements are estimated, management must decide the nature and extent to which internal resources are available.

When formulating project cost estimates, the complexity of the organization's business model and its underlying processes, including the complexity of the application of generally accepted accounting principles, also must be considered. For example, a company operating in several industries with multiple locations and units across the globe will present more challenges than a company operating in one industry and out of a single location with perhaps a few branch offices. A company with an active trading function is more complex in terms of its underlying processes impacting financial reporting than a company operating in the same business without a function of equivalent complexity. The point is that the intrinsic complexity of the business can impact Section 404 compliance costs.

Culture can also be a relevant consideration. If the corporate culture has traditionally supported companywide initiatives, then the project will be easier and less costly; however, if it hasn't, then the project will be harder and more costly to do. In addition, the level of change anticipated or underway in the organization is an important factor. If the company is emerging from bankruptcy, installing a major new system or integrating certain processes and controls of a newly acquired company, the project will be more difficult to plan and execute, and therefore more costly.

For these reasons and because there is no "one size fits all," it is difficult to generalize estimates, particularly since most companies used a "bottom-up" approach versus a top-down and truly risk-based approach to their initial compliance efforts. It is possible for one to speculate about the percentage breakdown of planning, documentation and design evaluation, testing and so forth. For example, planning is not likely to exceed five percent to 10 percent of total costs. However, estimating the split between documentation and design evaluation and testing operating effectiveness is another matter. For example:

- The number of processes, the number of control units, the number of systems and the number and relative size of locations and units impact the controls documentation and design evaluation.
- The total testing effort will be driven by the number of key controls and the location at which those controls are executed.
- The testing effort also will be impacted by the following:
  - The extent of reliance on self-assessment
  - The extent of reliance on entity-level and process-level monitoring controls, especially in low-risk areas
  - The extent of reliance on automated controls (versus manual controls)
  - The parameters around independent testing of manual controls, e.g., the desired confidence level and desired level of precision, which drive the resulting sample sizes
  - The number of exceptions encountered during the testing process
  - The extent of testing by the external auditor in areas considered by management to be low risk
- As noted previously, the extent of remediation and the resulting need to retest are a significant unknown for many companies undertaking compliance for the first time.
- The impact of reliance on outside service organizations and, if the outsourced processes are significant, the willingness of such organizations to provide a satisfactory SAS 70 letter.
- The extent to which the company has a repeating, defined and managed internal control structure is an important factor influencing Section 404 compliance costs. Typically, the more mature a company's upstream business processes, the less the expected costs to comply with Section 404. For example, the quality of the period-end financial reporting close process and the company's history with respect to internal control issues and material audit adjustments provide insights as to potential cost drivers from a Section 404 compliance standpoint.
- The availability of qualified internal resources to lead the effort and to support all or various phases of the effort. (By "qualified," we mean project management capabilities at the appropriate "scale," business process knowledge, internal controls subject matter expertise, knowledge of the Section 404 rules, etc.).

It is also possible that management may decide to do more documentation and control design assessment work in the first year of compliance as a way to provide better transparency as to how the processes affecting financial reporting are functioning, as well as the sources of risk and the controls in place to mitigate those risks. This initial documentation might serve to enable everyone to apply more effectively a top-down, risk-based approach and would reinforce to everyone the importance of internal control over financial reporting. Even though controls testing might be focused on key controls for "in-scope" units and controls, the more expansive

documentation and controls design assessment increases the first-year costs. However, the documentation also provides a good foundation for the compliance process going forward by facilitating development of cost-effective test plans and agreements with the external auditors regarding the key controls.

A final set of factors to consider relates to flexibility, i.e., the more flexibility management has from a Section 404 compliance standpoint, the greater the number of available options for managing costs. For example, the expected elapsed time from the date management plans to begin the project through the date by which the project must be completed (as well as have the necessary documentation available for the external auditor's use) has a significant impact on management's ability to formulate a cost-effective compliance plan. Likewise, the competency and responsiveness of personnel responsible for operating the key controls will affect the plan. Finally, the existence of an effective internal audit function increases management flexibility in terms of selecting the most cost-effective compliance plan.

The message is this: The Section 404 project is a phased project in which the results of each phase provide clarity as to the magnitude of the effort required for the next phase. To illustrate, referring to the suggested approach in Question 57, we recommend that the project team first complete both Set Foundation and Phase I before committing to an estimate. Further, many companies use pilots to develop realistic estimation guidelines as they progress through Phase II, as introduced in Question 57. This approach enables management to build up a more reliable "order of magnitude" view of Section 404 costs because it identifies the key areas and estimates the expected level of effort for each of those areas. The cost drivers we have summarized above can make a big difference in sizing the overall compliance effort.

In summary, there are many variables making realistic rules of thumb difficult to find, much less trust as reliable. The total effort ultimately is a function of many things. The total cost is also not necessarily the best indicator of the extent of the burden as viewed by management, since the size, structure and complexity of the company will often dictate how costly these requirements will be. The good news is that, regardless of the initial start-up costs, most issuers have reported a decrease in Section 404 compliance costs in subsequent years. In effect, the costs are front-loaded.

62. Will companies need to add internal resources to comply with Sections 404 and 302?

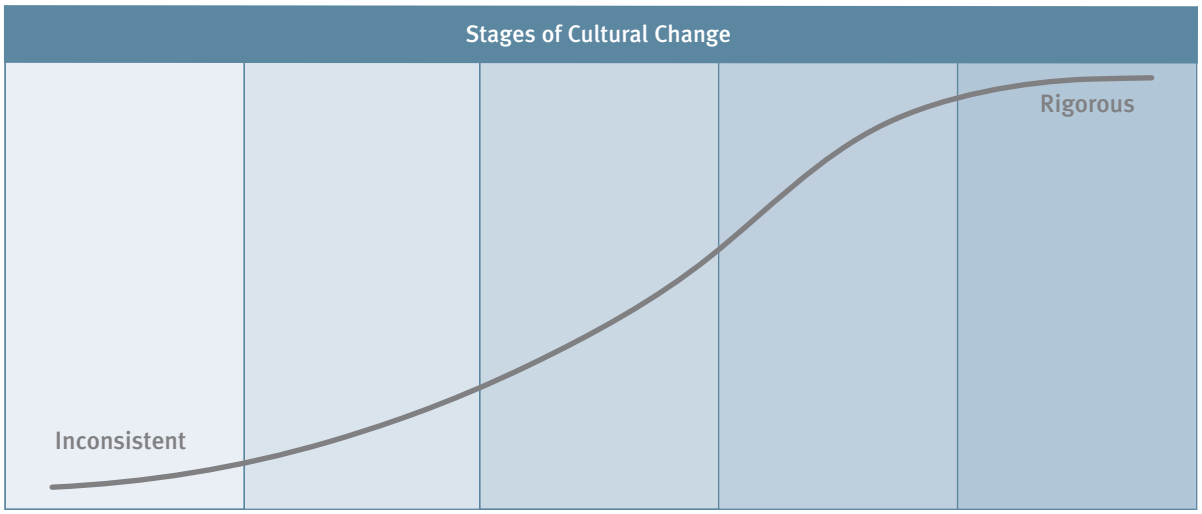
Not necessarily. With respect to the initial annual assessment of internal control over financial reporting, external resources may be used to supplement gaps that internal resources are unable to address. The key is to deploy qualified resources with the requisite knowledge of processes, risks and controls, as well as appropriate knowledge of the Sarbanes-Oxley Act and its specific requirements related to the application of a top-down, risk-based approach to evaluating internal control over financial reporting. With respect to the ongoing quarterly and annual assessments after the initial annual assessment, the evaluation process should be designed and supported to enable the existing complement of internal resources, including process owners, internal audit and risk control specialists, to execute it.

63. Is a cultural assessment necessary?

It depends. Several of the attributes used by COSO in defining the control environment, as part of the entity-level assessment, are relevant to an evaluation of the organization's culture. For example, "tone at the top," commitment to ethical behavior, and management's operating philosophy and leadership style are all evaluated as part of the entity-level assessment and have a significant impact on the organization's culture.

If there are questions as to the potential impact of culture on financial reporting, consideration should be given to interviewing key executives and conducting a cultural survey of employees to corroborate management's top-down assessment of the control environment. An organization's strategies, its performance expectations, its reward systems and the way it reacts to failures, makes decisions and manages conflicts all contribute to defining its culture. The organization's culture, in turn, can affect the attitude of its managers and key employees toward internal controls and the reliability of financial reporting.

The following graph illustrates the stages of cultural change as they relate to the disclosure infrastructure:



Denial	Remorseful Acceptance	Commit	Ownership/Accountability	Integrate
This is just bureaucracy Too many unknowns and no answers "We do it right anyway" No need to "rock the boat"	More work for scarce resources Take the easy way out Initiate ritualistic behavior Solutions with substance lacking	Initiate cultural change Form disclosure committee Implement interim solution Source public report information components Improve disclosure infrastructure Begin documenting critical processes, risks, controls Create a "chain of certifications"	Put infrastructure in place Document critical processes, risks, controls Close control gaps Align process owners and internal audit with quarterly evaluation process Continuously improve and focus evaluation process Focus on change and impact on controls Create a process-based "chain of accountability"	Disclosure infrastructure fully integrated with culture Formalize top-down, risk-based approach Integral to managing the business: "How we do business around here"

When Sarbanes-Oxley was passed, many U.S. accelerated filers were on the left side of the graph with respect to the executive certification process, either experiencing "denial" or "remorseful acceptance." With the initial filings in fall 2002 and spring 2003, companies began to move to the "commit" stage as they implemented an interim solution. Many companies formed a disclosure committee. Some companies created a chain of certifications (see Question 194 for explanation). Others began documenting their processes, such as the financial close process.

As the realities of the Section 404 compliance process became clearer, companies moved farther along the continuum to "ownership and accountability," in which the processes of the business are evaluated to (a) source financial reporting risks, and (b) identify the controls in place that reduce those risks to an acceptable level. Once Section 404 was implemented effectively, companies focused on aligning process-owner monitoring and internal audit plans with the level of independent testing required on an ongoing basis. Because self-assessment has not yet been embraced as a key enabler to a top-down, risk-based approach, many companies still have a ways to go with respect to creating a process-based chain of accountability by aligning the Section 404 evaluation process with the certifying officers' quarterly evaluation of disclosure controls and procedures. As the

disclosure infrastructure continues to evolve to "integrate," it will become an integral part of the business culture in which fair disclosure and transparency will be on every manager's radar screen.

A cultural assessment survey could be useful in evaluating what stage a company is at, as well as checking its preparedness for compliance with Section 404. This assessment can be particularly useful to nonaccelerated filers who may find their personnel in the same stage of readiness U.S. and foreign accelerated filers were years ago.

Identifying Reporting Requirements and Relevant Processes

64. How does management deploy a top-down, risk-based approach to determine the extent to which internal controls should be documented and validated?

A top-down, risk-based approach is the most practical way to evaluate internal controls. It focuses the evaluation on several key decisions early in the process, beginning with selecting the most significant captions and disclosures from the financial statements. These captions and disclosures, and the significant accounts supporting them, represent the priority financial reporting elements. That accomplished, the project team then identifies the financial reporting assertion risks relevant to each significant financial reporting element and sources these risks within the major transaction flows that impact the priority elements. Obviously, sourcing the risks requires an understanding of the major transaction flows.

Once the risks are sourced, the evaluation team then selects the key controls that address the most critical financial reporting assertions and evaluates the effectiveness of their design. A risk-based approach also (a) considers the relative risk levels (including the risk of control failure) when deciding the evidence needed to support a conclusion on the effectiveness of control operation, (b) determines multilocation scoping considerations based on risk, and (c) sets documentation standards appropriate to different levels of risk. All of these activities, and the factors affecting them, are discussed in this publication.

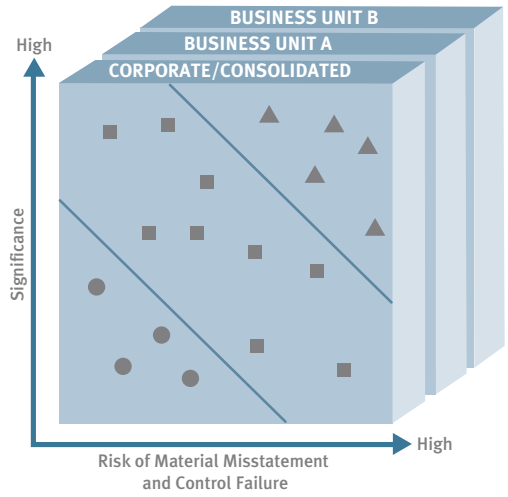
Risk Assessment Activities Driving a Top-Down, Risk-Based Approach	Discussed in Questions
(1) Select significant financial reporting elements	51, 52, 53
(2) Identify relevant assertions for each significant financial reporting element	52, 71, 72
(3) Understand major transaction flows	66, 67
(4) Source risks of material misstatement within major transaction flows	74, 90, 91
(5) Select effectively designed key controls addressing each relevant assertion	42, 81, 96, 97, 99, 140
(6) Decide documentation standards at different levels of risk	58, 59, 80, 92, 184
(7) Consider relative risk levels to decide tests of operating effectiveness	14, 64, 121, 141
(8) Determine locations and units to include into scope	54, 55

These activities are important because the SEC interpretive guidance allows management to exercise judgment during the risk assessment and scoping process. The decisions management must make in conjunction with these activities provide a context for management's dialogue with the external auditor during the early stages of the process. In fact, the external auditor's application of a top-down, risk-based approach is greatly augmented by, and reaches the highest level of efficiency when the auditor understands, a well-documented management application of that approach.

There is another vitally important reason why the eight risk assessment activities are so critical. If management and the external auditor can agree on the key decisions addressed through these activities, it leaves open one remaining critical decision – the testing of operating effectiveness. This particular decision is the most natural point of divergence between management and the auditor in their respective evaluations of internal control over financial reporting. Since management is an insider and the auditor is not, the two parties do not begin at the same point of knowledge when designing the necessary tests of operating effectiveness.

The key point is that the difference between management and the auditor in their respective approaches to testing operating effectiveness will be much less if there is convergence on the decisions addressed through the eight risk assessment activities. A well-documented management assessment maximizes audit cost-effectiveness. The documentation must include supporting rationale for management's decisions about the critical risks and key controls. The good news is that much of this "rationale documentation" is a one-time investment.

With respect to determining the extent to which internal controls should be documented and validated, we recommend that the level of risk be a determining factor. The following framework may be useful for illustrative purposes:



Documentation, Assessment and Validation Legend

▲	Document the critical processes affecting this priority financial reporting element Source the risks ("what can go wrong") and identify controls in place that mitigate those risks using a top-down approach starting with the entity-level and monitoring controls that operate at a sufficient level of precision at the process, transaction or application level Evaluate the effectiveness of controls design Validate that the controls are operating effectively
■	Understand the critical processes; however, documentation need not be as robust as for higher risk financial reporting elements Evaluate risks and controls as with higher risk elements; however, if entity-level controls include effective monitoring controls and analytics that enable management to evaluate reasonableness of reported balances, document and assess the entity-level and monitoring controls specific to this element and reduce emphasis on process-level controls
●	Minimum level of documentation and assessment required, unless more is desired by management Conclusion as to effectiveness may be supported with self-assessment and entity-level analytics and monitoring

NOTE: The symbols ▲, ■ and ● represent financial reporting elements, including financial statement accounts and disclosure items.

Prioritization of financial reporting elements is accomplished by evaluating the significance of the line item, caption, account balance, or disclosure to the reporting of financial position, results of operations and cash flows. When evaluating significance, consider the risk of a material misstatement and the importance to fairness of presentation and to a full understanding by investors of the financial statements. This evaluation should consider such issues as the nature and types of errors and omissions that could occur (i.e., "what can go wrong"), the degree of volatility in recorded amounts, the volume and size of the individual transactions processed through a given account, the complexity of calculation (e.g., can management predict results reliably and detect errors through monitoring or analytical activities), and the susceptibility to manipulation or material fraud.

When evaluating specific accounts, it is always appropriate to aggregate accounts affected by similar transaction flows. These accounts often have similar risk characteristics as well as similar controls. Other factors to consider when prioritizing financial reporting elements are summarized in our response to Question 51.

Following the selection of priority financial reporting elements, the evaluation team must next identify the assertions applicable to each element based on the nature of that element. Under Auditing Standard No. 2, all financial reporting elements were considered to be risk equivalent. However, the application of a truly risk-based approach opens the door to take an additional step. Going forward, management assesses the risk in not achieving the assertions by rating the applicable assertions according to the same risk factors applied when selecting the priority financial reporting elements. In other words, management assesses the same quantitative considerations and qualitative risk factors to identify the relevant assertions.

Once the financial reporting accounts and disclosures are prioritized and relevant assertions are identified, management should plan the appropriate documentation, assessment and validation activities. The preceding illustration includes a sample documentation, assessment and validation legend. The higher risk financial reporting elements are given the most attention. Less significant elements require less testing at the process level if effective analytics and entity-level monitoring, including self-assessment, provide reasonable assurance that the accounts and disclosures are fairly stated and presented and there is a low risk of control failure. Insignificant elements require a minimum level of documentation and little or no testing.

In summary, keep in mind four points:

- The illustration provided is just an example. Management and the project team must work out the method by which to (1) prioritize financial reporting elements, (2) identify financial reporting assertions relevant to each element and (3) select effectively designed key controls addressing each relevant assertion.
- Use "groups of related accounts" in lieu of individual accounts to facilitate the prioritization process. For example, sales, revenue deductions, cost of sales, selling expenses, receivables and finished goods are all components of the revenue cycle and are affected by routine revenue transactions.
- Break out separate accounts that are affected by separate transaction flows having unique risk characteristics.
- Last, but certainly not least, understand the independent public accountant's expectations and requirements, particularly with respect to the definition and application of materiality during the scope-setting process. It pays to avoid significant disconnects between management's risk assessment and the external auditor's risk assessment. Due to the judgmental nature of the process, an iterative dialogue with the auditor should be expected and encouraged.

65. What standards and criteria should be set before beginning the project?

Management must decide on several important scope-related issues during the project. For example, which financial reporting elements (i.e., the financial statement accounts and disclosures) should the project team review? What are the key risks? Which controls reduce these risks to an acceptable level? How much documentation is enough? How much validation and testing are needed? The criteria for addressing these scoping issues must be set at the beginning of the project. (See Questions 51, 52 and 53.)

66. Are all transactions evaluated in a similar manner when understanding transaction flows and the related controls?

No. The SEC states in its interpretive guidance that "management [is not required] to identify every control in a process or document the business processes impacting [internal control over financial reporting]." The Commission also states that "management uses its knowledge and understanding of the business, its organization, operations and processes to consider the potential sources and potential likelihood of misstatements in financial reporting elements and identifies those that could result in a material misstatement to the financial statements ('financial reporting risks')."

To put these statements into the context of the question, implementation of a top-down approach to sourcing financial reporting risk requires an understanding of the company's processes or major transaction flows affecting the significant financial reporting elements and the critical systems that support those processes or transaction flows. The PCAOB states the following in Auditing Standard No. 5:

> As a practical matter, the auditor will generally need to understand the company's processes to appropriately identify the correct controls to test.

Accordingly, an understanding of the key processes or major transaction flows enables the project team to identify the processes relevant to financial reporting. It is within these processes or transaction flows where significant errors, omissions or fraud might occur. Thus, an understanding of the flow of major transactions provides the foundation for a top-down, risk-based evaluation of internal control over financial reporting.

The processes of a business generate different types of transactions, which can be classified as routine transactions, unusual or nonroutine transactions and transactions from accounting estimates (so-called estimation transactions). The priority accounts (or groups of related accounts) are affected directly through daily entries in the general ledger for transactions occurring in the normal course of business, or indirectly through period-end adjustments to asset reserves and allowances, and for unrecorded liabilities. A more formal transaction flow consists of the records, documents and basic processing procedures used to initiate, authorize, record, process and report the transactions affecting key financial reporting elements on a daily basis. A less formal transaction flow could simply be the calculation of a month-end accrual or deferral, or the estimation of a reserve for doubtful accounts in conjunction with closing the books. The controls over these transaction types often vary in terms of formality – the less formal the processes generating the transactions, the less formal the controls.

Each transaction type is discussed further below:

- ***Routine transactions*** – Most of the relevant processes affecting financial reporting will be those that initiate, authorize, record, process and report routine transactions. These transactions represent frequently recurring data recorded in the books and records, or nonfinancial data used to manage the business. They are the recurring financial activities reflected in the accounting records in the normal course of business. For example, sales and accounts receivable, procurement and accounts payable, payroll, cash receipts and disbursements are routine transactions in the ordinary course of business. Standard journal entries booked every close, such as amortization of long-lived fixed and intangible assets, are routine transactions. These transactions are subject to more formal internal controls because of their recurring nature, the objectivity in accepting data, and the nature and volume of information processed.
- ***Other transactions*** – There are other transactions: unusual or nonroutine transactions and transactions arising from accounting estimates (estimation transactions). Unusual transactions include mergers, acquisitions, divestitures, plant closings, extraordinary items, disposals of a segment of a business and other transactions that occur infrequently. Nonroutine transactions are transactions that occur periodically, generally in conjunction with calculations by accounting personnel at month-end. They occur only periodically involving data that is generally not part of the routine flow of transactions. Examples include calculations of income taxes, accrued interest on investments and loans, depreciation expense, accrued liabilities for goods and services received but not invoiced, prepaid expenses, adjustments for foreign currency and liabilities for advance payments for services not yet delivered.

  Transactions arising from accounting estimates (estimation transactions) often involve management judgments or assumptions in formulating account balances in the absence of a precise means of measurement. They result in adjustments for loss contingencies that reduce recorded assets or record additional liabilities for the estimated effects of future events that are likely to occur and are reasonably estimable. Examples include estimating the allowance for bad debts or loan losses, allowance for excess and obsolete inventory, and warranty reserves. Estimation transactions often arise due to the uncertainty inherent in measuring assets and liabilities in the financial reporting process, i.e., there is uncertainty in measuring certain amounts or in

valuing certain accounts. If the outcome of future events is uncertain (i.e., not likely to occur) or relevant data concerning events that have already occurred cannot be accumulated on a timely and cost-effective basis (i.e., not reasonably estimable), such matters should be disclosed and not be recorded. An example is pending litigation.

With respect to routine transactions, the risk of error often lies within the process. For example, where do processing errors occur and how are they detected and corrected? When data is rejected, is it corrected in a timely manner and re-entered into the process? If multiple people or departments handle transaction data, is it tracked to reduce the risk of lost data? Is there an opportunity for fraud? If the processing involves complex mathematical calculations, how does the company identify potential errors or avoid changes to the application that could affect the accuracy of these calculations?

With respect to unusual or nonroutine transactions and estimation transactions, because they involve more subjectivity than routine transactions and occur less frequently, the process involved is often ad hoc, the controls are less formal and the risk of error is greater. These transactions are more likely to be influenced by management bias and even override of existing controls. The evaluation process must give appropriate emphasis to how significant unusual or nonroutine transactions and estimation transactions are controlled. For example, is data used in making accounting estimates reliable? Are underlying assumptions current and up to date? Are the methodologies used sufficiently robust? Significant unusual or nonroutine adjustments and transactions should be highlighted for review during the closing process because auditors can be expected to review them more carefully in order to understand how well they are controlled.

67. How are the critical processes identified?

Once the significant financial reporting elements are determined, management must identify the critical processes affecting them. The processes that most significantly affect the priority financial reporting elements are critical processes. Identifying these processes can be accomplished in two ways:

- One way is to summarize the major transaction flows for the types of transactions and the related accounting systems that materially affect the priority financial reporting elements. This is accomplished by segregating the business and the related accounting systems into a limited number of interrelated transaction flows. These transaction flows are groupings of similar economic events that directly involve the entity in exchanges with outsiders. Examples of such transaction flows include revenue, purchasing, payroll, conversion, treasury and financial reporting.
- Another approach is to segment the business into its actual processes. Ideally, this process classification scheme is one that already exists. Once the business has been decomposed into its various processes, the project team then identifies the critical processes for which to review risks and controls. Critical processes are identified based on the importance (significance) of each process to financial reporting (or, alternatively, to the business) and the likelihood of a material misstatement. The critical processes are then linked to the priority accounts and disclosures to establish their relevance to financial reporting.

Either of these approaches is acceptable. The first approach may be more efficient because it focuses solely on the information needed to support management's assertions related to the priority financial reporting elements. The second approach may be more value-added because it goes beyond the minimum compliance requirements and documents processes as they are defined in the business.

One thing to keep in mind is that the desegregation of processes may require several iterations in dialoguing with the external auditors, whose definition and application of materiality may lead them to conclude that there are additional financial statement accounts warranting analysis. These additional accounts may be derived from separate classes of transactions subject to different risks and controls or exceeding the auditor's planning materiality, and may even be peripheral to what management regards as the core processes of the business. Nevertheless, in the auditor's judgment, they may be material to financial reporting. For example, revenue streams having

different characteristics (e.g., product sales versus service revenues, sales on account versus sales-type leases or cash sales, sales through retail outlets versus direct sales from distribution centers, etc.) must be assessed separately.

68. What is a "reasonable" number of business processes for purposes of Section 404 compliance?

We are asked this question a lot. While this is a straightforward question, there isn't a straightforward response because rules of thumb are hard to come by. The answer depends on how the Section 404 compliance team chooses to define a process as well as the nature and complexity of the business. Processes can be defined as broadly as the major transaction flows, such as revenue, purchasing, payroll, conversion, treasury and financial reporting. They can be defined at a more granular level, e.g., "purchasing" can consist of procurement, receiving, accounts payable, etc. It is within these processes where risks of material errors or omissions might be sourced. Thus, an understanding of the flow of major transactions provides the foundation for an evaluation of internal control over financial reporting. This understanding is needed to support an effective risk assessment that makes the approach risk-based, provided the focus on risk is directed to the risk of material misstatement to the financial statements.

As discussed in Question 66, the processes of any business generate different types of transactions, which can be classified as routine transactions, unusual or nonroutine transactions, and estimation transactions. A more formal transaction flow consists of the records, documents and basic processing procedures used to initiate, authorize, record, process and report the transactions affecting key financial reporting elements on a daily basis. A less formal transaction flow could simply be the calculation of a month-end accrual or deferral, or the estimation of a reserve for doubtful accounts in conjunction with closing the books. The controls over these transaction types often vary in terms of formality – the less formal the processes generating the transactions, the less formal the controls. Controls must be evaluated for all types of transactions and processes having a major effect on relevant assertions pertaining to significant financial reporting elements. The process breakdown to decompose the business is intended to enable the compliance team to identify the key controls that reduce the material financial reporting risks to an acceptable level. For these and other reasons, it is difficult to generalize the number of processes.

69. What role do process owners play?

Once the critical processes are selected, the owners of those processes are identified. A process owner is an individual, a group or a unit who makes decisions with respect to the process and designs and monitors the process. Thus, for every process, there are five questions: who decides, who designs, who builds, who executes and who monitors? A process owner decides, designs and monitors. Process owners may outsource responsibilities to build and execute the process.

If there isn't a clear owner of a process, this fact should be discussed with the project sponsor as quickly as possible. Someone must be accountable, and accountability is hard to come by if no one owns a process. A point to remember, however: Too many "owners" could be just as dysfunctional as no owner of a process.

Once the process owners are identified, the project sponsor should communicate with them to explain their role in supporting the project. That role includes, among other things, assisting the project team, accumulating existing process documentation, developing additional process documentation, providing documentary evidence of the controls in place and self-assessing controls effectiveness on a continuing basis.

Summarizing Risks and Developing Control Objectives

70. Why identify risks?

Any evaluation of internal controls requires a context. Objectives provide a clear context for evaluating controls. The evaluator can source the potential root causes (or "what can go wrong") of failure to achieve the stated objectives. If the root causes are sourced to specific points within the processes of the business, the evaluator can then focus on whether there are controls that mitigate the risks. In this way, the focus of the evaluation is sharpened considerably.

Controls that mitigate risks are identified either at the source (the point where the root cause lies within the process) or downstream from the source. Controls at the source of the risk are "preventive" controls. Controls farther downstream in the process from the source are "detective" controls. Whether preventive or detective, controls are evaluated in terms of their effectiveness in reducing the process risks to an acceptable level.

71. How are risks identified?

Risks are identified using objectives as a framework. When evaluating internal control over financial reporting, these objectives are sometimes referred to as assertions. For example, COSO provides the following assertions that underlie an entity's financial statements:

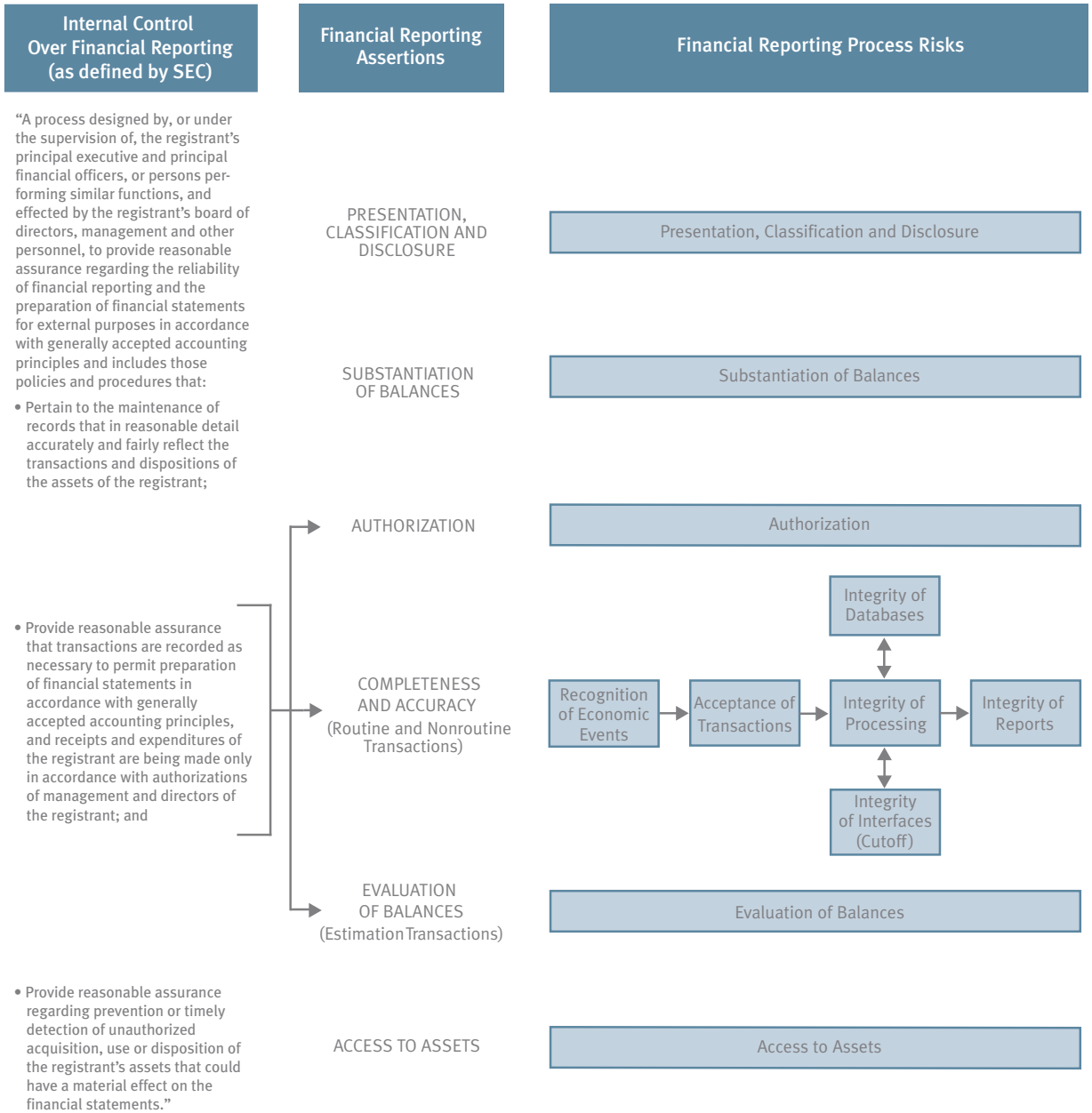
- ***Existence*** – Assets, liabilities and ownership interests exist as of a point in time.
- ***Occurrence*** – Recorded transactions represent economic events that actually occurred during a stated period of time.
- ***Completeness*** – All transactions and other events and circumstances that occurred during a specific period, and should have been recognized in that period, have, in fact, been recorded or considered. Therefore, there are no unrecorded assets, liabilities or transactions, and no omitted disclosures.
- ***Rights and Obligations*** – Assets and liabilities reported on the balance sheet are bona fide rights and obligations of the entity as of that point in time.
- ***Valuation or Allocation*** – Assets, liabilities, revenues and expenses are recorded at appropriate amounts in accordance with relevant accounting principles.
- ***Presentation and Disclosure*** – Items in the statements are properly described and classified as well as fairly presented.

When analyzing the critical routine processes (see Questions 66 and 67), the project team should identify and understand the flow of the significant transaction streams where economic events are recognized, transaction data are accepted, transaction data are processed and the results of processing are reported. When analyzing unusual or nonroutine transactions and estimation transactions, the team should examine the underlying methodologies, assumptions, supporting data sources and review processes. The PCAOB has stated that the auditor's evaluation may be based on assertions other than the ones listed above so long as there is testing of the controls over the pertinent risks in each significant account and disclosure that could result in a material misstatement in the financial statements.

Likewise, management must use assertions that have a reasonable bearing as to whether the significant accounts are fairly stated. Therefore, the above assertions (or alternative assertions – see Question 72, for example) are used to identify points within the transaction process, estimation methodology or disclosure generation process where things can go wrong that could lead to a material misstatement. The Section 404 compliance team should determine the sources and potential likelihood of material misstatements in each significant account. These sources of risk provide the focal point for evaluating controls to provide reasonable assurance that the relevant assertions are being met.

72. What are control objectives and how do they relate to risks?

Statements of objectives and statements of risks are often "mirror images" of each other. One approach in formulating useful financial reporting assertions is to build on the objectives for financial reporting that are implicit in the SEC's definition of internal control over financial reporting, as cited in its final rules on Section 404. As the following illustrates, this definition gives rise to financial reporting assertions and provides a context for examining any process in terms of "what can go wrong."



The objectives of financial reporting are converted into financial reporting assertions. These assertions are then used to articulate relevant financial reporting process risks when evaluating processes. The "Financial Reporting Process Risks" may be stated in the form of risks or as control objectives.

Note that "completeness and accuracy" is broken down into more granular assertions relating to the initiation, acceptance, recording, processing and reporting of transactions. For example, "processing" is reflected in integrity of databases, processing and interfaces. Interfaces are particularly important as they represent the "hand-offs" between units and processes. Intercompany transactions, related party transactions, transfer pricing issues, and transfers between processes and functions must be understood and controlled, because they create processing issues requiring careful attention.

For examples of financial reporting assertions from the COSO framework, see Question 71. Some companies selected these alternative assertions or similar assertions prior to the release of standards by the PCAOB. While Auditing Standard No. 5 reinforces the assertions defined in Question 71, the PCAOB also indicated that those assertions are not absolute requirements. As long as the assertions used are defined in a manner so they are in effect equivalent to the COSO assertions, they are acceptable for use now and in the future. Thus, the message is one of flexibility. That said, for companies just getting started, we recommend the use of the COSO assertions provided in Question 71.

73. How are control objectives defined?

Our responses to Questions 71 and 72 illustrate the use of financial reporting objectives or assertions for purposes of focusing an evaluation of internal control over financial reporting. These assertions may be defined more specifically as objectives in the context of a process or, alternatively, they may be defined more granularly in the form of specific risk statements (i.e., risks to the achievement of the assertions). In practice, the more specific objectives related to an assertion and the granular risks related to an assertion are often "mirror images" of each other. Therefore, we see some variability in practice with some companies evaluating controls in the context of achieving objectives and others in the context of mitigating risks. Either approach gets the job done, provided they are appropriately linked to the relevant financial reporting assertions.

Management also may choose to expand the project beyond financial reporting to consider other categories of objectives. For example, management may decide to consider such other objectives as operational effectiveness and efficiency and compliance with applicable laws and regulations.

If an expansion to other categories of objectives is intended, the project team will need to obtain information about entity- and activity-level objectives. This input can come directly from management. Alternatively, it can come from reviewing the key performance measures or indicators that are used in the business to execute the business strategy and identify performance gaps. A balanced family of measures cascading down through the organization and used to manage and run the business can provide a useful context. Management can use these measures to formulate sufficiently granular control objectives that extend beyond financial reporting.

Integrating Fraud Considerations Into the Assessment

74. What is the scope of an anti-fraud program and controls?

An anti-fraud program and controls are those controls related to the prevention, deterrence and detection of fraud. In the context of Sarbanes-Oxley, they are the controls that are intended to mitigate the risk of fraudulent actions that could have an impact on financial reporting. Examples include:

Fraudulent financial reporting	Inappropriate earnings management or "cooking the books" – e.g., improper revenue recognition, intentional overstatement of assets, understatement of liabilities, etc.
Misappropriation of assets	Embezzlement and theft that could materially affect the financial statements
Expenditures and liabilities incurred for improper or illegal purposes	Bribery and influence payments that can result in reputation loss
Fraudulently obtained revenue and assets and/or avoidance of costs and expenses	Scams and tax fraud that can result in reputation loss

The SEC provides that there be a sourcing of the risks within the processes at which a material misstatement, including a misstatement due to fraud, can occur. In addition, the Commission requires an evaluation of the controls specifically intended to address these risks. The approach to evaluating the design and operating effectiveness of the anti-fraud program is no different than it is for other controls, except that the focus under Section 404 is primarily on management fraud and the risk of management override of controls. The SEC's interpretive guidance for management states:

> [O]ne type of fraud risk … is the risk of improper override of internal controls in the financial reporting process. While the identification of a fraud risk is not necessarily an indication that a fraud has occurred, the absence of an identified fraud is not necessarily an indication that no fraud risks exist. Rather, these risk assessments are used in evaluating whether adequate controls have been implemented.

This evaluation takes place at the company level because the control environment includes, but is not limited to, controls specifically established to prevent and detect fraud that is reasonably possible to result in a material misstatement of the financial statements. It also takes place at the process level with the identification of specific controls that mitigate the risk of material fraud within key processes. See Question 81 for additional discussion of the entity-level assessment and its impact on the assessment conducted at the process level.

75. What's new and what really matters with respect to fraud?

There is relatively little new with respect to the nature and causes of fraud itself. However, the fraud regulatory environment has changed dramatically, elevating expectations of management and auditors to be more vigilant about fraud risk and of audit committees to focus on the risk of management override of established controls. Authoritative guidance – including Sarbanes-Oxley, Statement on Auditing Standard (SAS) 99, the SEC, the Federal Sentencing Guidelines as well as others – emphasize the need for stronger anti-fraud programs and related controls. For example, Sarbanes-Oxley sets the expectation for reliable financial reporting. SAS 99 sets requirements for external auditors to consider fraud in the execution of a financial statement audit. In Auditing Standard No. 5, the PCAOB makes the consideration of fraud more explicit during the assessment of internal control over financial reporting. For example, the Board states that "the risk that a company's internal control over financial reporting will fail to prevent or detect misstatement caused by fraud usually is higher than the

risk of failure to prevent or detect error." This point resonates with investors who are likely to be much more concerned with deliberate errors in the financial statements with the intent to deceive than with unintentional errors and oversights. Finally, the Federal Sentencing Guidelines have been enhanced and underscore the importance of ethics and compliance programs – a key component of many organizations' anti-fraud initiatives. Corporate fines have been substantially increased, and stiff jail terms have been set for obstruction of justice and securities fraud.

The SEC states in its interpretive guidance that "management's evaluation of the risk of misstatement should include consideration of the vulnerability of the entity to fraudulent activity (for example, fraudulent financial reporting, misappropriation of assets and corruption) and whether any such exposure could result in a material misstatement of the financial statements." In Auditing Standard No. 5, the PCAOB also clarifies that the focus on fraud, from a financial reporting context, is directed to matters that could result in a material misstatement of the financial statements. It is within this context that management has the responsibility to prevent, deter and detect fraud. If there are deficiencies in the anti-fraud program and related fraud controls, the external auditor is likely to consider them at least a significant deficiency in internal control over financial reporting. Furthermore, the Sarbanes-Oxley and revised NYSE and NASDAQ listing requirements as well as Auditing Standard No. 5 all place greater responsibility on audit committees to provide oversight with respect to financial reporting and internal control over financial reporting. This oversight extends to reporting, documentation, investigation, enforcement and remediation related to fraud.

The SEC's and PCAOB's underlying premise is that the absence of fraud does not necessarily mean that fraud risk does not exist. There is a presumption that most companies face some degree of fraud risk. Therefore, companies of all sizes should have controls to prevent and detect management override.

For many companies, the anti-fraud model:

- Is often narrowly focused on industry fraud risks (e.g., retail shrinkage, healthcare/Medicare fraud, and similar matters);
- Is frequently reliant on "silo" management techniques in which the responsibility for managing fraud resides in a "silo" separate from all other key organizational functions; and
- Leaves the responsibility to mitigate fraud to middle managers who maintain autonomy and are not held accountable except for third-party fraud.

Differentiating the Role of Management and the Audit Committee

The above model is inadequate to address regulatory expectations in the post-Sarbanes-Oxley world. While there is no "one-size-fits-all" approach to managing fraud risk – and the various regulations allow for some flexibility in approach – companies need an effective anti-fraud program that will enable the evaluation, mitigation and monitoring of fraud risk. To be successful, senior management must be involved in supervising the program, and the audit committee must provide appropriate oversight. Management must be prepared to demonstrate they have developed an effective anti-fraud program. Following are attributes of an effective program:

- There should be strong emphasis on creating a culture of honesty and high ethics, evaluating anti-fraud processes and controls, and developing an appropriate oversight process.
- Both management and the audit committee are focused on an effective anti-fraud program. Management generates – and the audit committee actively reviews – reports evidencing effective operation of the anti-fraud program.
- Ineffective "silo" management of fraud risk is eliminated as the fraud risk focus is broadened and integrated with other aspects of the business. For example, a sustainable fraud risk assessment is conducted and includes consideration of vulnerabilities across the enterprise and within business units, geographies and the industry.

- Audit committee, board, external auditors, internal audit and other advisors collaborate on a regular basis to ensure the anti-fraud program is effective and meets the requirements of all applicable regulations, laws and rules.

Ineffective oversight by the audit committee of the company's financial reporting process (and the related internal controls) is an indicator of a material weakness. Paragraph 25 of Auditing Standard No. 5 requires the external auditor to "assess … whether the board or audit committee understands and exercises oversight responsibility over financial reporting and internal control."

An effectively functioning audit committee augments the "tone at the top" that is so vital to an effective control environment. The SEC expects the audit committee, as part of its oversight responsibilities for the company's financial reporting, to be knowledgeable and informed about the Section 404 evaluation process and management's assessment results. The audit committee should ensure that a rigorous evaluation is conducted to address fraudulent reporting risk, including the risk of management override in the financial reporting process. In exercising its oversight role, the committee should review management's overall summary documentation articulating the overall approach to and the results of the Section 404 assessment process.

76. What suggested steps should management take with respect to fraud?

Following is a list of 10 suggested steps for management:

- ***Ascertain comprehensiveness of the program.*** Determine that the anti-fraud program has all requisite elements. For example, does the program have the key elements of an ethics and compliance program, as outlined in the Federal Sentencing Guidelines? Does it consider the key elements of SAS 99, The IIA fraud practice advisories and the AICPA Fraud Task Force Antifraud Program Guidelines? Does the program involve all key business processes, business units and divisions that significantly impact financial reporting? Are the key fraud risks identified and prioritized on a periodic basis? Is there an effective pre-employment screening process? Is there segregation of duties? Is there due diligence with respect to suppliers and business partners? Does management determine whether the anti-fraud program is integrated throughout all new acquisitions and expansion efforts of the organization? These and other questions facilitate the assessment of the anti-fraud program to ensure it is sufficiently comprehensive.
- ***Maintain tone at the top.*** Evaluate the evidence of tone at the top, including the policies and processes prohibiting management override of established controls. For example, does senior management actively support the anti-fraud program efforts? Is there consistency in the way the code of conduct is enforced across all locations and units? Are there controls over nonroutine transactions? Are company-level controls adequately documented? Do company-level controls include codes of conduct and fraud prevention that apply to all locations and units?
- ***Assess fraud risk.*** Determine the specific industry, geographic and other relevant fraud risks and ensure the anti-fraud program addresses these risks appropriately. What are the specific industry fraud risks? What are the geography-specific fraud risks (e.g., risks pursuant to the Foreign Corrupt Practices Act)? Fraud risks may be assessed using a scenario approach, by evaluating risks with specific processes and by considering applicability of relevant fraud risk indicators. See Question 77 for further discussion of these approaches.
- ***Identify mitigating controls.*** Does the anti-fraud program consider the identified fraud risks? For example, controls should be linked to specific fraud risks identified at both the entity and process levels. With regard to the design of controls, a company's documentation should encompass the design of controls to prevent or detect fraud, including who performs the controls and the related segregation of duties.
- ***Conduct fraud testing.*** Management must determine the controls that should be tested, including the anti-fraud program and controls. Internal audit activity relating to fraud should be adequate, and the internal audit function should report directly to the audit committee. The audit committee should demonstrate an adequate

level of involvement and interaction with internal audit on fraud matters. With respect to the external auditor, the PCAOB states in Auditing Standard No.5 that the controls evaluation should consider "whether the company's controls sufficiently address identified risks of material misstatement due to fraud and controls intended to address the risk of management override of other controls." The Board lists the following controls that might address these risks:

- Controls over significant, unusual transactions, particularly those that result in late or unusual journal entries
- Controls over journal entries and adjustments made in the period-end financial reporting processes
- Controls over related party transactions
- Controls related to significant management estimates
- Controls that mitigate incentives for, and pressures on, management to falsify or inappropriately manage financial results

Management and the audit committee should also focus on these controls to ensure that they are in place and operating effectively.

- ***Maintain effective code of conduct.*** Documentation of the code of conduct provisions should exist, especially those related to conflicts of interest, related party transactions, illegal acts and the monitoring of the code by management and the audit committee or board. If there is a code, is it public? Is it communicated adequately throughout the organization? Is it periodically reinforced? Is it enforced consistently?
- ***Exercise anti-fraud program oversight.*** Fraud needs to be on the agenda of audit committee meetings, disclosure committees and fraud program management at appropriate times. There should be clear documentation of such considerations to establish the viability of the anti-fraud program.
- ***Identify and investigate complaints.*** There should be adequate procedures for handling complaints and for accepting anonymous, confidential submissions of concerns about questionable accounting or auditing matters. Determine whether the audit committee has established procedures to handle anonymous, confidential complaints and submissions regarding financial reporting and/or audit irregularities. Is there a "whistleblower" process in place in accordance with Sarbanes-Oxley Section 301? How are concerns or complaints reported directly through the chain of command captured, elevated and addressed? What is the frequency of reported frauds? Is there a procedure in place to ensure that investigations (both internal and independent) are conducted in a timely, efficient and consistent manner? Do corrective and remediation activities address the root cause(s) of misconduct? What testing is conducted to determine if fraud is reported, investigated and resolved in the manner described in the anti-fraud program?
- ***Remediate deficiencies.*** When deficiencies in the anti-fraud program are identified, they should be remedied in a timely manner.
- ***Consult with advisors.*** Management should consult with legal advisors, fraud specialists and the external auditors as the company documents, evaluates and refines the anti-fraud program.

77. How are fraud risks assessed?

There are at least three approaches for considering implications of fraud to financial reporting: common scenarios, process-by-process and fraud indicators. Management can use all of these approaches when evaluating fraud risk.

When using the "common scenarios" approach to conduct a fraud risk assessment, management's approach is to first identify relevant scenarios that potentially could occur within the organization, resulting in a material impact on the financial statements. For each identified scenario, either internal audit or the Section 404 compliance team describes how the scenario would be perpetrated within the company, the individuals who could make it happen and the financial statement accounts that would be affected. Based on the documented

scenarios, the team then identifies the controls that would prevent, deter or detect each scenario. These controls documented through this step would be compared with the controls in place, and gaps would be identified. An action plan would be developed to remediate significant gaps.

When using the "process-by-process" approach to document the anti-fraud program and controls, management should identify and document the points within each significant process where a misstatement – including a misstatement due to fraud – related to each relevant financial statement assertion could arise. Then management must identify and document the controls that have been implemented to address these potential misstatements. Risk and Control Matrices (RCMs) can be useful in this regard. For example, the Section 404 compliance team can review the RCMs to ascertain whether the fraud risks already identified are complete. When applying this approach, remember it is important to move beyond third-party fraud to consider risk of management override, particularly in the financial close process and in nonroutine and estimation processes.

Finally, there are fraud risk indicators that provide risk considerations for management to use when developing a sustainable fraud risk assessment approach. These indicators can be used to facilitate gathering of fraud risk factor information and serve as a guide for dialogue (or "brainstorming") with relevant individuals at the entity and process levels. While not conclusive, the existence or absence of risk indicators within a company may provide insights as to the appropriate scope of fraud monitoring, testing and oversight.

78. How should management get started with integrating fraud considerations into the Section 404 assessment?

We suggest management consider three key words: "Make fraud explicit." Make fraud explicit in the company's risk assessment and controls design and testing. Make fraud explicit during the entity-level controls assessment. Make it explicit during the review of the financial reporting process and when identifying assertion risks at the process level.

The fraud area is important because insufficient attention could put a company at risk of significant deficiencies or material weaknesses. There should be sufficient focus directed to the risk of management override of controls. The company's anti-fraud program also should be integrated with the overall governance process.

When evaluating mitigating controls at the process level, companies should begin the process of understanding the incremental steps to complete the Section 404 assessment so it is fully responsive to the requirements and expectations relating to the "anti-fraud program and controls." If this process has not begun, we recommend that management get started by taking two steps:

- Determine from the external auditors their expectations and requirements.
- Inventory the elements of an anti-fraud program currently in place and under development.

These two steps will enable management to conduct a "gap analysis" and determine whether amendments to the Section 404 project plan are necessary. Following are additional steps after completion of the two initial steps above:

- If not already completed, conduct a fraud risk assessment.
- Identify gaps in the company's anti-fraud program and controls.
- Provide a checkpoint to the external auditors to assess the process and provide input on the development of the action plan.
- Develop an action plan and determine amendments to the project plan.
- Execute the action plan.

The approach to evaluating the design and operating effectiveness of an anti-fraud program and related controls is no different than it is for other controls. In fact, many elements of the anti-fraud program and controls

are often already in place. Many companies are implementing other elements of the anti-fraud program and controls, e.g., initiatives relating to Sarbanes-Oxley Sections 301, 406 and 806. The documentation of controls on risk and control matrices often identify some controls that serve a dual purpose of mitigating risks of inadvertent and intentional errors. All told, fraud prevention and deterrence and the mitigation of related financial reporting risks must become a more active part of the management and audit committee agenda.

Identifying, Documenting and Assessing Controls

79. What are the primary sources of the SEC's guidance to management for purposes of evaluating internal control over financial reporting?

Yes. There are two primary sources of guidance. First, the SEC's final rules provide general guidance:

- The methods of conducting evaluations of internal control over financial reporting will, and should, vary from company to company. For example, the nature of a company's testing activities will depend largely on the circumstances of the company and the significance of the control.
- The assessment of a company's internal control over financial reporting must be based on procedures sufficient both to evaluate its design and to test its operating effectiveness. Controls that will require testing include, among others:
  - Controls initiating, authorizing, recording, processing and reconciling account balances, classes of transactions and disclosure and related assertions included in the financial statements
  - Controls related to the initiation and processing of nonroutine and nonsystematic transactions
  - Controls related to the selection and application of appropriate accounting policies
  - Controls related to the prevention, identification and detection of fraud
- Inquiry alone generally will not provide an adequate basis for management's assessment.

Second, the SEC has published interpretive guidance providing more granular guidance on the following topics relating to the evaluation process:

- Identifying financial reporting risks and controls
  - Identifying financial reporting risks
  - Identifying controls that adequately address financial reporting risks
  - Consideration of entity-level controls
  - Role of general information technology controls
  - Evidential matter to support the assessment
- Evaluating evidence of the operating effectiveness of internal control over financial reporting
  - Determining the evidence needed to support the assessment
  - Implementing procedures to evaluate evidence of the operation of internal control over financial reporting
  - Evidential matter to support the assessment
- Multiple location considerations

We have incorporated aspects of this guidance into this publication, and we strongly recommend companies review and understand it.

80. Does the SEC provide any guidance to management for purposes of documenting its evaluation of internal control over financial reporting?

Yes. The SEC's final rules provide the following general guidance:

- In conducting an evaluation and developing its assessment of the effectiveness of internal control over financial reporting, a company must maintain evidential matter relating to both the design process and the testing process. This documentation must provide reasonable support for management's assessment of the effectiveness of the company's internal control over financial reporting. Developing and maintaining such evidential matter is an inherent element of effective internal controls.
- An instruction to Item 308 of Regulations S-K and S-B and Forms 20-F and 40-F reminds registrants to maintain evidential matter.
- Evidential matter, including documentation, must support the assessment of both the design of internal controls and the testing processes. This evidential matter should provide reasonable support:
  - For the evaluation of whether the control is designed to prevent or detect material misstatements or omissions
  - For the conclusion that the tests were appropriately planned and performed
  - That the results of the tests were appropriately considered

The Commission's interpretive guidance also explains the nature and extent of evidential matter that management must maintain in support of its assessment, including how management has flexibility in approaches to documentation. The basic premise of the guidance is the same as expressed in the final rules; i.e., management's assessment must be supported by evidential matter. That evidential matter must provide reasonable support for management's assessment of internal control over financial reporting. The SEC indicates that "reasonable support for an assessment would include the basis for management's assessment, including documentation of the methods and procedures it utilizes to gather and evaluate evidence." Documentation of the design of key controls is an integral part of that support. To illustrate, the Commission's interpretive guidance provides the following example:

> [M]anagement may document its overall strategy in a comprehensive memorandum that establishes the evaluation approach, the evaluation procedures, the basis for management's conclusion about the effectiveness of controls related to the financial reporting elements and the entity-level and other pervasive elements that are important to management's assessment of [internal control over financial reporting]. If management determines that the evidential matter within the company's books and records is sufficient to provide reasonable support for its assessment, it may determine that it is not necessary to separately maintain copies of the evidence it evaluates. For example, in smaller companies, where management's daily interaction with its controls provides the basis for its assessment, management may have limited documentation specifically for the evaluation of [internal control over financial reporting]. However, in these instances, management should consider whether reasonable support for its assessment would include documentation of how its interaction provided it with sufficient evidence.

The nature of the evidential matter may vary based on the assessed level of risk and other circumstances. However, the SEC's comments above suggest there are some minimum expectations as to what constitutes "reasonable support." The Commission's interpretive guidance asserts that the evidential matter provide the basis for management's conclusions about the controls related to individual financial reporting elements.

Points made by the interpretive guidance regarding documentation include the following:

- ***Recognize that the form and extent of documentation will vary depending on the size, nature and complexity of the company.*** For example, the SEC points out that in smaller companies, management's daily interaction with its controls may provide the basis for its assessment in specific areas. In such instances,

"management may have limited documentation created specifically for the evaluation of [internal control over financial reporting]." Management should consider whether reasonable support for its assessment in these instances would include "documentation of how its interaction provided it with sufficient evidence," such as memoranda, e-mails, and instructions and other correspondence between management and company employees. In addition, the evidential matter will vary depending on the assessed level of risk. To determine the evidence needed to support the assessment for a given financial reporting element, the SEC is of the view that management should consider both the materiality of the financial reporting element and its susceptibility to a material misstatement.

- ***Recognize that documentation can take many forms.*** Documentation may consist of paper documents and electronic or other media, and it can be presented in a number of ways (e.g., policy manuals, process models, flowcharts, job descriptions, documents, internal memorandums, forms, etc.).
- ***Document only the controls that matter.*** The documentation supporting management's assessment does not need to include the entire population of controls that exists within a process that impacts financial reporting. The documentation should be focused on those controls that management concludes are adequate to address the identified financial reporting risks.
- ***Accomplish other important internal control-related objectives through documenting controls design.*** In addition to providing support for the assessment of internal control over financial reporting, the SEC's guidance asserts that documentation of the design of controls "serves as evidence that controls within [internal control over financial reporting], including changes to those controls, have been identified, are capable of being communicated to those responsible for their performance, and are capable of being monitored by the company." The guidance also requires that there be evidential matter, including documentation, of the "entitywide and other pervasive elements of [internal control over financial reporting] that [the company's] chosen control framework prescribes as necessary for an effective system of internal control."
- ***Consider the entity-level controls in place when evaluating the extent of evidence needed.*** The existence of entity-level controls may influence management's determination of the evidence needed to sufficiently support its assessment. For example, if management determines that there is a strong control environment, management may consider this conclusion when determining the evidence needed to evaluate whether a particular control is operating effectively. If management believes that an entitywide control addresses a specific financial reporting risk, then the company's reasonable evidential matter would ordinarily include documentation of how management reached that conclusion.
- ***Recognize that reliance on management's daily interaction impacts the level of documentation available.*** The guidance indicates that in those situations in which management is able to rely on its daily interaction with its control processes as the basis for its assessment, "management may have limited documentation created specifically for the evaluation of [internal control over financial reporting]" in addition to "documentation regarding how its interaction provided it with sufficient evidence."

The independent accountant can also impact a company's documentation practices. Auditors ordinarily require documentation to complete an audit of internal control over financial reporting. If there is inadequate documentation of management's assessment process, the auditor will be forced to create appropriate supporting documentation to provide evidence supporting an opinion on the effectiveness of internal control over financial reporting. The absence of a trail for the auditors can be costly. Thus, it would be wise to obtain input from the auditor at an early stage of the project regarding his or her expected documentation standards.

81. How and why are entity-level controls assessed?

Entity-level controls form an important foundation for management's assessment of internal control over financial reporting. Using a top-down approach, an entity-level control assessment should be conducted as early as possible in the Section 404 evaluation process and should never be an afterthought. If there are significant issues with respect to entity-level controls, they should be surfaced and corrected as soon as possible. If entity-level

controls are strong with effective analytics and monitoring applied in specific areas affecting significant financial reporting elements, that fact should be considered in the scope-setting stage of the project. Such controls could reduce reliance on process controls and reduce testing requirements.

The SEC's interpretive guidance states that "entity-level controls may be designed to operate at the process, application, transaction or account level and at a level of precision that would adequately prevent or detect on a timely basis misstatements in one or more financial reporting elements that could result in a material misstatement of the financial statements." There are other entity-level controls comprising the control environment (e.g., the tone at the top and entitywide programs such as codes of conduct, background checks and fraud prevention). Some entity-level controls that do not operate at the process, application, transaction or account level – such as controls to monitor results of operations – may be designed to identify possible breakdowns in lower-level controls. However, being only indirectly related to financial reporting elements, these controls, by themselves, may not be effective at preventing or detecting a misstatement in a financial reporting element. Therefore, while management ordinarily would consider entity-level controls of this nature when assessing financial reporting risk and evaluating the adequacy of controls, it is unlikely management will identify only this type of control as adequately addressing a financial reporting risk identified for a particular financial reporting element.

A determination that the so-called "indirectly related" entity-level controls are weak can also present formidable issues for purposes of completing the assessment. The independent public accountant could view the existence of a strong entity-level control environment as a "pass/fail" or "go/no go" decision. Poor entity-level controls will drive an increase in reliance on lower level controls and, therefore, increase the auditor's testing requirements.

An entity-level assessment is broken down into four steps. These steps are discussed below:

Step 1: Determine the entity-level controls on which management can rely – The first step is to understand the entity-level controls currently in place. This phase entails understanding the control environment, the company's risk assessment process and the activities of the internal audit function, as well as identifying the entity-level analytics and other monitoring programs utilized by management. When understanding the control environment, management should consider the attributes provided by the selected internal control framework. For example, the COSO framework lists seven attributes for the control environment, such as integrity and ethical values, board and audit committee oversight, assignment of authority and responsibility, and human resources policies and practices. The control environment is important because it sets the tone at the top for internal control over financial reporting and is the foundation for designing effective controls over management override.

In this phase, it is appropriate to inventory the monitoring controls that the company already has in place. According to the SEC, entity-level controls also include centralized processes and controls, including shared services environments. Because these controls are entitywide in scope, they should be documented and understood if they impact significant financial reporting elements. Finally, the controls over the period-end financial reporting process should be understood and documented.

The scope of entity-level controls, as defined by the SEC, is a broad one. It includes controls over management override, self-assessment programs and policies addressing significant business control and risk management practices.

Step 2: Determine the significant financial reporting areas that are viable candidates for increased reliance on entity-level controls – In the prior step, management developed an understanding of the current state of entity-level controls. In this step, management must differentiate the entity-level controls that directly impact one or more significant financial reporting elements from those entity-level controls with only an indirect impact.

The theory is articulated as follows:

- If the entity-level controls, including monitoring controls, are tested as effective (i.e., they are well understood and applied by key employees and are reviewed by corporate and/or operating company management), management should carefully consider whether these entity-level controls directly impact a significant financial reporting element and, if so, alter the nature, timing and extent of independent tests of the transaction controls affecting that element.
- If entity-level controls are tested as ineffective and there is no effective monitoring in place, management must assess whether a higher level of testing at the transactional level is necessary to support a positive assertion in the internal control report and ensure that financial statements are not misstated.

The question often arises as to how management puts the above theory into practice. A "direct impact" means the control is effective in achieving one or more financial reporting assertions or, said another way, the control is effective in reducing one or more key financial reporting assertion risks (i.e., "what can go wrong"). This is an important distinction because only the entity-level controls that directly impact a financial reporting element represent controls on which management can rely in lieu of transaction processing controls. The remaining entity-level controls – those that are more pervasive in nature and generally comprise the control environment that sets the tone at the top – may not be relied upon *solely* to mitigate fully risks at the process, application and transaction levels. However, these pervasive controls may still be considered in establishing testing scopes and in determining the overall extent of the evidence management gathers with respect to a particular financial reporting element.

The following summary illustrates the different categories of entity-level controls, as defined by the SEC, and shows which ones could have a direct impact on financial reporting elements:

	Impact of Controls on Significant Financial Reporting Elements	
Examples of Entity-Level Controls	**Directly Related**	**Indirectly Related**
Control environment • Management's philosophy and operating style • Integrity and ethical values • Board and audit committee oversight • Assignment of authority and responsibility • Human resources policies and practices • Commitment to competence • Organizational structure		●
Controls over management override		●
The company's risk assessment process		●
Centralized processes and controls, including shared services environments	●	
Controls to monitor results of operations	●	●
Controls to monitor other controls • Activities of the internal audit function • Activities of the audit committee • Self-assessment program	●	●
Controls over the period-end financial reporting process	●	●
Policies addressing significant business control and risk management practices	●	●

Note that the various elements of entity-level controls defined by the SEC are reasonably aligned with the five COSO components. This is important because the COSO framework requires an assessment at the entity level and at the process level. For purposes of complying with Section 404, we believe that consideration of the

various categories of entity-level controls, as defined by the SEC, are sufficient for purposes of conducting an overall entity-level control assessment, as required by the COSO framework.

In addition, note that most of the entity-level controls that impact the significant financial reporting elements will be monitoring controls. Starting with an inventory of the monitoring controls currently in place, management should link these controls to financial reporting elements using three categories:

(1) Controls that can be relied upon, *as currently designed*, for purposes of mitigating relevant financial reporting assertion risks

(2) Controls that can be relied upon, *with design improvements*, for purposes of mitigating relevant financial reporting assertion risks

(3) Financial reporting elements for which there are opportunities to design effective monitoring controls, *which currently do not exist*

This approach will enable management to identify the "low hanging fruit" and separate those monitoring controls that are "reliance ready" at the present time from those controls that require improvement. This process also helps management understand how the entity-level controls they currently have in place can impact the Section 404 evaluation.

With respect to the entity-level controls that directly impact financial reporting elements, management must select only those controls that are designed effectively and test their operating effectiveness. For example, for monitoring controls to qualify as directly impacting significant financial reporting elements, they must be robust. To satisfy the test of "robustness," the controls must satisfy the following criteria:

- Operate at an acceptable level of precision (see discussion in Step 3)
- Be effective in preventing or detecting errors on a timely basis at the process, transaction or application level
- Be executed by the appropriate management
- Be documented and supported in reasonable detail with appropriate evidence
- Provide evidence that errors and other issues affecting the integrity of financial reporting are periodically identified and addressed timely

To illustrate, in low risk and relatively stable areas, a company may have effective monitoring activities through their monthly budget-to-actual comparison process and tracking key performance indicators where management reconciles operating and financial information utilizing its knowledge of the business and the price, volume and mix factors established during the budget process. In addition, management may also deploy a robust self-assessment process that is focused on evaluating the performance of specific process-level controls. These monitoring activities may give management confidence that the process owners understand the importance of internal control and that they can detect a material misstatement in financial reporting, should one arise. As a result, independent testing in these areas may be considered unnecessary.

In summary, management should begin with the areas that are most likely to be impacted by effective entity-level controls. One possible approach is to begin with lower risk areas, which are the areas where one would generally expect greater reliance on entity-level controls in lieu of a more granular focus on transaction processing controls. From there, the evaluation team progresses to higher risk areas.

Keep in mind that many monitoring controls are often dependent on the effectiveness of general IT controls. If general IT controls are not operating effectively, the data and reports used to support critical monitoring controls must be sourced and tested separately to justify reliance on them. That process can be time consuming and can be avoided with a strong general IT control environment.

Step 3: For each significant risk for which there is a direct impact, document the evidence that the specific entity-level control reduces the risk – When documenting the controls that mitigate each significant process-level risk, consider first the controls in the inventory of entity-level controls, as discussed in the previous step. Look for evidence that the entity-level control(s) set a strong "tone at the top" and operate at an appropriate level of precision. To illustrate, an "appropriate level of precision" means the control does the following:

- It is designed to perform at an appropriate error threshold, i.e., it is designed to detect errors of an amount lower than the established planning materiality.
- It consistently identifies variances, anomalies, out-of-balance conditions and other instances at a sufficiently granular level, which may be indicative of potential errors or omissions.
- It prompts investigation in instances where potential errors or omissions are identified.
- It closely monitors any investigation to ensure timely completion, and results in timely identification and correction of errors and omissions before financial reports are issued to the public.
- It establishes accountability for results with a clearly described process, robust documentation standards and evidence of periodic performance.

Step 4: Review the entity-level control reliance plan with management – Management should be comfortable with reliance on entity-level controls in lieu of transaction processing controls in specific areas. In reviewing the plan with management, consider the precision of the selected entity-level controls, the priority management places on the control, the changes in scope from the prior year and the evidence of direct impact on relevant financial reporting assertions. In addition, consider the track record for identifying, investigating and correcting errors and omissions. Finally, discuss the plan with the external auditor.

When summarizing the impact of entity-level controls, the following points apply:

- The *absence* of entity-level controls having an *indirect effect* on significant financial reporting elements – the controls comprising the control environment, for example – *increases* the risk of control failure.
- The *existence* of entity-level controls having a *direct effect* on significant financial reporting elements – effective monitoring controls and entity-level controls designed to operate at a sufficient level of precision to prevent or detect material error or fraud at the process, application, transaction or account level, for example – *reduces* the scope of testing lower-level controls.

Note that reliance on an entity-level control for purposes of compliance with Section 404 does not mean elimination of reliance on transaction processing controls. In addition, a Section 404 evaluation is focused on compliance with Sarbanes-Oxley and reliable financial reporting, and does not address the other relevant business objectives that transaction processing controls might address.

82. How is an assessment of the design effectiveness of entity-level controls conducted?

In Question 81, we discuss how and why entity-level controls are assessed. In that question, we discuss the theory and basic approach to an entity-level control assessment and present the SEC's articulation of the various categories comprising these controls. In this question, we discuss more specifically how to assess the design effectiveness of these controls.

There are four steps to evaluating the design effectiveness of the control environment:

Step 1: Customize the assessment – The project team customizes the COSO framework to the organization's specific circumstances. This customization process can be accomplished using a tool developed by management or an outside firm. A useful tool is typically a diagnostic questionnaire linked to COSO components and attributes. Once the approach and customized diagnostic are developed, the evaluation approach and plan should be reviewed with the independent public accountant.

The five COSO components provide a framework for evaluating internal control over financial reporting at the entity level. However, it is important to understand that the SEC has defined the categories of entity-level controls for purposes of the Section 404 evaluation. The following table illustrates how the SEC's articulation relates to the five COSO components.

	COSO Component				
Examples of Entity-Level Controls	**Control Environment**	**Risk Assessment**	**Control Activities**	**Information/ Communication**	**Monitoring**
Control environment • Management's philosophy and operating style • Integrity and ethical values • Board and audit committee oversight • Assignment of authority and responsibility • Human resources policies and practices • Commitment to competence • Organizational structure	●		●	●	
Controls over management override	●		●	●	
The company's risk assessment process		●			
Centralized processes and controls, including shared services environments			●	●	
Controls to monitor results of operations				●	●
Controls to monitor other controls • Activities of the internal audit function • Activities of the audit committee • Self-assessment program				●	●
Controls over the period-end financial reporting process	●		●	●	
Policies addressing significant business control and risk management practices			●		

In our response to Question 41, we explain that for each COSO component, there are several attributes. For each attribute, there are points of focus. These terms must be understood to appreciate fully the following discussion. This thinking is particularly useful in organizing an evaluation of the design of the control environment that, as illustrated in the above table, is a subset of entity-level controls. It may also be useful when organizing the assessment of other entity-level controls.

Step 2: Assess the overall entity-level controls – The project team begins the assessment with an interview of the certifying officers (the CEO and CFO) to obtain their perspective regarding the controls at the entity level and, in particular, the control environment. This discussion is as much about validating the assessment approach as it is about conducting the assessment. For each "control unit" (see Questions 54 and 55 for explanation) within the organization, interviews should be conducted with unit management to assess the control environment as well as other entity-level controls that should be considered for purposes of management reliance (as discussed in Question 81). For the various points of focus for the control environment and for other entity-level controls, the project team should request input as to the nature and type of evidence that exists to support management's response that the stated controls are in place. As an additional step, the team may request selected members of

the management team to complete a self-assessment using the customized assessment tool. If there is a large survey population, the team should consider using web-based technology. As an additional alternative, the team should consider working with unit management through a facilitated workshop. However it is done, the objective is to document the attributes comprising the control environment and other controls in place at the entity level. Note that Question 81 provides illustrative points of focus regarding the evaluation of the design effectiveness of monitoring controls.

Step 3: Gather supporting evidence – The project team should develop and execute a plan to obtain, document and assess relevant supporting evidence of controls at the entity level. For example, an overall assessment of the control environment is often subjective and requires considerable judgment. Assessments that lead management and other personnel to conclude that a given attribute is effective require supporting evidence. When evaluating the attributes of the control environment, the project team may consider risk indicators that suggest the existence or the absence of financial reporting risk, e.g., whether there is a dominant CEO, whether senior executives live flamboyantly, if performance expectations are unrealistic, whether investments and loans are concentrated in high-risk areas, if management accepts significant risks or generates returns that are unusual in the industry, and so on. However, the assessment of risk indicators is more subjective than the assessment of policies, processes, competent people, reports, methodologies and systems, all of which are more susceptible to independent validation.

When evaluating entity-level controls having a direct impact on significant financial reporting elements, as discussed in Question 81, management's rationale for the direct impact needs to be carefully documented. That "rationale documentation" is important because it will provide a context for the evaluation of design effectiveness.

Step 4: Formulate the conclusion with respect to design effectiveness – When all assessments of entity-level controls (including the control environment) are completed, management evaluates the combined results and concludes as to the effectiveness of each of the COSO components at the entity level. The project team should ascertain that management's overall conclusion is supported by the findings on the various attributes and the evidence obtained supporting those attributes (see Question 41 for further explanation). The overall results and documentary evidence as to design should be validated to ensure that the controls are operating effectively (see next question).

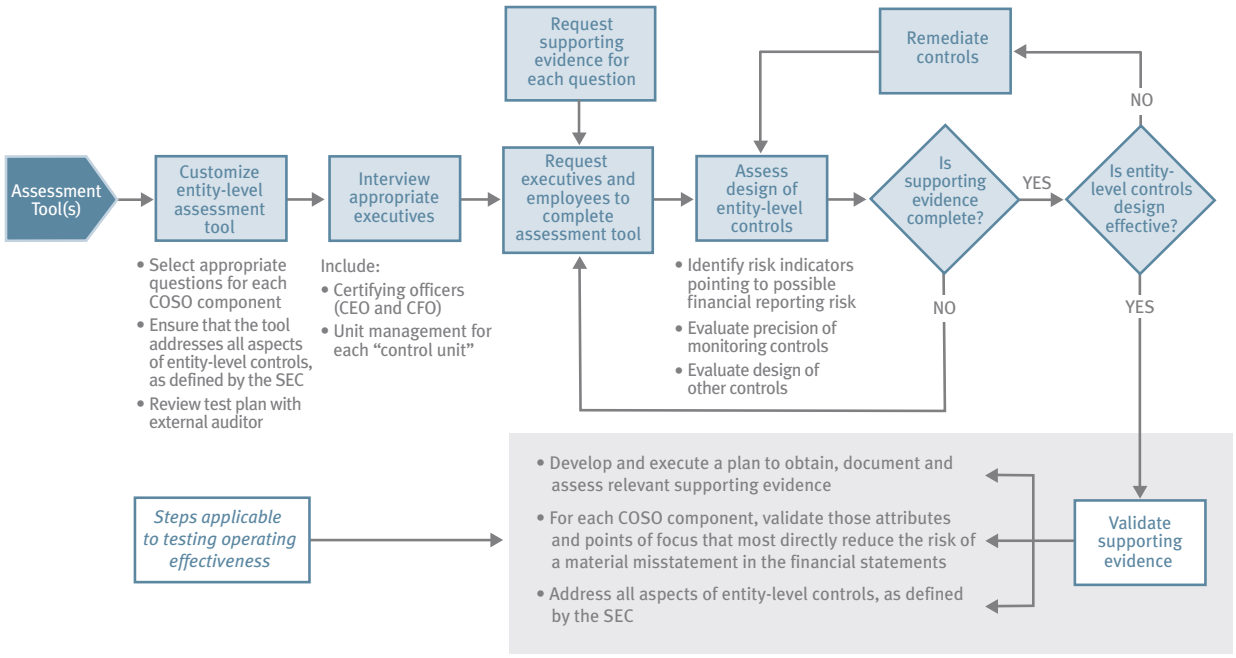
Based on the results of the assessment and validation activities, a conclusion that the entity-level controls are effective as to design may reduce the need to document processes, risks and controls in less significant areas where there isn't a reasonable possibility for a material misstatement. Negative assessments about the entity-level controls, however, require careful consideration. Such assessments may be an indication of one or more significant deficiencies or material weaknesses in internal control. Management should communicate these conditions to the audit committee and independent public accountant.

As discussed in Question 81, when the entity-level review of design effectiveness is completed, management should review the overall conclusion, the underlying support and the implications to the control assessment at the process level with the independent public accountant. Communicating results with the independent public accountant at periodic checkpoints reduces the risk of surprises later.

83. How is the operating effectiveness of entity-level controls validated?

Validation is the process of determining that effectively designed internal controls are functioning as intended. Validation consists of the specific steps to assess the operating effectiveness of the control environment and other entity-level controls. Validation is not a one-time event but a continuous and ongoing process and, depending upon the nature of the control, a judgmental process.

Following is an approach to evaluating entity-level controls:



The Section 404 compliance team should validate effective operation as soon as possible after concluding on design effectiveness. Ultimately, management must be prepared to address the question, "What evidence supports your conclusion that the entity-level controls are operating effectively?" If management chooses not to validate all entity-level controls due to personal knowledge and the extent of daily interaction with the controls, management may want to at least consider selective testing of attributes of the control environment with respect to points of focus they may not be sure about, e.g., background checks. If there is a weak company-level environment that can't be remediated in a timely manner, more testing may be necessary at the process level.

How does the project team validate the so-called "soft controls" that often define certain aspects of the control environment as part of the entity-level controls evaluation (e.g., management's philosophy and operating style, integrity and ethical values, etc.)? Granted, it is difficult to perform an objective test of tone at the top-type controls. There is significant subjectivity involved in making this evaluation. That also is why the project team should have a discussion with management as to what they want to do in validating the entity-level controls. Management should weigh in on the following questions:

- Is management satisfied that:
  - The control environment is strong and delivers the right tone, given management's daily interaction with the controls and with the personnel responsible for executing the controls?
  - There are clearly articulated policies addressing significant business control and risk management practices?
  - The aforementioned policies are understood? If so, how does management know?
  - The company's risk assessment process is performing as intended?
  - The activities of the company's internal audit function are effective in monitoring critical financial reporting control activities?
  - The company's self-assessment program is effective in monitoring critical financial reporting control activities?

- What are the hard spots (the areas that are working well) and how does management know?
- What are the soft spots (the areas that are not working well) and should they be corrected? If so, when will they be corrected?
- Is there sufficient documentation supporting a conclusion that:
  - Centralized processes and controls, including shared services environments, affecting significant financial reporting elements are operating effectively?
  - Controls over the period-end financial reporting process are operating effectively?
- Finally, do the activities of the audit committee and the checks and balances in place to provide controls over management override function as intended? (Note that the audit committee must also weigh in on this important question.)

Many potential issues can be addressed with this dialogue. On both practical and economic grounds, management may want to be selective in deciding the validation activities that are necessary for its purposes. There are several factors to consider when validating entity-level controls.

- There are four types of testing: inquiry, observation, inspection and reperformance. Reperformance is often not an option for many entity-level controls, e.g., many attributes of the control environment, the company's risk assessment process, etc. Therefore, the project team is left with inquiry, observation and inspection. Thus, inquiries of key personnel, observation of management actions, and inspection of written policies and documents are things the evaluator often does at the entity level.
- Management should choose to validate only areas where validation is appropriate. It is not necessary to validate every single control at this or at any other level. The focus should be on the most critical controls with the highest risk of performance failure.
- One approach to validation at this level is the absence of risk factors, e.g., the dominant CEO, the extravagant spending and lifestyles of executives, the ignoring of warning signs, the taking on of risks that are not customary to assume in the industry, the aggressive behavior when under fire, the attitude of indifference toward financial reporting and compliance with Sarbanes-Oxley, etc. The absence of warning signs says a lot about management's philosophy and operating style, commitment to ethical values and other qualitative measures of the tone at the top.
- Emphasis should be given to validating the integrity of information supporting entity-level monitoring of the financial reporting process and entity analytics. Management cannot place reliance on these reports without also testing the controls over the underlying processes that generate those reports, including the relevant general IT controls.
- Still another option is to use survey instruments in selected areas. For example, to validate commitment to ethical values, surveys of employees can provide an indication as to whether management's perceptions of employee perspectives and behavior, and the reality of employee perspectives and behavior, are consistent. Broader-based surveys may also be used. These are common techniques for validating tone at the top and supplementing the use of inquiry and observation techniques.
- Validation procedures might include steps such as:
  - Periodic discussions with key members of the management team regarding operating issues and the resulting financial reporting implications
  - Reviews of evidence documenting the effective operation of specific control activities, including financial and operating reports, written explanations and analyses of variances, internal audit reports, written plans for corrective action, written codes of conduct, board minutes, conflict-of-interest policies, HR policies, etc.
  - Evaluation of the process for communicating the code of conduct, handling exceptions to the code and periodic reporting of exceptions to executive management and the audit committee

- Obtaining an understanding of documented authorizations and job descriptions for key financial reporting functions and determining there is an adequate understanding of roles, responsibilities and authorities
- Reviews of management's process for identifying and prioritizing risk
- Corroboration of important discussions with key members of senior management by review of pertinent company reports, and analyses and inquiries of line management and process owners
- Reviews of company reports evidencing the planning and budgeting process
- Testing of specific controls over centralized processes, including shared services environments, affecting significant financial reporting elements
- Testing of specific controls over the period-end financial reporting process
- Testing of the basis for representations made during the conduct of the company's self-assessment program to assess the overall quality and effectiveness of the program
- Obtaining an understanding of processes for updating accounting policies whenever there are changes in policies
- Observations of senior management personnel in the performance of their duties to understand the processes they use to control the business, e.g., attendance at regular budget review meetings, loan approval committee meetings, etc.

Note that the project team need not validate the existence and effectiveness of each and every response supporting the various points of focus underlying each attribute at the control environment or for any other entity-level controls (see Question 41 for an explanation of these terms), but rather only those responses considered most significant to management's overall assessment of internal control over financial reporting. For example, assume a company's budgetary control process includes evaluation of external and internal environmental factors, interactive participation of top management and line personnel, timely comparison of actual results against plan, appropriate management investigation and review of actual results and significant variations from plan, and effective corrective action. In order to be satisfied that the budgetary control process is functioning effectively as an ongoing monitoring process, the project team need not observe or review evidence supporting each step of the process.

The extent of validation of the operational effectiveness of the entity-level controls also will be influenced by many factors, including the following:

- The conservatism of accounting policies used in public reporting
- The timeliness of management's identification and resolution of problems
- The results of prior years' external and internal audits, e.g., proposed adjustments as a result of the audit, disagreements with the independent auditors, etc.
- Historical experience regarding the adequacy of controls, e.g., significant fourth-quarter adjustments, extensive audit confirmation exceptions, existence of significant deficiencies, etc.

A general guideline is to validate only those attributes and points of focus that most directly reduce the risk of material misstatement in the financial statements and then be more selective with respect to validating the remaining attributes and points of focus.

84. Are entity-level controls the same thing as entitywide controls?

Entitywide controls include controls that operate at the entity-level plus controls over processes that are entitywide in scope. For example, entitywide controls include:

- The control environment, including the assignment of authority and responsibility, consistent policies and procedures, and entitywide programs such as codes of conduct and fraud prevention that apply to all locations and business units

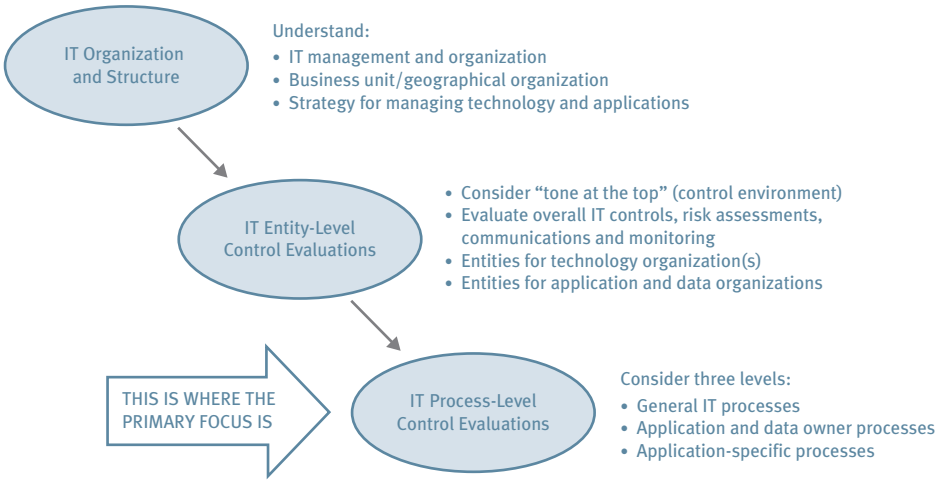
- The risk assessment processes used by management and process owners
- Centralized processing and controls, including shared services environments
- Procedures and analytics for monitoring results of operations
- Processes for monitoring performance of controls, including activities of the internal audit function and self-assessment programs
- Controls over the period-end financial reporting process
- Board-approved policies that address significant business control and risk management practices

Note that the SEC has defined the term "entity-level controls" in a manner that includes entitywide controls.

85. How are IT risks and controls considered?

The response to this question is more fully discussed in Protiviti's companion publication, *Guide to the Sarbanes-Oxley Act: IT Risks and Controls*, which outlines an overall approach for integrating the consideration of IT risks and controls into a Section 404 compliance project. The overall approach can be depicted as follows:

The IT assessment should be performed in the following illustrated sequence because each step impacts the scoping and, in some instances, the nature of the work to be performed in subsequent steps. For example, the initial step of understanding the "IT organization and structure" addresses the IT organization (e.g., centralized versus decentralized, shared services, business unit alignment, geographic alignment, etc.), management structure and reporting, and the entity's vision for IT. This initial step sets the foundation for the IT entity-level control evaluations. Subsequently, the strengths and weaknesses of the entity-level controls will impact the nature and extent of the IT process-level control evaluations for each of the three levels evaluated.



The IT process-level control evaluations are, by far, where the most time and effort will be incurred for Section 404 compliance projects. The IT process-level evaluations are made up of three distinct sets of processes that must be considered. These processes are sequenced in the order by which they should be evaluated. Following is a brief discussion of each of these areas:

- ***General IT Processes*** – The review of general IT controls addresses the critical IT processes within each entity or for each key location that supports key financial reporting-related applications. General controls typically impact a number of individual applications and data in the technology environment. As a general

rule, these controls impact the achievement of the financial statement assertions germane to critical processes by supporting an environment that provides for the integrity of processing and data. The general IT processes that should be evaluated in almost every instance include:

- Security administration
- Application-change controls to ensure that changes to application systems (through systems development, upgrades and maintenance) are authorized, tested and approved before they are implemented
- Data management and backup/recovery
- Data center operations and problem management
- Asset management

In certain circumstances, the Section 404 compliance project team may need to review the same general controls area more than once. For example, if there are multiple processes impacting each priority financial reporting area that are not subject to similar policies, process activities and control procedures, these multiple processes may need to be separately reviewed.

- ***Application and data-owner processes*** – The processes evaluated in this area are those that should be controlled and owned directly by the application and data owners. Typically, application and data owners are part of the business process. Often they also own the overall business process from a controls design and operations perspective. The overall process owner can delegate this ownership to someone, but the process owner must clearly communicate what is expected out of the delegate. The application and data owner must take responsibility to understand, design and maintain the controls within the application. These individuals must understand computerized controls so that they can knowledgeably design such controls and communicate these needs to IT personnel. The application and data owner also must understand the limitations of computerized controls, and be able to assist in the design of detective and monitoring controls that may be needed to compensate for weak general controls for certain IT processes.

  The processes that should be evaluated in almost every instance for purposes of completing the Section 404 compliance project include establishing and maintaining segregation of incompatible duties (security roles and administration) as well as confirming/reviewing access to critical transactions and data. These processes provide assurance that critical IT infrastructure components and application systems and data are in place so that only authorized persons and applications have access to data and then only to perform specific functions, which directly relate to the authorization and access to assets assertions. The application and data owners also have a critical role to play in the application development and maintenance process, and the effectiveness of that role should be evaluated as an integral part of that process.

- ***Integrated application-specific processes*** – Application-level controls include such controls within business processes as application-programmed controls, access controls (for critical transactions and data), data-validation and error-checking routines, and error reporting. They also include controls over complex calculations, critical interfaces and other aspects of the process to ensure complete and accurate reporting. These application controls should be understood for each critical financial application within the critical business processes. It is essential to evaluate, on an integrated basis, all IT and manual controls at the business-process level. The IT-related portion of this assessment focuses on controls within key applications. It is important to integrate this IT risk and control evaluation with the business-process evaluation so that a holistic understanding of the control environment is achieved.

Each of the areas in the preceding discussion is reviewed in more detail in *Guide to the Sarbanes-Oxley Act: IT Risks and Controls*. The impact of IT must be carefully considered in an evaluation of internal controls. For example, if management relies on programmed controls (with limited or no user verification of the results of processing) or, alternatively, a critical control is dependent on IT-generated data, the effectiveness of pervasive IT controls is a significant consideration when evaluating the process-level controls dependent on the IT

system or on IT-generated data. With respect to transaction processing that is outsourced, please refer to the next question.

During their assessment, IT personnel and the Section 404 compliance team evaluate IT-related risks and the effectiveness of IT controls, and also indicate the nature and type of available supporting evidence. Working with appropriate IT personnel, the compliance team must develop and execute a plan to obtain, document, assess and validate the relevant supporting evidence.

Management's evaluation must consider the combined results and conclude on the general IT controls and application and data owner controls. This assessment should provide specific control-related findings that support specific control objectives at the process level (and also relate to specific financial reporting assertions). It could include an evaluation of the adequacy of detective and corrective controls that compensate for identified weaknesses in general IT controls. For example, user input and output controls may be deployed to provide reasonable assurance that processing results are complete and accurate. There are limitations, however, to the effectiveness of user controls in compensating for weaknesses in general IT controls.

86. What if transaction processing is outsourced?

When transaction processing is outsourced, management must still assess controls over processing that are significant to the company's systems which impact financial reporting and disclosures and the related controls. IT and other control issues exist regardless of whether the processing takes place internally or externally. Under the provisions of Section 404 of Sarbanes-Oxley, management must evaluate the controls over the process activities and applications that are critical to the company's internal control over financial reporting. This evaluation must be directed to processes and applications that the company operates and processes and applications that the company outsources to external service providers. The SEC and PCAOB have reinforced this point of view.

When an organization considers internal controls relative to outsourced processes and systems, reviewing the outsourcing agreement is a critical first step. The agreement ideally will describe the responsibilities of each party related to key aspects of the process and the application's operations and maintenance (e.g., security administration, change management, data management, computer operations and ownership rights, etc.). It should also define service-level agreements, which also may address some of the control aspects that need to be understood. The contract is an important control document evidencing an outsourcing relationship as it articulates "who is responsible for what."

The evaluation of internal controls resident in business processes should consider the controls needed to achieve all relevant financial statement assertion objectives, which are likely to require appropriate controls residing at the service organization (outsourcer). During a Section 404 compliance project, these controls must be evaluated and tested like any other controls for a process or an application managed and controlled directly by the company. The SEC and the PCAOB have made it clear that the use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting. Organizations may accomplish this evaluation and testing through either an SAS 70-type report provided by the outsourcer (provided the issues noted in this response are addressed) or by having independent testing performed by the company's designee (e.g., internal audit, outside consultant, etc.).

When deciding on the approach for pursuing this evaluation effort, here are a few thoughts to consider:

- The contents of an SAS 70 report are reviewed in relation to controls at the user organization. Therefore, the user organization should develop a process map that documents input controls, the processing that is done at the service organization, and the outputs and output controls. In addition, the user would also map key master file maintenance processes and user organization security administration procedures for the application because, typically, the key controls over authorization and segregation of duties are internal to and under the control of the user organization.

The service organization merely executes the directions issued by the user organization, consistent with the view that under most outsourcing arrangements the user is buying expertise and competence and not transferring process risk. Therefore, the user organization's controls obviously will need to be evaluated and tested along with the service organization's controls.

- In the past, SAS 70 reports typically were written and scoped for the purpose of communication between the independent auditor for the service organization and the user company's external auditor for his or her use in conjunction with the audit of the user organization's financial statements. Section 404 has changed the dynamics of these requirements by assigning *management* the responsibility to make an assertion with respect to the entity's internal control over financial reporting. Thus, management will likely need an SAS 70-type report from the service organization's auditors. The alternative is for management to test the service organization's controls independently, which may not be a practical option.

  If an SAS 70-type report is to be used by management, there are several considerations to keep in mind:

  - First, while a reading of an SAS 70 report clearly indicates that it is an auditor-to-auditor communication and it is possible that the now-defunct Auditing Standards Board did not intend for it to be used for management reliance from a regulatory standpoint, the PCAOB has a different idea. In its interpretive guidance to management, the SEC clearly extends the use of SAS 70 reports to management. If the outsourcing agreement is appropriately modified to articulate the SAS 70 report requirements, then the letter and reporting relationship can be conformed to satisfy those requirements. Both user and service organizations may want to seek advice from legal counsel as they review the legal aspects of this reporting and the reliance on it.
  - Second, the scope of the SAS 70 review needs to be evaluated carefully. Prior periods' scope to satisfy the auditors for purposes of expressing an opinion on the financial statements may need to be expanded, perhaps significantly, to satisfy the additional requirements of management. For example, the SAS 70 report must address relevant financial reporting assertions and focus on both design and operating effectiveness. Again, this is an area for which management is clearly responsible under Sarbanes-Oxley. In conjunction with the controls over processes and applications managed by the entity, management must make the decisions regarding the sufficiency of scope and is responsible for determining the adequacy of the testing coverage and evaluation of test results. The extent to which management is also responsible for making these decisions with respect to service-provider controls is driven by many factors, including the strength of the input, output, segregation of duties and other controls of the user organization, and the criticality of the service provider's processes and applications to the reliability of the user's financial statements.
  - Finally, we expect companies and their service providers to take advantage of the SEC's extension of the Section 404 transition period by renegotiating their service agreements. For example, management may specify its testing requirements in the outsourcing agreement, and the report issued by the service provider's auditor can refer to those requirements. Many outsourcing service providers may, in fact, look to coordinate these types of requirements with all of their clients and their independent accountants in order to avoid a time-consuming, case-by-case approach.

- There is also the matter of the point-in-time internal control report that management must issue to comply with Section 404 as of its annual report year-end. An SAS 70 report may cover either a point in time or a period of time, with a warning about projecting the results into the future. Typically, an SAS 70 report is a point-in-time report with a warning about projecting the results into the future. How would this requirement affect management's ability to sign off on its assertion about the controls as of year-end if the date of the SAS 70 report differs significantly from that date?

  From a practical standpoint, unless service organizations choose to have their auditors issue periodic (e.g., quarterly) SAS 70 reports that they can provide to interested user organizations, there will almost always be a difference between the time period covered by the SAS 70 report and the date of management's assessment. Neither the SEC nor the PCAOB provide a "bright line" test as to when a significant period of time has elapsed between the period covered by the service auditor's report and the date of management's assessment.

The Board probably anticipated a difference of six months or more when it provided guidance as to the procedures necessary for the auditor to address such differences. For example, management should understand at a minimum whether there have been changes in the service organization's controls subsequent to the period covered by the service auditor's report. Such changes might include:

- Changes communicated from the service organization to management
- Changes in service organization personnel, with whom management interacts
- Changes in reports or other data received from the service organization
- Changes in contracts or service-level agreements with the service organization
- Errors identified in the service organization's processing

If changes or errors have been noted subsequent to the period covered by the SAS 70 report, management must evaluate the need to perform procedures to evaluate the effect of such changes on internal control over financial reporting. The PCAOB also requires additional evidence of the operating effectiveness of controls at the service organization based on consideration of such risk factors as: (1) the elapsed time between the time period covered by the tests of controls in the SAS 70 letter and the date of the user organization management's assessment; (2) the significance of the service organization's activities to the user organization's financial reporting; (3) the extent of errors, if any, noted at the service organization and the nature of those errors; and (4) the nature and significance of any changes identified in the service organization's controls. If needed, such evidence may include obtaining specific information from management of the service organization, requesting a service auditor to perform appropriate procedures to obtain such information or arranging to have company representatives visit the service organization to perform such procedures.

While there are many issues that should be considered, it is clear that for significant applications some work at the service organization is required. A satisfactory SAS 70 report is a useful tool for obtaining evidence as to the effectiveness of internal controls at a service organization. The financial reporting implications of the outsourcing arrangement are a critical factor, and management is ultimately responsible for deciding what must be done. Due to management's responsibilities to report on internal control and the independent auditor's responsibility to attest to and report on management's assertion, it is now necessary to focus closer attention on the adequacy of SAS 70 reports for management's purposes.

In some circumstances, management may encounter difficulty in obtaining the requisite SAS 70 letter from the service organization. In such instances, management also may be unable to assess the underlying controls, and sufficient compensating controls may not be in place. As management is not permitted to issue a report with a scope limitation, the SEC has stated that a determination must be made as to whether the inability to assess controls over a particular process is significant enough to conclude that internal control over financial reporting is not effective.

In closing, it is important to note that there are some areas that cannot be outsourced effectively and must remain the focus of the user organization's management. For example, the work of application and data owners who own the overall process from a controls design and operations standpoint should ordinarily not be outsourced.

87. Do SAS 70 reports apply to processes other than IT and to specialists?

SAS 70 reports apply to all outsourced business processes. As set forth in AU Section 324, *Service Organizations*, these reports represent a service auditor's report on a service organization's description of the controls that may be relevant to a user organization's internal control as it relates to the achievement of specific control objectives, either as of a point in time or during a specified period of time. For example, SAS 70 reports apply to processes that include more than IT, such as payroll processing, tax return preparation, tax provision and reserve calculation, and accounts payable processing.

Many companies deploy the services of a specialist from time to time to assist in interpreting technical matters, developing valuations, preparing estimates and supporting disclosures used during the financial reporting process. Specialists include such individuals as actuaries, appraisers, investment bankers and reserve engineers. The question arises as to whether SAS 70 reporting applies to the use of specialists. SAS 70 reporting applies in circumstances when a company outsources a process that it could otherwise perform itself. Specialists, on the other hand, often bring core competencies to the financial reporting process that most companies do not possess. The distinction is one of "procuring a service" versus "outsourcing a process." The PCAOB staff reinforces this distinction when they point out that a specialist is not part of a company's information system and, accordingly, cannot be an outsourced process. For example, when a company engages an actuary to calculate the required post-retirement benefit disclosures, the nature of these services involves the use of a specialist. In these instances, the auditing literature emphasizes evaluating the qualifications of the specialist versus evaluating the underlying process used by the specialist. The contribution of a specialist is rooted in the skill and competency he or she brings to bear as opposed to a proprietary process. Therefore, with respect to a specialist, management's focus should be as follows:

- First, management should evaluate the qualifications of the specialist to determine that he or she has the requisite subject matter expertise, knowledge and skills.
- Second, management should clarify the objectives and scope of the specialist's work as it relates to the financial reporting process.
- Third, management should understand the methods or assumptions used by the specialist to accomplish the specified financial reporting objectives, and ascertain whether those methods or assumptions are consistent with the prior period.
- Finally, the company should evaluate its controls to ensure the specialist receives the precise information he or she requests for purposes of making his or her calculation(s), and that the information received from the specialist is in accordance with the requirements of generally accepted accounting principles.

The auditing literature requires the auditor to evaluate the above matters; therefore, management should be prepared to respond to questions regarding these matters when using a specialist during the financial reporting process.

88. Where does an entity-level controls review end and a process-level controls review begin?

The line between these two reviews is not always clear because of the broad nature of entity-level controls as defined by the SEC. Entity-level controls include controls that are directly related to significant financial reporting elements. These controls often operate at a process, transaction and application level. Many of these controls are monitoring activities. There are also controls pertaining to processes that are entitywide in scope, such as IT processes or shared services. While these controls function at the process level, they are entitywide in nature.

The project team ultimately must decide where the line is drawn. Generally, controls at the entity level are not directly involved with initiating, authorizing, recording, processing and reporting transactions. Controls at the process level are directly involved with the critical transaction flows affecting financial reports.

89. How is the process- or activity-level assessment conducted?

Question 42 addresses how the COSO framework is applied to the activity or process level. Generally, the following steps apply.

Document targeted processes – This step identifies key inputs, activities and outputs that are relevant to the priority financial reporting elements in accordance with management's documentation standards. It sources where the risks are and indicates the key control points. It also engages the process owners in the evaluation process, including obtaining their sign-off. With respect to applying a top-down approach, there may be instances where

an understanding of the flow of transactions can be gained through walkthroughs and discussions with, and involvement of, process owners who are sufficiently knowledgeable of the processes and systems underlying the critical financial reporting elements. However, if company personnel are not sufficiently knowledgeable of the control environment or lack a sufficient fact base supporting their input to the top-down approach, then the company must document the control environment sufficiently to obtain the requisite understanding for applying the top-down approach.

Document the risks and controls – After the process inputs, activities and outputs have been documented, or an understanding by the appropriate process owners has been confirmed, the next step is to work with process owners to source the financial reporting risks within the process and define the key control points either at the source of the risk or downstream from the source. Financial reporting risks are derived from financial reporting assertions (see Questions 71 and 72 for illustrations). When identifying controls, the project team filters them down to the vital activities (i.e., the key controls) that control the risk. When mapping processes, sourcing the risks and identifying the control points, engage the process owners by involving them in the analytical process and obtaining their sign-off on the completed documentation. These maps should specifically reference, where appropriate, the IT-related risks and controls discussed in Question 85.

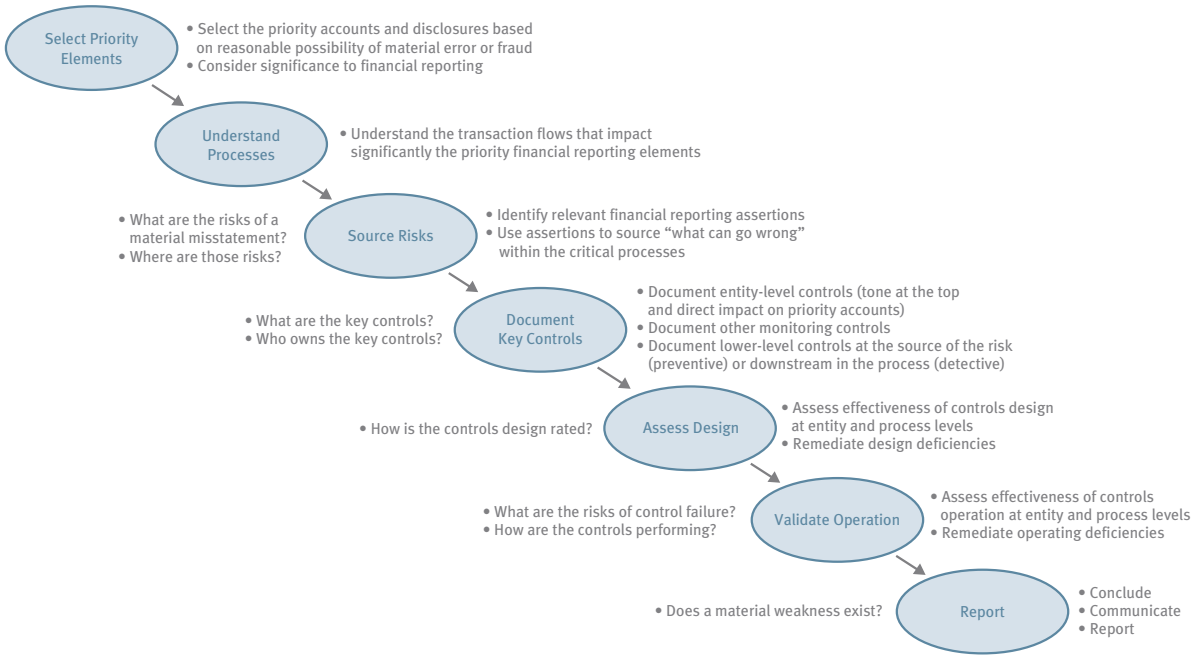
Assess design effectiveness – After the risks and controls are documented, the project team evaluates whether the controls, as designed, provide reasonable assurance that the relevant assertion risks have been reduced to an acceptable level, i.e., the stated financial control objectives have been met. If there are significant design deficiencies, they should be remediated in a timely manner *before* testing operating effectiveness.

Validate operational effectiveness – For those internal controls where the design is determined to be effective, require the process owners and internal audit to validate or test the operational effectiveness of the controls. If there are significant operating deficiencies, they also should be remediated timely.

Summarize control gaps – Based on the assessment of design effectiveness and tests of operational effectiveness, identify and summarize areas requiring improvement in internal controls.

In summary, following is a "plain English" illustration of the sequence of steps at the activity or process level. (Note: The attestation process is not included.)

A Plain English Summary



90. What are walkthroughs, why are they necessary and how should the Section 404 compliance team prepare for them?

The PCAOB requires the independent auditor to accomplish certain objectives outlined in Auditing Standard No. 5 relating to understanding the likely sources of potential misstatements. These objectives are:

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

The PCAOB is of the view that "performing walkthroughs will frequently be the most cost-effective way to accomplish the [above] objectives." In performing a walkthrough, the auditor is instructed to "[follow] a transaction from origination through the company's processes, including information systems, until it is reflected in the company's financial records." Basically, the auditor is required to follow the process flow of actual transactions using, as the PCAOB states, "the same documents and information technology that company personnel use."

If a significant process affects multiple major classes of transactions, the auditor might decide to determine, during the walkthrough itself, how the significant process addresses the risks unique to those transactions. Note that major classes of transactions are often broken down into routine transactions, nonroutine transactions and estimation transactions. See Question 66.

The Purpose of Walkthroughs

The purpose of walkthroughs is to enable the auditor to obtain a sufficient understanding of the organization's processes, risks and controls so he or she can effectively evaluate controls design and plan effective tests of controls. In essence, walkthroughs can provide the auditor with evidence to verify his or her understanding of the design of controls, including those related to the prevention or detection of fraud.

A walkthrough is performed through a combination of procedures (e.g., inquiry, inspection, observation and reperformance). In fact, the Board asserts that the techniques implicit in performing most walkthroughs may be sufficient to test the operating effectiveness of some lower risk controls. The PCAOB also points out that, as a test of controls, inquiries might be made concurrently with performing walkthroughs. In Auditing Standard No. 5, these inquiries are called "probing questions." They are used to ask process owners about their understanding of what is required by the company's prescribed procedures and controls. According to the Board, these questions "allow the auditor to gain a sufficient understanding of the process and to be able to identify important points at which a necessary control is missing or not designed effectively."

As noted earlier, the focus of a walkthrough for the upstream business processes is on the activities to initiate, authorize, record, process and report transactions. Those activities ordinarily would include procedures for correcting and reprocessing previously rejected transactions and for correcting erroneous transactions through adjusting journal entries. However, a walkthrough of the period-end financial reporting process is different. Because of the nature of the period-end financial reporting process, the auditor's focus would be on understanding how transaction totals recorded in the general ledger are ultimately reflected in the financial statements and related disclosures.

Preparing for Walkthroughs

In preparing for walkthroughs, management and Section 404 compliance teams should ensure that there is sufficient process documentation addressing the major classes of transactions. With this focus in mind, it is important that the company document its processes in reasonable detail, as required by the SEC's interpretive guidance. If there is sufficient process documentation available, the auditor will find it useful during the walkthroughs. If the company has not documented its processes in reasonable detail, then the auditor will likely have to create the documentation.

While the SEC has made it clear that alternative forms of documentation are acceptable, we believe that process maps – at least for the higher risk processes – are an excellent tool for providing management and the auditor the transparency needed for an effective walkthrough (see Question 91 for further discussion about process mapping). In addition, process owners must be prepared for the auditor. For example, to facilitate the walkthrough, they should have available legible copies of the most up-to-date materials, key control reports, screenshots and forms. Process owners need to "stay on message." In other words, they should focus on describing their processes, risks and controls, and avoid speculating about who does what in other groups, departments or units. They should ascertain that the documentation provided to the auditor is consistent with the documentation he or she requests. They need to be prepared to demonstrate the control activities for which they are responsible. For example, if the signature block is supposed to be locked, they should be sure to lock up after showing it to the auditors.

What to Expect from the Audit Process

What can process owners expect during a walkthrough? Following is a list of things an auditor may do as he or she performs the walkthrough with appropriate management, supervisory and other personnel:

- Request information about documented policies and procedures.
- Request information about controls to understand which controls are manual versus automated and which controls are preventive versus detective.
- Inspect specific documents and observe application of specific controls.
- Inquire about exception scenarios arising during execution of the process, and the handling and resolution of exceptions as well as re-entry of corrected data into processing. (Note: It is possible the auditor will want to see actual exceptions in process to follow them all the way through to resolution and re-entry.)
- Request evidence of important controls, including access controls for specific applications, segregation of duties, management monitoring and oversight, and other critical controls.
- Trace transactions through the information systems relevant to financial reporting.
- Inquire about processes and controls that would prevent, deter or detect fraud, and whether fraud had ever been detected in the process.
- Inquire as to the frequency with which each control operates to prevent or detect errors or fraud.
- Inquire as to instances of management override with respect to established controls.

In summary, the auditor will want to know where the risks are, what the controls are, how the controls are performed, who performs the controls, and the data reports, files or other information used in performing the controls. The auditor will also want to know the physical evidence, if any, produced as a result of performing the controls, as well as the effectiveness of the controls in preventing or detecting and correcting errors or fraud on a timely basis.

We are aware of companies training their process owners to facilitate preparation for auditor walkthroughs. We believe this is a smart approach. All told, process owners must understand that during the walkthrough the auditor is carefully evaluating them and their subordinates in terms of their skill and competence in performing

the process and the related controls. The auditor will be looking for answers to the "how do you know" questions. For example, how do you know the process results are reliable? How do you know all transactions that should be processed during the period are in fact processed? How do you know that transactions are processed accurately? Expect a stronger emphasis on understanding the application of manual controls, including who is responsible for performing them, how often and when.

91. How are processes and transaction flows documented?

When evaluating internal controls, management needs to demonstrate knowledge of the underlying processes of the business. That is why processes and transaction flows are documented. The extent of existing documentation carries substantial weight in determining the nature and extent of additional documentation required. Historically, the professional auditing standards and the COSO framework have not dictated the format of the required process documentation; they require only that there is an adequate understanding of the underlying processes (or major transaction flows) so that the sourcing of financial reporting risks and the documentation of the relevant controls is sufficiently granular to support management's assertions. The SEC interpretive guidance provides similar direction.

What is important is that the key components of the processes and transaction flows are documented so that the project team can understand how transactions are initiated, authorized, recorded, processed and reported. This understanding will enable the team to source the risk of errors and omissions and assess the controls that mitigate these risks. Furthermore, the nature of the documentation will vary according to the nature of the transactions involved. In Question 66, transactions were categorized as routine, unusual or nonroutine and accounting estimates. These types of transactions are differentiated in the following comments.

Routine Transactions

The documentation of the key components for routine transaction processes affecting a significant financial statement account should address the following:

Initiate	• Identify where all significant economic events relevant to the account are recognized.
Authorize	• Describe the procedure by which transactions are approved for processing, including what specifically is approved, who approves the transaction and the timing of their approval.
Record	• Describe how authorized transactions are accepted for input into processing, including online entry procedures.
Process	• Describe the significant processing activities, including processes for correcting rejected transactions and re-entering them into processing. • Identify the critical data files used during processing (e.g., customer, pricing, accounts receivable, credit, perpetual inventory, and employee and supplier master files). • Identify the key forms, documents and records used during processing. • Identify the departments and functions involved in processing so that an assessment can be made of the extent to which incompatible duties are segregated.
Report	• Define the key reports resulting from processing. • Identify the key output files and records that may be used as inputs to other critical processes and accounting systems.

For most companies, Section 404 requires more support than in the past to document that the internal control structure is working properly. A company's process owners ultimately are responsible for evaluating the critical processes and controls as they relate to the financial statements. Their evaluation must provide management with reasonable assurance that the internal control environment is both adequate and effective. The question is, under the top-down approach, how do they document their processes to support their evaluation?

The SEC has stated that only the key controls need be documented. Therefore, it is possible that the Section 404 project team can gain an understanding through process walkthroughs and discussions with, and involvement of, process owners who are sufficiently knowledgeable of the processes and systems underlying the critical financial reporting elements. However, if company personnel are not sufficiently knowledgeable of the control environment or lack a sufficient fact base supporting their input to the top-down approach, then the company must document the control environment sufficiently to obtain the requisite understanding for applying the top-down approach. That documentation may entail development of process documentation.

In considering the type and depth of process documentation for routine transactions, there are two questions to ask for each relevant process. First, should the process be mapped? Second, if a process map is appropriate, what is the appropriate level of process documentation?

In Auditing Standard No. 5, the PCAOB provides insights to answering these questions with the following direction:

> To further understand the likely sources of potential misstatements, and as part of selecting the controls to test, the auditor should achieve the following objectives:
>
> - Understand the flow of transactions related to the relevant assertions, including how these transactions are initiated, authorized, processed and recorded.
> - Verify that the auditor has identified the points within the company's processes at which a misstatement – including a misstatement due to fraud – could arise that, individually or in combination with other misstatements, would be material.
> - Identify the controls that management has implemented to address these potential misstatements.
> - Identify the controls that management has implemented over the prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could result in a material misstatement of the financial statements.

While this language may not explicitly mandate the use of flowcharts, it supports an assertion that process mapping is a best practice for fulfilling the above requirements. For high and medium risk areas, management must demonstrate an understanding of the major transaction flows and potential points of failure within those flows. This "sourcing principle" and the objective of linking controls to the risks they mitigate capture the essence of what process mapping helps to accomplish.

Process mapping is a valuable tool for documenting processes and transaction flows; however, it is also an investment of project resources. It requires time to map a process. It requires standards so that maps provide a common language across the organization. It requires a requisite level of skill to prepare and maintain. If not managed, process maps can become an end unto themselves instead of a means to an end. However, an effectively organized approach to mapping processes provides important benefits. For example, a process map:

- ***Provides a common language*** – Provides easy-to-follow, visual, supporting documentation for the information included in the risk and control matrix, supplying the project team with a frame of reference for discussing control strengths and weaknesses or planned changes.
- ***Reduces project risk*** – Reduces risk that the project team misses key risks and key controls during the evaluation process.
- ***Facilitates analysis*** – Surfaces risks and controls related to the timing and sequence of events, so that control points at the source of risk can be differentiated from control points downstream from the source.
- ***Documents evidence*** – Gives the process owners a visual tool to use to assert that their process continues to work correctly and that the controls embedded within the process are effective.
- ***Supports auditor walkthroughs*** – Facilitates the walkthrough process by providing a visual depiction of all important aspects of each critical process.

- ***Enables focus on change*** – Provides a way to identify process changes during subsequent reviews.
- ***Provides operating benefits*** – Provides a framework for tying together the individual activities of people who work on a process to help each member of the team understand the other roles and responsibilities within the process; provides a training tool to enable new hires to learn their jobs quickly; and offers identification of opportunities to improve efficiency and effectiveness.

For significant financial reporting elements, the evaluator of the key controls on which management is relying for purposes of complying with Section 404 must understand the major transaction flows. However, the SEC interpretive guidance and auditing literature does not dictate the form of documentation required. Therefore, management must decide whether or not the company's process owners can conclude that all of the material risks, for which the likelihood of occurrence is at least reasonably possible, have been sourced for each financial reporting assertion applicable to each significant process. If the answer is "yes," then the next question should be, "How do you know the risk assessment is sufficient given the extent of process documentation?"

Maps do not have to be highly sophisticated or detailed. Project teams should set their sights on documenting, communicating and understanding major transaction flows using a framework within which to source risks and identify key controls.

There are several reasons justifying a conclusion not to map a relevant process. For example:

- The process owner has a sufficient understanding of the key components of the process to source areas where material errors can occur and document the control activities in place to prevent or detect those errors.
- The process is simple enough to be described in procedural write-ups and other similar documentation.
- The company has sufficient documentation of the process. Such documentation may be in the form of policy statements, procedural write-ups, job descriptions, flowcharts, desk procedures or a combination of these things. If process owners can confirm the existing documentation is current, further documentation may not be needed.
- The company is very mature with stable processes (versus a new, constantly evolving company requiring more formalization to ensure relevant points have been captured since the last review).

When management decides not to map a relevant process, it should recognize that the independent public accountant might decide documentation is necessary to facilitate the attestation process. In those instances, the auditor could create process documentation.

If there is little or no documentation, the project team must decide on the level of documentation to address the key elements of the process. Following are examples of different levels of process documentation:

- ***Top-down flowchart (Level 1)*** – Most processes in organizations are complex. When mapping processes, it is easy to get lost in the details. A top-down flowchart is useful in documenting complex processes and instilling discipline in process mapping. The top-down flowchart documents the beginning and end of a process with no more than six or seven critical steps in between. The project team has the flexibility to select only two or three of the critical steps for more detailed analysis. By itself, a top-down map is not sufficiently robust to source risks and control points.
- ***Process flowchart (Level 2)*** – A process flowchart displays a series of actions and decisions in a manner that is easy to understand and allows companies to document things quickly. It portrays inputs, activities, interfaces and outputs. It can be used to source risks and identify control points at the source or downstream from the source. Generally, Level 2 should be used for all critical processes affecting significant financial reporting elements, except for the period-end financial reporting process (the "close-the-books" process).
- ***Process interfunctional chart (Level 3)*** – This chart shows the cross-functionality of a process and highlights the handoffs during the process. The cross-functional focus (so-called "swim lanes") is invaluable when analyzing processes for simplification, streamlining and elimination of nonessential tasks. Use Level 3 for the period-end financial reporting process and for any other critical processes where management wishes to

emphasize such objectives as improving quality, reducing costs and compressing cycle time. Reducing elapsed time may be a management prerogative due to the SEC's accelerated filing deadlines for 10-Ks and 10-Qs, particularly for large accelerated filers.

Other Transactions

With respect to unusual or nonroutine transactions as well as transactions arising from accounting estimates (estimation transactions), there is less formality in processing. While a Level 1 or Level 2 flowchart may be used to document these flows, process narratives may also be appropriate.

For unusual transactions (e.g., mergers, divestitures, debt restructurings, plant closings, etc.), emphasis should be given to understanding the extent of documentation required to support these transactions and to the timeliness of involving persons with the specialized knowledge and expertise to determine the correct accounting and reporting. There should also be evidence of board approval of significant unusual transactions.

The documentation of nonroutine transactions should address:

- The frequency and timing of the transactions
- The people involved in the processing of the transactions and the methods and assumptions they use
- The key forms and documents and the information systems used to process these transactions
- The persons responsible for approving results of processing

For transactions arising from critical accounting estimates, special attention should be given to these transactions due to their subjective nature. The SEC defines "critical accounting estimates" as "estimates or assumptions involved in the application of generally accepted accounting principles where the nature of the estimates or assumptions is material due to the levels of subjectivity and judgment necessary to account for highly uncertain matters or the susceptibility of such matters to change[,] and the impact of [such] estimates and assumptions on financial condition or operating performance is material." Because the controls over these estimation transactions are subject to the risk of management override, involve significant judgment or are complex, the SEC asserts that the financial reporting elements affected by these transactions generally would be assessed as having higher risk for both the risk of a material misstatement and the risk of control failure.

Factors to consider in documenting the processes affecting significant accounting estimates include:

- The frequency and timing of how often the estimate is used by management in processing transactions, i.e., is the estimation process performed quarterly, monthly, etc.
- The reliability of the data used in making the accounting estimate and of the process for gathering that data
- The methodologies and underlying assumptions used in calculating estimates
- The applicable and relevant accounting literature
- The prevailing practice generally used in the industry to document the results of estimation processes
- The people involved in making the estimate
- The robustness of the estimation process and the critical points within the process that have the greatest impact on the resulting calculation
- The key forms and documents used in supporting the estimate
- The persons responsible for approving results of the estimation process

Given the attention paid by the SEC's interpretative guidance to the importance of effective controls over estimation transactions, management may want to focus carefully on documenting, understanding and improving the processes underlying these transactions.

92. Should we reduce the extent of our process documentation as we apply the top-down, risk-based approach?

We advise companies to be careful about mandating reduced process documentation costs. As discussed in Question 91, the real question is whether process owners understand the process sufficiently to provide input to the top-down approach. Another question arises as to whether the process documentation is sufficient to facilitate completion of the external audit.

The above said, there is a more important reason to consider the adequacy of the existing process documentation. With respect to selecting the vital few controls on which management will rely for purposes of complying with Section 404, if management's understanding of the control environment is sufficient and that understanding is documented in reasonable detail, then it is more likely that the application of the top-down approach will result in selecting the control set that is the most effective in mitigating financial reporting assertion risks. On the other hand, a deficient understanding of the control environment will lead to a lack of transparency that will likely result in failure to select a reduced number of controls. A reduced control set is important from a cost-effectiveness standpoint for two reasons:

- With respect to the evaluation of design effectiveness, it is the reduced number of controls that will reduce the cost in current and future years – not the nature and extent of documentation itself.
- With respect to tests of operating effectiveness, management has multiple ways to evaluate controls operating effectiveness, not all of which demand the same level of written evidence as the evaluation of design effectiveness. Both the reduced number of controls and the nature of evidence gathering to support a conclusion on operational effectiveness have the potential to reduce the cost of testing in current and future years.

Thus a one-time investment in process documentation to ensure a reduced control set can result in significant dividends in terms of reduced costs of evaluating controls design effectiveness and testing controls operating effectiveness in the years to come. A reasonable level of process and systems documentation is appropriate for financial reporting elements of high to moderate risk and complexity. The nature and extent of this documentation is a separate question from the nature and extent of management testing. While we have observed that low-risk processes have been overdocumented in years past, we believe it is important that companies complying with Section 404 for the first time understand that it is an efficient controls design and a cost-effective test plan – not the initial documentation – that will have the greatest impact on the cost of Section 404 compliance on an ongoing basis.

93. What are some examples of control activities?

Control activities are the policies, procedures, reports, methodologies and systems that responsible people use to reduce to an acceptable level the likelihood of an undesirable risk event occurring. These activities require supervision, enforcement and periodic evaluation. Controls over financial reporting may be pervasive or may be embedded within information processes. They are designed to either prevent or detect and correct errors and omissions affecting financial reports.

In its final rules, the SEC provided several examples of controls subject to management's assessment of internal control over financial reporting:

- Controls over initiating, authorizing, recording, processing and reconciling account balances, classes of transactions, and disclosure and related assertions included in the financial statements
- Controls related to the initiation and processing of nonroutine and nonsystematic transactions (such as accounts involving judgments and estimates)
- Controls related to the selection and application of appropriate accounting policies
- Controls related to the prevention, identification and detection of fraud

Other examples include:

- Controls, including general IT controls, on which other significant controls are dependent
- Each significant control in a group of controls that function together to achieve a control objective or financial reporting assertion
- Controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; initiate, authorize, record and process journal entries in the general ledger; and record recurring and nonrecurring adjustments to the financial statements

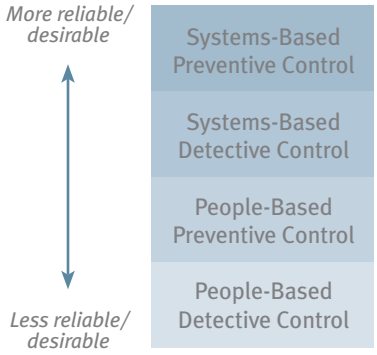
In its interpretive guidance, the SEC clarifies that only the key controls have to be documented. Thus the controls that management relies upon to mitigate the significant financial reporting assertion risks are the ones that matter from a Section 404 compliance standpoint.

Examples of control activities applied at the process, transaction and application level applicable to financial reporting are provided below in two categories – pervasive process controls and information process controls:

Pervasive Process Controls	Information Process Controls
• Establish and communicate objectives	• Obtain prescribed approvals
• Authorize and approve	• Establish transaction/document control
• Establish boundaries and limits	• Establish processing/transmission control totals
• Assign key tasks to quality people	• Establish/verify sequencing
• Establish accountability for results	• Validate against predefined parameters
• Measure performance	• Test samples/assess process performance
• Facilitate continuous learning	• Recalculate computations
• Segregate incompatible duties	• Perform reconciliations
• Restrict process system and data access	• Match and compare
• Create physical safeguards	• Independently analyze results for reasonableness
• Implement process/systems change controls	• Independently verify existence
• Maintain redundant/backup capabilities	• Verify occurrence with counterparties
	• Report and resolve exceptions
	• Evaluate reserve requirements

The so-called pervasive process controls apply to all categories of process objectives, including operational effectiveness and efficiency, and compliance with applicable laws and regulations. Information process controls apply to any process generating financial and/or operating information, and provide assurance that information is reliable for use in decision-making.

Pervasive process controls and information process controls are either preventive or detective, and can be positioned at either the source of the risk (preventive) or downstream from the source within a process (detective). Controls are also systems-based or people-based. The hierarchy shown at the right should be considered during the assessment of design, particularly in dynamic environments involving large volumes of transactions. As transaction volumes and the velocity and complexity of risk increase, systems-based controls are often more reliable than people-based controls because, if designed, developed, maintained and secured effectively, they are less prone to mistakes than human beings.



Furthermore, an anticipatory, proactive approach to controlling risk requires greater use of preventive controls than the reactive "find-and-fix" approach embodied in detective controls. Effectively designed control processes that prevent errors and omissions at the source free up people resources to focus on the more critical tasks of the business.

The COSO framework also applies to other objectives – effectiveness and efficiency of operations, and compliance with applicable laws and regulations. Following are other examples of control activities that apply to these categories of objectives – operational process controls and compliance process controls:

Operational Process Controls	Compliance Process Controls
• Define processes • Describe procedures • Supervise activities • Evaluate processes to eliminate, simplify and focus nonessential tasks • Test and pilot improvements • Organize cross-functional teams • Design interactive feedback systems • Appraise performance and link to reward system • Capture and share relevant knowledge and information	• Monitor the legal and regulatory environment • Assess impact of environment change • Articulate clearly compliance policies • Communicate compliance policies • Integrate compliance activities into business processes • Manage and monitor compliance • Take remedial and disciplinary action when necessary • Involve counsel in key business affairs • Manage the cost of litigation • Establish a fraud-preventing organization

As noted in our response to Question 44, some operational and compliance controls may be relevant to reliable financial reporting.

94. What are monitoring activities?

According to the SEC's interpretive guidance, "monitoring activities may include controls to monitor results of operations and controls to monitor other controls, including activities of the internal audit function, the audit committee and self-assessment programs." Monitoring activities would likely include those entity-level controls directly impacting the assessment of a financial reporting element, as discussed in Question 81. In effect, a monitoring activity is a procedure that ensures that a key control is operating effectively and is generally considered within the "monitoring" component of the COSO framework.

There should be more emphasis on monitoring activities, because effectively functioning monitoring activities provide increased assurance to certifying officers that the internal control structure is sustainable. Sustainability is an important objective, and monitoring activities play a role in achieving sustainability. This principle is inherent in the SEC's explanation of monitoring activities.

Monitoring activities assess the quality of internal control performance over time. They involve assessing the design and operation of controls on a timely basis and taking necessary corrective action. As set forth by COSO, they are accomplished through ongoing monitoring activities, separate evaluations by internal audit or personnel performing similar functions. Ongoing monitoring activities are often built into the normal recurring activities of an entity and include regular management and supervisory review activities.

95. When and how should the period-end financial reporting process (close the books) be evaluated?

The financial reporting process should be evaluated as early in the assessment process as possible to identify the significant upstream processes that "feed" the priority financial reporting elements. Desirably, the financial reporting process should be documented using a Level 3 map, as discussed in Question 91. This analysis should document:

- The closing process itself, including the consolidation process
- The information processed during the close, including the automated and manual inputs to the process
- The resulting outputs from the process used to develop financial statements, including recording and processing nonroutine adjustments and accounting estimates (e.g., consolidating adjustments, classifications, etc.)
- The various individuals responsible for different phases of the close
- The number of locations involved and the movement of documents, data and information during the process
- The process for preparing financial statement drafts and generating financial statement disclosures, including the extent of involvement of the disclosure committee
- The procedures for entering transaction totals into the general ledger
- The procedures used to initiate, authorize, record and process journal entries in the general ledger, including the use of IT, manually prepared spreadsheets and manually compiled data during the process
- The nature and extent of oversight of the process, including management and the audit committee
- The procedures for establishing and monitoring the selection and consistent application of accounting policies

Once the period-end financial reporting process is documented, the team should:

- Source the risks (i.e., determine "what can go wrong"), identify the controls and summarize the gaps
- Identify opportunities for accelerating the process, e.g., early elimination of intercompany transactions, streamlining of account reconciliations, reduction of manual and nonstandard journal entries, simplification of targeted areas and elimination of nonessential tasks
- Evaluate the report preparation process, including the processes for accumulating disclosure information

96. What are examples of controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles?

In its interpretive guidance, the SEC defines "critical accounting policies" as "those policies that are most important to the financial statement presentation, and require management's most difficult, subjective or complex judgments, often as a result of the need to make estimates about the effect of matters that are inherently uncertain." For example, such policies might relate to such matters as revenue recognition, hedge transactions, goodwill impairments, income tax accounting and lease transactions. The point is that certain financial reporting elements, such as those involving critical accounting policies, generally would be assessed as having higher risk for both the risk of material misstatement to the financial reporting element and the risk of control failure. When the controls related to these financial reporting elements are subject to the risk of management override, involve significant judgment or are complex in their execution, they should also generally be assessed as having higher risk.

The question often arises as to what the controls over the selection and application of accounting policies are. We believe these controls are integral to the company's period-end financial reporting process and disclosure controls and procedures. They ensure the company is using appropriate accounting policies, has communicated its accounting policies to appropriate personnel throughout the organization and is applying the selected policies consistently from period to period. Examples of such controls include the following:

- Qualified financial personnel with the resourcefulness, requisite knowledge and subject matter expertise to:
  (a) Research the accounting and reporting literature and stay abreast of an ever-changing research base
  (b) Obtain the input needed and understand the accounting and reporting requirements well enough to make decisions as to how the company should comply with those requirements
  (c) Implement the processes needed to execute the decisions to comply with the stated requirements

  The above excludes reliance on the external auditors, which was customary in the past.
- Clear articulation in writing of the critical accounting policies, particularly for the more complex and significant financial reporting areas
- Effective procedures in place that provide reasonable assurance the company is in touch with new developments in financial reporting requirements, including new and emerging releases by regulatory authorities and standard-setters
- Appropriate training of personnel who are assigned the task of applying critical accounting policies
- Periodic assessment of accounting policies in high-risk areas to evaluate whether they are sufficiently developed, articulated and documented to ensure objective and consistent application
- Audit committee understanding and approval of the critical accounting policies

Deficiencies in the controls over the selection and application of accounting policies are likely to be regarded by auditors as at least a significant deficiency in internal control over financial reporting.

97. What should the Section 404 compliance team consider when documenting controls over estimation transactions?

As noted in Question 91, the SEC defines "critical accounting estimates" as "estimates or assumptions involved in the application of generally accepted accounting principles where the nature of the estimates or assumptions is material due to the levels of subjectivity and judgment necessary to account for highly uncertain matters or the susceptibility of such matters to change; and the impact of the estimates and assumptions on financial condition or operating performance is material." The inherent risk related to these types of transactions warrants careful attention by management.

For estimation transactions, the controls for preventing and detecting errors often will be relatively informal and involve more judgment compared to the controls within and related to other processes. Further, the performance of controls for these transactions may not be documented. When evaluating these controls, the Section 404 compliance team must identify the accounts and estimates that are manually adjusted at the end of each period.

Following are things the Section 404 compliance team should consider and understand when documenting controls over each type of estimation transaction:

- The experience and knowledge of the personnel who prepare the estimate
- The experience, knowledge and objectivity (freedom from bias) of the managers who are responsible for making and reviewing the estimate
- The supporting documentation maintained to support the estimate and the resulting adjusting entries

- Whether the estimation methodology is sufficiently clear to enable consistent application by different company personnel, including the documentation of key assumptions, the support of assumptions with available information and the articulation of guidelines for applying the assumptions
- Whether other processes provide relevant and reliable data for use in calculating the estimation transaction
- Whether changes in the estimate are based on legitimate changes in underlying assumptions and economic and business conditions
- Whether an appropriate expert is used when an estimate involves highly technical or specialized computations and subject matter
- Whether an outside expert is used to obtain an independent determination, e.g., a reserve engineer, an appraisal firm, an actuary, etc.
- The extent to which past estimates have approximated actual results
- Whether the estimate or the methodology for calculating the estimate is refined when comparisons of actual to estimated results indicate a need to do so
- The degree of conservatism applied in executing estimation transactions (including whether management's incentives may have changed since the prior year)
- The variation, if any, in estimation procedures during the year compared to year-end

98. What is the external auditor looking for with respect to the period-end financial reporting process (close the books)?

In Auditing Standard No. 5, the PCAOB states the period-end financial reporting process is vital to financial reporting. The process includes the following:

- Procedures used to enter transactions into the general ledger
- Procedures related to the selection and application of accounting policies
- Procedures used to initiate, authorize, record and process journal entries in the general ledger
- Procedures used to record recurring and nonrecurring adjustments to the annual and quarterly financial statements
- Procedures for drafting annual and quarterly financial statements and related disclosures

The Board states that the auditor should evaluate the following with respect to this process:

- The inputs, procedures performed and outputs of the company's processes designed to produce annual and quarterly financial reports
- The extent of IT involved in the period-end financial reporting process
- The degree of participation from management, including who participates and why
- The number of locations involved in the period-end financial reporting process
- The nature and types of standard and nonstandard adjusting, eliminating and consolidating adjusting entries
- The nature and extent of oversight of the process by management, the board of directors and the audit committee

In summary, the Board requires the auditor to evaluate the period-end financial reporting process. In meeting this requirement, it is likely the auditor will perform a walkthrough of the process. As noted in Question 90, because of the nature of this process, the auditor's focus would be on understanding how transaction totals recorded in the general ledger are ultimately reflected in the financial statements and related disclosures. In addition, the auditor will ordinarily test operating effectiveness of the controls over the period-end financial reporting process only in conjunction with a period-end.

99. What factors are considered when evaluating the design effectiveness of controls?

A generic definition of "design effectiveness" might be as follows:

> The effectiveness of a given documented controls design in achieving relevant objectives (or assertions), including the reduction of risks of nonachievement to an acceptable level.

In a Section 404 environment, a customized definition might be the following:

> The effectiveness of a given documented controls design in achieving relevant financial reporting objectives (or assertions), including the reduction to an acceptable level of the risks of errors or fraud that could result in material misstatements in annual or interim financial statements.

With this customized definition as a context, we can assert that there is a presumption that the documented controls design, if operating properly, would provide reasonable assurance that errors or fraud that could result in material misstatements in annual or interim financial statements would be effectively prevented or detected. Once the critical processes are documented, risks are sourced and control points are identified, the project team is ready to evaluate the effectiveness of controls design for the key controls. The purpose of this step is twofold:

- Assess the effectiveness of the controls design in both reducing the stated risks to an acceptable level and achieving the stated assertions or objectives.
- Document the results of that assessment, including any gaps.

Documentation of the design of controls is vital to the evaluation of design effectiveness. For example, the independent accountant may refuse to issue an audit report without sufficient control documentation on which to base attestation decisions. In its final rules, the SEC stated:

> … a company must maintain evidential matter, including documentation, to provide reasonable support for management's assessment of the effectiveness of the company's internal control over financial reporting. Developing and maintaining such evidential matter is an inherent element of effective internal controls.

In its interpretive guidance, the SEC further states that the determination of whether an individual control, or a combination of controls, adequately addresses a financial reporting risk involves judgments about both the likelihood and potential magnitude of misstatements. When a combination of controls is required to adequately address the risks affecting a financial reporting element, the SEC guidance asserts that management should analyze the risk characteristics of each control.

A suitable form (e.g., a risk and control matrix) should be used to document this evaluation for each critical process. This document normally includes appropriate information with respect to each relevant financial reporting assertion, e.g., specific risks ("what can go wrong?"), description of relevant controls, identification of control owners, assessment of design effectiveness, validation of operating effectiveness and recommendations. The document also would need to be expanded to incorporate risk characteristics of the controls design to enable the evaluation team to consider the potential for control failure. When documenting the controls design, the project team should focus on a combination of controls in achieving a given assertion rather than specific controls in isolation. That said, there may be occasions where a single control is so critical to the achievement of an assertion, it stands alone because if it fails there may not be adequate compensating controls in place.

The completed document is the key deliverable from this step. It addresses four questions with respect to controls design: (1) what are the controls; (2) who owns the controls; (3) how are they rated; and (4) is there a risk of control failure? This document is prepared for all critical processes and is used irrespective of how the processes are documented. For example, if a process owner is able to articulate the risks and controls and prepare the gap analysis without a detailed process map – as might be the case for a simple process – that approach will often be satisfactory.

When assessing the "design effectiveness" of process-level controls and documenting that assessment, consider the following:

- The results of the entity-level controls assessment
- The results of the assessment of general IT controls
- The nature of the identified financial reporting risks or assertions
- The effectiveness of all five COSO components
- The nature and types of errors and omissions identified that could occur, and the effectiveness of the controls in mitigating the risk of these errors and omissions
- The extent of change in the business and its expected effect on internal controls

One other factor to consider is the degree of assurance provided by the identified controls. For example:

- Whether the process, including the controls within the process, is at a minimum at the "defined state" of capability (see Question 104 for explanation). The higher the level of capability, the greater the degree of assurance and sustainability of the internal control structure.
- Whether the identified controls are preventive versus detective and manual versus systems-based. The greater the volume and velocity of transaction processing, the more desirable it is to increase the emphasis on preventive and automated controls. The greater that emphasis, the more assurance the controls provide.
- Whether the identified controls are simple versus complex to operate and/or are operated by experienced versus inexperienced personnel. The simpler the control (in terms of the number of tasks or calculations required to operate it) and the more experienced the personnel executing the control, the more assurance it provides.
- Whether the identified controls apply analytics or utilize sampling techniques versus check all transactions. The more comprehensive the control, the more assurance it provides.
- Whether the control occurs downstream after the transaction is processed or occurs real-time as the transaction is processed. The closer the control to the source, the more assurance it provides.

In summary, there are three important steps to evaluating controls design effectiveness:

(1) Define the financial reporting assertions or control objectives for each significant financial reporting element and source the assertion risks within the critical processes affecting those elements.

(2) Identify the controls, and only those controls, that satisfy each assertion or objective and reduce the assertion risks to an acceptable level.

(3) Determine whether the controls, if operating properly, can effectively prevent or detect the errors or fraud that could result in material misstatements in the financial statements. The standard for this assessment is "reasonable assurance."

100. What factors are considered when evaluating the operating effectiveness of controls?

After the controls design is determined to be effective in reducing financial reporting risks to an acceptable level, selected controls should be validated or tested over an appropriate period of time to ensure they are operating as designed. There are several methods of validating controls – process-owner monitoring, entity-level monitoring by reporting unit or operating unit management, and internal audit validation. Management

must decide which controls are to be validated, how they are to be validated and how often. In considering the likelihood that a control might fail to operate effectively, the SEC's interpretive guidance points out that management should consider the following factors, among other things:

- The type of control (manual or automated) and the frequency with which it operates
- The complexity of the control
- The risk of management override
- The judgment required to operate the control
- The competence of the personnel who perform the control or monitor its performance
- Whether there have been changes in key personnel who either perform the control or monitor its performance
- The nature and materiality of misstatements that the control is intended to prevent or detect
- The degree to which the control relies on the effectiveness of other controls (e.g., general IT controls)
- The evidence of the operation of the control from prior year(s)

Once the key controls have been selected and scoping decisions have been made, unit managers and process owners can conduct periodic self-assessments with web-enabled technology serving as the prime tool for accumulating the results of assessments as of a point in time.

Internal audit plans also are aligned with management's needs for assurances in the financial reporting area. These plans may be executed throughout the year to ensure that control deficiencies can be remediated on a timely basis.

101. Must a company link its key controls directly to financial statement accounts?

No. While Auditing Standard No. 2 was interpreted by some to require this linkage, there is no such requirement in Auditing Standard No. 5. Auditors are likely to link the controls they test with the relevant assertions to which the controls relate. Controls are embedded within processes, and processes feed the significant accounts. Therefore, assertions provide the vital link between accounts and controls, as follows:

- First, link significant ***accounts*** to relevant financial statement ***assertions*** (see Questions 71 and 72).
- Second, link the significant ***accounts*** to the critical ***processes*** that affect them.
- Third, assign the relevant financial statement ***assertions*** to the appropriate ***processes***.
- Finally, show the linkage of the ***controls*** within the ***processes*** to the ***assertions*** affecting the priority ***accounts***.

The objective is to demonstrate that the assertions used at the process level are consistent with the assertions relevant to the accounts affected by the processes. The controls are then directly related to the assertion risks they mitigate.

102. What level of assurance must management attain when reaching a conclusion on the design and operating effectiveness of internal controls?

"Reasonable assurance" is the standard that internal controls must meet. Management must attain this level of assurance when formulating a conclusion regarding the effectiveness of internal controls in achieving specific objectives or assertions. This is intended to be a practical standard. No matter how well designed, most systems of internal controls can only provide reasonable assurance to management and the board of directors. There are

inherent limitations in any internal control system such that absolute assurance is a cost-prohibitive standard, if not an impossible one. Human judgments in decision-making, breakdowns due to human error and simple mistakes, collusion by two or more people, and even management override can circumvent an effective system of internal controls. Reasonable assurance is a more realistic standard than absolute assurance because of these inherent limitations.

The concept of reasonable assurance is built into the definition of internal control over financial reporting adopted by the SEC's rules. If management decides to include a discussion regarding the meaning of "reasonable assurance" in the context of internal controls, the discussion must be presented in a manner that neither makes the disclosure in the report confusing nor renders management's assessment concerning the effectiveness of the company's internal control over financial reporting unclear. (See Question 236.)

103. How does management define "reasonable assurance" for purposes of evaluating the effectiveness of controls?

In its interpretive guidance, the SEC states that "Exchange Act Section 13(b)(7) defines 'reasonable assurance' … as such … degree of assurance as would satisfy prudent officials in the conduct of their own affairs." (See Question 113 for a discussion of the prudent official test.) Therefore, according to the Commission, "reasonableness is not an absolute standard of exactitude for corporate records." Management must exercise its judgment when evaluating whether the level of assurance attained is "reasonable." The SEC also points out that "while 'reasonableness' is an objective standard, there is a range of judgments that an issuer might make as to what is 'reasonable' in implementing Section 404 and the Commission's rules."

According to the SEC, management must bring its own experience and informed judgment to bear in order to design an evaluation process that meets the needs of its company and that provides reasonable assurance for an assessment. For example, implicit in the concept of reasonable assurance is that the assessment of internal controls requires multiple individuals (with the requisite expertise in processes, risks and controls) to evaluate the internal controls, as documented, against specified risks and assertions, and formulate a conclusion that the controls are effective in mitigating risk and achieving assertions. The concept of reasonable assurance also implies consideration by management of the cost of a control and its resulting benefits in terms of reducing risk. Incurring excessive and extreme costs to eliminate risk is not consistent with the concept of reasonable assurance.

104. How should control gaps be identified and summarized?

Control gaps can be identified and summarized two ways. The first and easiest approach is through a Risk and Control Gap Analysis. This approach evaluates the effectiveness of internal controls in preventing or detecting financial reporting errors or omissions. This analysis evaluates the effectiveness of the controls design in reducing identified risks to an acceptable level. It addresses the following questions: What are the risks, what are the controls, who owns the controls, how are they rated and how are they performing? These questions are addressed when evaluating controls design and controls operation, as discussed in Questions 99 and 100, respectively. The analysis may be documented in many ways, such as through the use of the risk and control matrix introduced in Question 99.

A second approach is the Internal Controls Capability Maturity Continuum, which can be used in tandem with the Risk and Control Gap Analysis. The continuum provides a scale for evaluating the sufficiency of a company's internal controls in a given area so that the current state may be contrasted against a desired future state.

The following five capability levels represent states of maturity by which the project team can rate the upstream business processes in which the company's internal controls are embedded:

Impact of Process Maturity on Internal Control over Financial Reporting

Capability Level	Capability Description	Capability Attributes	Section 404 Implications
Optimizing	CONTINUOUS IMPROVEMENT • Continuously improving controls enterprisewide	• Best practices identified and shared • World-class financial reporting processes • Organized efforts to remove inefficiency • External and internal change monitored for impact on control structure	• Internal controls – Integrated framework fully implemented • Entity-level analytics fully operational • Effective monitoring fully operational • Faster decisions on improving controls • Controls preventive and systems-based
Managed	QUANTITATIVE • Risks managed quantitatively enterprisewide • "Chain of accountability"	• Control process performance standards established and managed • Rigorous estimation methodologies and analysis • Process risks are managed quantitatively and aggregated at corporate level • Process-based self-assessment applied	• Controls effectiveness continuously assessed and validated • Process owners report to management • Internal audit plans aligned • Entity-level analytics and monitoring controls emerging • Primary effort directed to high-risk areas
Defined	QUALITATIVE/QUANTITATIVE • Policies, process and standards defined and institutionalized • "Chain of certification"	• Internal control uniform across the entity's processes • Transaction flows documented • Risk of fraud, errors and omissions sourced • Control processes for mitigating risk better documented and integrated	• All groups accountable to use organization's control standards • Remaining *known* gaps closed • Control reports not very robust • Assurance lacking that all deviations from control standards detected
Repeatable	INTUITIVE • Process established and repeating; reliance on people continues • Controls documentation lacking	• Common control framework • Increased controls awareness • Basic policies and control processes established • Process activities are repeating but not necessarily documented	• Quality people assigned to support control activities • Some control gaps identified and fixed • Communication is lacking • Limited monitoring controls and activities • Control structure still not sustainable
Initial	AD HOC/CHAOTIC • Control is not a priority • Unstable environment leads to dependency on heroics	• Reliance on individual initiative • "Just do it" • Ad hoc disclosure activities • Policies not articulated • Few process activities are defined • Institutional capability lacking	• Overemphasis on detective controls • Controls are not periodically evaluated for deficiencies • Success depends on manual efforts and validation by seasoned managers • Gaps result when key people leave

- At the **Initial State**, control is fragmented and ad hoc. The organization manages individual risks and controls in silos and is generally reactive. There is a general lack of policies and formal processes, so the organization is totally dependent on people acting on their own initiative to "put out fires." There is very little accountability at this state. The lack of accountability is either due to the absence of a clearly designated owner of a risk or, because there are so many owners of that risk, no one can be held accountable. There is a general lack of institutional capability, meaning the organization is highly dependent on its people. If any one of its key people leaves, the organization has difficulty replicating what he or she does. The Initial State is rarely sustainable not only because of the high potential for error, but also because the significant inefficiencies that characterize this state drive high costs, many of which may be unknown to management.
- Moving to the **Repeatable State**, the organization's capabilities are improved with a basic policy structure, basic processes and controls, and increased clarity as to defined roles, responsibilities and authorities. Accountability is an issue at this stage because reporting is not rigorous enough to hold people accountable for results. Nevertheless, the processes in place show evidence of uniformity or consistency across segments of the enterprise. The "repetition" that is taking place is a result of increased process discipline and established guidelines. There is still reliance on people at this state. Process documentation is still lacking. This state is also characterized by high costs.
- As we progress to the **Defined State**, policies are further developed and processes are further refined. Processes and transaction flows are documented, risks of errors and omissions are sourced within the processes, and the key controls that mitigate these risks are identified. Known control gaps are effectively closed. If further gaps come to management's attention, they are closed as well; however, there is no assurance that all existing gaps are identified. Process owners are not self-assessing their processes against established management control standards linked to the controls documentation supporting the internal control report. Internal audit plans are not fully aligned with the controls documentation. However, a disclosure creation process is designed, documented and implemented. It is at the Defined State where we see evidence that controls awareness and an increased focus on improving efficiency are taking hold. The foundation is laid for progressing to the Managed State.
- The **Managed State** of capability is fueled by the improved process analysis at the Defined State. The Managed State is more quantitative than the Defined State, with entity-level analytics and monitoring starting to emerge. Quantitative performance measures provide management the basis for determining whether mitigating controls are functioning as intended. The operating effectiveness of control activities is evaluated on (at least) a quarterly basis. Process owners self-assess the controls for which they are responsible and report the results of their assessments to management. Internal audit plans are aligned with management expectations to provide assurances as to the quality of the process owner self-assessments. At this stage, a process-based chain of accountability exists and the appropriate efficiencies are driven into the processes.
- The **Optimizing State** is the highest level of process capability. This state continuously improves on the capabilities developed during the prior states, suggesting that the journey of building control capabilities is one that is ongoing in the face of ever-changing external and internal conditions. The entire organization is now focused on continuous improvement as organized efforts are made to remove inefficiencies with formal cost/benefit analysis applied to all processes and controls. Entity-level monitoring and analytics are fully operational, resulting in real-time reporting, early warning and better decisions. Best practices are identified and shared across the organization. Continuing self-assessments result in continued improvements in the control structure. Process owners use technology to keep the documentation of controls policies, processes, competencies, reports and methodologies current. It is at this stage that the organization fully aligns its policies, processes, people, technology and knowledge to achieve fair and transparent reporting, not just externally but internally as well. Not coincidentally, after incurring the necessary design and implementation costs, this stage achieves the greatest ongoing efficiencies in the design and operation of the processes.

We believe that top-performing companies improve their processes, including their financial reporting processes, to increase quality and reduce risk. Cost reduction, improved quality and reduced risk – often a result of simplifying, focusing and automating processes and eliminating nonessential tasks – enable companies to redeploy their resources to create value for their operations and reduce the overall cost of the finance function. By implementing improved processes, new key performance indicators (KPIs) and effective controls, these companies achieve the largest reduction in risk.

If the organization uses the process maturity continuum to rate its controls rigorously in all key areas affecting financial reporting, this tool is a useful way to pinpoint the gaps based on the level of capability management desires to achieve. When summarizing the results of the assessment of design effectiveness, determine the current state of internal controls for each critical process affecting financial reporting. Management can then decide where on the continuum the company needs to be with respect to each process. For example, assume that the revenue process is at the Repeatable State. Management must decide at what state they want this process to be and by when. In this way, the continuum may be used to identify change management issues as change is often better managed moving from one state to another in stages over time rather than closing gaps all at once. Management may also make the assessment at a more granular level; e.g., in lieu of "revenue processing," management may assess order entry, shipping, billing, costing of sales, commission accounting, etc.

105. What should be done to address control gaps if any are found during the assessment?

Assume the assessment of controls design and operational effectiveness is complete and gaps in key controls have been identified. A control gap results from a conclusion that the controls design is ineffective or only partially effective in providing reasonable assurance that there is less than a reasonable possibility of a material misstatement in the financial statements not being prevented or detected in a timely manner. In other words, the gaps lead to a conclusion that there isn't reasonable assurance that critical financial reporting objectives or assertions are achieved or critical assertion risks are reduced to an acceptable level. This gap is a design deficiency, which arises when a necessary control is missing or an existing control is not properly designed so that even when the control is operating as designed, the control objective is not always met.

A gap also arises when the controls design is effective but the control itself is not operating as designed. This gap is an operating deficiency, which arises when a properly designed control either is not performing as intended, or the person or group performing a control does not possess the necessary authority or qualifications to perform the control effectively. Control deficiencies vary in significance. They may be either inconsequential or significant. If significant, they could also constitute a material weakness.

Deficiencies can also arise over time from process inefficiencies. For example, unnecessary adjustments may arise due to imbalances, errors and omissions occurring upstream in the process. If possible, these unnecessary adjustments should be eliminated. Root-cause analysis can identify areas in the process that must be improved to eliminate the need for adjustments. Such activities, of course, make the closing process more efficient and reduce the risk of financial misstatements, because quality is built into the process upstream rather than inspected in when the books are closed.

So what happens after the evaluation of design and operating effectiveness is completed? An action plan should be developed to close the identified gaps. First, management must design a solution to close the gap. Then management must implement the solution. An action plan for designing solutions to close identified control gaps should differentiate between design and operating deficiencies. For design deficiencies, a detailed design is critical to ensure the proposed solution improves control and meets the company's needs in reducing the critical financial reporting assertion risks to an acceptable level. The design should facilitate identification of the specific tasks, resources (people, technology, processes, etc.) and timeline needed to develop the desired solution, leading to the action plan for implementation. It should identify performance measures to ensure the control performs in accordance with the design. For operating deficiencies, management often must clarify roles and

responsibilities and make sure that control owners have the requisite competence and resources to complete the necessary work. As with design deficiencies, performance measures should be identified to provide evidence of reduced exceptions and deviations.

The plan for ***designing solutions*** to close identified control gaps should include the following steps:

- ***Determine responsibility for design process.*** When control gaps are identified during the assessment of controls design or controls operation, management and the project team should address the following questions:
  - Who should be primarily responsible for key internal control activities requiring improvement?
  - What will be expected of these individuals in closing identified gaps?
  - What will be expected of these individuals after the gaps are closed?
- ***Document revised and improved internal controls.*** Designing solutions may require evaluation of existing processes and developing appropriate revisions to those processes to improve internal controls. The revisions could include improvements to policies and procedures, enhanced competencies, improved reports, more robust methodologies or systems upgrades. Develop detailed descriptions of the revisions and improvements, including an explanation as to how they will close an identified control gap.
- ***Design unit and process-owner monitoring reports.*** The organization should be looking for ways to improve monitoring by unit managers and process owners over time.
- ***Align process-owner roles and responsibilities with relevant objectives.*** Confirm process owner and management acceptance of solution design. Obtain agreement and approval to proceed with implementation.
- ***Align process-owner compensation with performance objectives.*** Process owner buy-in facilitates agreement with detailed solution specifications and deliverables. Management approval ensures that resources will be dedicated to make the solution happen.
- ***Identify and design other improvements.*** Evaluate whether the proposed revisions are sufficiently comprehensive and ready for implementation. A detailed design is critical to ensure the solution improves control and meets management's need for closure.
- ***Develop implementation plan and timeline.*** Determine sequence and timing of planned changes.

Once the solution design is complete, management should proceed with implementation. This phase focuses on implementing specific solutions in accordance with the detailed design specifications. Timing is of the essence. Unnecessary delays should be avoided.

An action plan for implementing solutions to close identified control gaps should also differentiate between design and operating deficiencies. For design deficiencies, management should proceed with implementation in stages in accordance with the company's current and desired state of maturity (see Question 104) and measure performance to ensure that the control operates in accordance with the design. Such remediation efforts will often focus on increasing controls design effectiveness by automating manual controls, improving the mix of preventive and detective controls, placing the point of control at the source of the risk, simplifying overly complex control procedures, consolidating and centralizing control procedures, and improving monitoring controls and analytics.

For operating deficiencies, management often will focus on updating and publishing policies to clarify roles and responsibilities, implementing hiring and training initiatives to ensure the requisite competence and resources are brought to bear, and measuring performance for evidence of reduced exceptions and deviations.

The plan for ***implementing solutions*** to close identified control gaps should include the following steps:

- ***Develop training guidelines and documentation.*** Guidelines should be defined at sufficient granularity for process-owner approval and acceptance.

- ***Obtain management acceptance of the solution.*** Management acceptance of the developed solution is obtained, as well as a commitment to proceed with implementation in the business environment, subject to any approved changes.
- ***Provide necessary training.*** Training is a vital component of the implementation process.
- ***Develop, test and roll out improvements.*** The "build-and-test" phase results in the following deliverables: solution components, solution documentation and documented test results. A built and tested solution is ready for rollout across the organization. Any issues arising during tests in the business environment should be addressed and documented. The rollout strategy should address any issues based on test results so that the completed solution can be implemented within the appropriate processes and its operation verified before completely turning over maintenance and administration of the solution to process owners as part of their new and ongoing duties.
- ***Apply continuous process-improvement methodology.*** Measure performance of the implemented solution to ensure it has been implemented in accordance with design specifications. Verify that the implemented solution meets or exceeds management's approved functional/performance expectations.

106. How does a company define a "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. When testing controls to determine whether they are operating effectively, evaluators will note test exceptions. The existence of control exceptions does not necessarily mean a control deficiency exists. Internal controls are not expected to operate perfectly, all the time, to be effective. While the SEC's interpretive guidance recognizes the inherent limitations of internal control, the Commission's focus is on material weaknesses.

107. How are compensating controls considered?

According to the SEC's interpretive guidance, compensating controls are defined as follows:

> [C]ontrols that serve to accomplish the objective of another control that did not function properly, helping to reduce risk to an acceptable level. To have a mitigating effect, the compensating control should operate at a level of precision that would prevent or detect a misstatement that was material.

The SEC states that management should evaluate the effect of compensating controls when evaluating whether a deficiency, or a combination of deficiencies, is a material weakness. For this purpose, the compensating controls must be operating effectively, i.e., there must be evidence that the controls are operating effectively.

Note that compensating controls are *not* considered when determining whether a control deficiency exists. Control deficiencies must be considered individually and in isolation of the performance of other controls. Compensating controls are appropriately considered when evaluating whether a significant deficiency or a material weakness exists.

108. How does a company define a "significant deficiency" in internal control?

The SEC and PCAOB define the term "significant deficiency" as follows:

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

Note that there isn't a probability threshold in the above definition. The SEC states that it is not necessary for the definition to include a likelihood component, as "it could have the unintended effect of diminishing the use of appropriate judgment by management and independent auditors in performing the [Section 404] evaluation." The SEC also has stated that "excluding a likelihood component from the definition reduces the chance that

management or independent auditors will design and implement evaluations or audits for the purpose of identifying deficiencies that are less severe than material weaknesses."

The Commission's clear statement of intent to avoid unintended consequences is important. It clarifies that the SEC's primary focus in defining a significant deficiency is on the communications required to take place among management, audit committees and independent auditors. That focus is directed to the importance of a matter for purposes of elevating it to the attention of the appropriate parties and decision-makers rather than on executing an intricate analytical process using specified criteria. In choosing to vary the framework for defining a significant deficiency from the one used to define a material weakness, the SEC stated that it wanted to "allow for, and indeed encourage, sufficient and appropriate judgment by management to determine the deficiencies that need to be reported to the independent auditor and the audit committee." See Question 109 for a discussion of the framework for defining a material weakness.

Examples of control deficiencies that might be considered at least a significant deficiency in internal control over financial reporting, and therefore worthy of elevation to parties responsible for oversight of financial reporting, include deficiencies in:

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

Because there is not a likelihood component in the definition of a significant deficiency, some may assert that a matter does not merit elevation to parties responsible for oversight of financial reporting if it is not at least "reasonably possible" of occurrence. However, evaluators should be careful jumping to that conclusion. For example, the lack of a probability threshold also could suggest that a matter that could result in a material error but is not "reasonably possible" of occurrence at the present time might warrant elevation and is therefore a significant deficiency. Obviously, this is a matter requiring the exercise of judgment, which is exactly where the SEC decided to leave it. One possible result will be different points of view between management and the auditor, as reasonable men and women often differ in matters involving significant judgment. Different views will foster more dialogue, which is probably the end result desired by the Commission.

In summary, the SEC and PCAOB concluded that a deficiency in internal controls is significant if it could adversely affect the company's financial reporting process and the critical processes that feed data and information to the financial reporting process to the point that persons responsible for oversight of the company's financial reporting would be concerned about it. Consistent with the Board's risk-based approach, the context for evaluating the significance of a deficiency in internal control over financial reporting is management's assertions as to the fairness of presentation of financial condition, results of operations and cash flows, as expressed in or implied by both the financial statements and the executive certifications required under Sarbanes-Oxley Section 302. In practice, once the Section 404 evaluation is completed, and a conclusion is reached as to whether there are any material weaknesses, then the evaluator reviews the remaining control deficiencies and determines whether there is a deficiency, or combination of deficiencies, that is important enough to elevate to the appropriate decision-makers. Whether a significant deficiency is in design or in operation, it should be corrected as quickly as possible if it provides an early warning of a condition that could become a material weakness in internal control.

Both management and the external auditor are required to report significant deficiencies to the audit committee. In addition, management is required to report significant deficiencies to the external auditor. From a practical standpoint, if management identifies a control deficiency that it believes *could be* a significant deficiency, it should discuss that deficiency with the internal auditors, the external auditors and the audit committee before finalizing a conclusion as to the severity of the deficiency. This is particularly important because the independent public accountant must report to the audit committee all significant deficiencies identified in

connection with the audit. Management would not want a situation where the independent public accountant reports significant deficiencies at the conclusion of the audit that were not reported by management to the auditors and audit committee during the year. This situation could potentially increase management's exposure if these matters resulted in errors or omissions in the company's interim financial reporting and were not reported on a timely basis, particularly if they came to management's attention earlier.

109. How does a company define a "material weakness" in internal control?

In its interpretive guidance, the SEC defines a "material weakness" as follows:

> [A] deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis.

To clarify, a "reasonable possibility" of an event exists when the likelihood of the event occurring is either "reasonably possible" or "probable." This definition lays the foundation for management's year-end assessment under Section 404, which is based on whether the controls will fail to prevent or detect a material misstatement (or omission) on a timely basis. Whether or not a misstatement actually has occurred is not germane to this assessment.

The SEC and PCAOB listed the following four indicators of a material weakness in internal control over financial reporting:

(1) Identification of fraud, whether or not material, on the part of senior management

(2) Restatement of previously issued financial statements to reflect the correction of a material misstatement

(3) Identification of a material misstatement in financial statements in the current period in circumstances that indicate the misstatement would not have been detected by the company's internal control over financial reporting

(4) Ineffective oversight of the company's external financial reporting and internal control over financial reporting by the company's audit committee

In addition, there are other potential indicators the audit firms are likely to consider. Following are two examples:

(1) The internal audit function or the risk assessment function is ineffective at a company needing such a function to have effective monitoring and risk assessment

(2) Significant deficiencies that have been identified and remain unaddressed after some reasonable period of time[3]

[3] At the time this publication went to print, there was no authoritative guidance as to what constitutes a "reasonable period of time." There are many factors to consider in this regard, including the complexity of the deficiencies, the difficulty in fixing them and the progress made to date by management. If the control deficiency(ies) in question presented a difficult decision for management to classify them as a significant deficiency (rather than a material weakness), another factor might be management's disclosures. For example, some companies provide full disclosure about their significant deficiencies when they are on the borderline in terms of being classified as a material weakness. Clearly, the best practice is to remediate the significant deficiencies on a timely basis. As significant deficiencies are remediated, it is vital that the external auditor and audit committee see clear evidence of a plan as well as management's commitment to resource that plan and make it happen. If companies choose to allow their significant deficiencies to continue without justification, they expose themselves to unexpected surprises from the attestation process. We believe that the primary factor the auditor will consider is likely to be the pervasiveness of the issue, for example, general IT.

A Framework for Evaluating Deficiencies

The SEC's and Board's framework for evaluating deficiencies in internal control over financial reporting is therefore based primarily on an assessment of the severity of the potential misstatement, with the likelihood of occurrence a factor only when considering whether a deficiency is a material weakness. When evaluating whether the likelihood a deficiency could result in a misstatement of an account or disclosure is at least reasonably possible, many factors are considered including:

- The nature of the financial statement accounts, disclosures and assertions involved, e.g., suspense accounts and related party transactions involve greater risk
- The susceptibility of the related assets or liability to loss or fraud, resulting in increased risk
- The subjectivity, complexity or extent of judgment required to determine the amount involved, i.e., the greater subjectivity, complexity or judgment (as with an accounting estimate), the more risk
- The cause and frequency of known or detected exceptions for the operating effectiveness of a control, including the results of controls testing
- The interaction or relationship of a control with other controls, i.e., the extent of interdependence or redundancy of the control (such as the dependency on general IT controls)
- The interaction of the deficiencies, e.g., whether two or more deficiencies could affect the same financial statement accounts and assertions
- The possible future consequences of the deficiency

When evaluating whether the magnitude of a potential misstatement is material to either interim or annual financial statements, many factors are considered including:

- The financial statement accounts or the 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

Note that both quantitative and qualitative factors, as outlined in our response to Question 53, are considered when evaluating the materiality of a potential misstatement. For purposes of applying quantitative factors to the assessment of the severity of a control deficiency, or combination of deficiencies, the issue is one of considering the magnitude of the misstatements that are reasonably possible of occurring and would not be prevented or detected on a timely basis due to the absence of controls. With respect to evaluating the potential for overstatement, the maximum amount is the recorded amount. The recorded amount, however, is not a limitation on the amount of potential understatement.

In the final Section 404 rules, the SEC points out that a "material weakness" and a "significant deficiency" both "represent deficiencies in the design or operation of internal control that could adversely affect a company's ability to record, process, summarize and report financial data consistent with the assertions of management in the company's financial statements, with a 'material weakness' constituting a greater deficiency

than a 'significant deficiency.'" Due to the need for guidance, the SEC and PCAOB provided, through their respective definitions of these terms, the following framework:

	Severity	Likelihood
Material Weakness	Material	Reasonably Possible (2) (3)
Significant Deficiency	Important Enough to Elevate (1) (4)	N/A (5)
Insignificant Deficiency	Not Important Enough to Elevate	Not Relevant

(1) Less severe than a material weakness, but important enough to merit the attention of those responsible for financial reporting oversight.

(2) The likelihood is either "reasonably possible" or "probable."

(3) Replaces "more than a remote likelihood."

(4) Replaces "more than inconsequential."

(5) Because a probability threshold is not explicit in the definition of a significant deficiency, control deficiencies might warrant elevation if they could result in (a) a material error that is not "reasonably possible" to occur at the present time, (b) an error that is not expected to be material at the present time but is at least "reasonably possible" to occur, or (c) a matter that is sensitive (such as fraud, influence payments, etc.).

As discussed further in Question 108, the framework points out that an explicit probability threshold is not necessary when evaluating a significant deficiency.

What's the message? Significant judgment is required when formulating a conclusion that a control deficiency, or combination of deficiencies, is a material weakness. The SEC did not provide any "bright line" tests. For purposes of Section 404, the primary objective after a control deficiency is identified is to determine whether it is a material weakness, either alone or in combination with other deficiencies. The assessment of the remaining deficiencies that are not material weaknesses is primarily around whether to elevate them to the attention of those individuals responsible for financial reporting oversight. For purposes of this evaluation, both the SEC and the Board assert that an aggregation of deficiencies could constitute a material weakness in a company's internal control over financial reporting.

Needless to say, this is a complex determination that often must consider the financial statements taken as a whole and the overall financial reporting picture before an informed conclusion can be reached. There are many issues that come into play, *beyond the evaluation of the likelihood and magnitude of one or more identified control deficiencies*. We believe that there are four issues that are especially important for management to consider beyond likelihood and magnitude:

- ***Direct impact on achievement of relevant assertion(s).*** To warrant a material weakness conclusion, a control deficiency, or combination of deficiencies, must directly impact the achievement of relevant financial reporting assertions. These deficiencies usually pertain to the so-called "key controls" on which management places reliance for purposes of concluding that the relevant assertions are met. Deficiencies in controls that relate only indirectly to the achievement of relevant financial reporting assertions typically affect the effectiveness of other controls as part of the overall design of the internal control structure; however, one or more deficiencies in these so-called "indirect controls" do not in and of themselves comprise a material weakness. Examples of such controls include entity-level controls relating to the control environment and certain general IT controls.
- ***Existence of compensating controls.*** Control deficiencies may be categorized as relating to either a preventive control or a detective control, depending on management's selection of the key controls. Sometimes, preventive control deficiencies may be offset by other preventive controls or by properly designed and

effectively operating detective controls. For example, if a company having deficient internal controls with regard to tracking inventory quantities always takes a physical inventory at the end of each quarter (i.e., each reporting period), this control deficiency might be fully mitigated by the detective control. A detective control serves as a compensating control if it operates at a level of precision that results in the detection and correction of a material misstatement to annual or interim financial statements before the statements are issued to the public.[4]

- ***Presence of other control deficiencies.*** The definition of a material weakness focuses on both a single condition as well as those circumstances in which several control deficiencies, which are individually immaterial, create the possibility that the combined effect of errors that could result from the deficiencies would be material to the financial statements. Both the SEC and PCAOB have reinforced this point of view when referring to a "combination of deficiencies." This point of view suggests that aggregation of multiple deficiencies may be necessary, depending on a company's facts and circumstances.
- ***The judgment expected of a prudent official.*** The judgment expected of an informed and objective prudent official who is knowledgeable of the matters in question is the ultimate test of whether a control deficiency, or combination of deficiencies, is a material weakness. The question is whether a reasonable and competent third party would reach a conclusion, after a careful evaluation of the facts, that a material weakness exists. See Question 113.

Other Issues to Consider

While the above issues are especially critical, along with the likelihood and magnitude of a deficiency or a combination of deficiencies, there are other influencing factors that also should be considered by management:

- ***The effectiveness of the overall control environment.*** The overall operating environment and management attitude regarding internal control over financial reporting are important factors. A deficiency in a specified area would be considered much more significant when the control environment is weak (for example, incompetent personnel and/or general understaffing, high employee turnover, liquidity problems, lack of written policies and procedures, lack of senior management concern about controls, excessive reliance on manual detection controls, etc.) than when the environment is strong and well controlled due to established policies, documented procedures, competent personnel, adequate training, proper supervision and prompt follow-up on issues.
- ***Nature of assets at risk.*** The nature of the assets that might be affected by a control deficiency, or combination of deficiencies, is another important consideration. Attributes such as mobility, salability and alternative uses to others can affect the assessment of probability for misappropriation. For example, an inventory of diamonds is certainly more subject to misappropriation than an inventory of partially completed construction equipment. Consequently, failure to achieve certain control objectives regarding the safeguarding of assets in the case of the former generally will be of greater concern than the latter in assessing the probability that errors or irregularities in amounts material to the financial statements could occur and not be detected by employees in the normal course of performing their assigned functions.
- ***The extent of changes in company practices and procedures.*** The extent of recent changes, if any, in the company's accounting procedures or business practices is yet another factor to consider. For example, significant changes in operations, personnel, procedures and/or accounting systems not only increase the potential for material errors in the processing of transactions, but also reduce the chances for detection when controls are

[4] Over time, detective controls should not be relied on to the exclusion of preventive controls. In a mature, well-controlled company, there are usually effective, systems-based controls in place to control errors at or near the start of information flows (an example of controlling risk at the source). If a company doesn't implement the right controls at the start of the transaction flow (i.e., the control point is not at the source of the risk), it can be costly and inefficient – not to mention risky – to find and fix errors later. The internal control structure is not as sustainable as it should be if it is totally reliant on detective controls.

generally weak. Conversely, even in a situation in which some control deficiencies are present, if there have been no changes in processing routines or business practices, the probability that material errors could occur and go undetected by detective controls may not be as great as in the former situation. This is why excessive reliance on manual, ad hoc processes can result in a sustainability issue during stressful times.

Notwithstanding the preceding discussion, the list of four "indicators" provided by the SEC, as noted in the beginning of this response, also must be considered. The independent auditor will take into account these indicators as well as factors related to the integrated audit required by the PCAOB when evaluating whether a material weakness exists. For example, the auditor must consider the results of substantive audit tests. If there are material audit adjustments, the independent public accountant (and management) must review the nature and root causes of those adjustments to determine whether they result from a control deficiency. To illustrate:

- Proposed adjustments that are the result of fraud (e.g., intentional misstatements, misappropriation of assets or illegal acts) may be indicative of a material weakness. The SEC has stated that materiality is not a factor if senior management is involved.
- Proposed adjustments that result from inadequacies in controls over transaction processing and their summarization in the books and records ordinarily would be indicative of a control deficiency, the magnitude of which would depend upon consideration of other factors, as discussed in this response.
- Proposed adjustments involving accounting estimates that result from a flawed process, incompetence of company personnel or inaccuracies in the underlying data upon which the estimate is based ordinarily would be indicative of at least a significant deficiency and, depending on the magnitude, could possibly be a material weakness.
- When an assertion regarding a priority financial reporting element is not met, at least a significant deficiency in internal controls exists and possibly a material weakness exists. For example, assume there is a reasonable possibility that material routine transactions are not processed in a manner to satisfy the completeness and accuracy assertion such that it is reasonably possible that a material error could occur. That condition is at least a significant deficiency and is possibly a material weakness if management is unable to determine that adequate compensating controls are in place (see Question 107).
- Proposed adjustments that relate to (a) unique and/or complex transactions for which the applicable generally accepted accounting principles are similarly complex and highly judgmental to apply, or (b) estimates for which there is little historical experience and therefore require the use of significant judgment as to the outcome of future events, may or may not be indicative of a control deficiency. For example, a proposed adjustment relating to a difference of opinion between the independent public accountant and management as to the need for and/or amount of an accrual for a significant and unusual uncertainty (e.g., litigation) may not constitute a control deficiency if there aren't any underlying questions about the integrity of the fact base and the audit committee has been sufficiently involved in the discussions.

We expect situations where a material audit adjustment or restatement of previously issued financial statements is not attributed to a failure in internal control to be rare in practice. In these situations, the independent public accountant's experience with the entity may be a consideration. For example, does the auditor's experience with the entity indicate that management's processes for making accounting estimates and measuring values that involve significant judgment consistently result in estimates and measures that are overly optimistic, misstated or intentionally biased? Still another factor is the nature, timing and extent of the audit tests the independent public accountant must perform to reduce residual audit risk. For example, the severity of an identified control deficiency is often reflected in the amount of audit testing deemed necessary by the auditor to reduce residual audit risk to an acceptable level as of the audit date. The more extensive the procedures, the larger the sample size, and the closer the timing of the work to the balance sheet date, the more likely that the control deficiency is a severe one. These and other considerations may have a bearing on the auditor's judgment regarding whether the severity of a control deficiency warrants a conclusion that the deficiency is a material weakness, and are beyond the control of management if the conditions giving rise to the deficiency remain unabated.

Because of the complexity of these issues and the extent of judgment involved, management should consult with the independent public accountant and the audit committee.

110. Why is the distinction between a significant deficiency and a material weakness so important?

If a deficiency is a significant deficiency, management must disclose it to the auditors and audit committee as soon as practicable. Generally, disclosure to investors is not required of a significant deficiency, unless (a) the remediation process materially affects or is reasonably expected to materially affect internal control over financial reporting, or (b) the significant deficiency when combined with other deficiencies is considered a material weakness and disclosure of the significant deficiency is necessary to adequately explain the material weakness.

If a deficiency is a material weakness, management must disclose it to the auditors and audit committee as soon as practicable. In addition, if the deficiency is uncorrected as of year-end, management cannot issue a positive assertion in the company's internal control report and the external auditor must issue an adverse opinion in the attestation report. Generally, disclosure to investors is required because there is a presumption that the remediation process usually materially affects or is reasonably expected to materially affect internal control over financial reporting.

The distinction between these two types of control deficiencies is important because of the obvious impact on disclosure. It is also important because, in practice, reasonable men and women can differ in distinguishing them. For example, what is a "reasonable possibility"? What is the meaning of "significant"? What is "material"? How are deficiencies "aggregated"? There is such a significant level of judgment to be applied in the process of answering these and other questions, management is advised to fix significant deficiencies as soon as practicable rather than letting them accumulate unresolved. Management should avoid the scenario of having many unresolved significant deficiencies to discuss with the independent auditor at the end of the reporting year.

111. Is it possible for a material weakness reported in a prior year to be classified as not a material weakness in the current year, even though it has not been fully remediated?

Assume Company X reports three material weaknesses in 2006. At the conclusion of the 2007 assessment process, management analyzes and aggregates deficiencies for the year for purposes of formulating their assessment. Assume further that new personnel and new controls were put in place during 2007. It is clear the situation is improved; however, a full remediation has not occurred because of a conclusion that the newly implemented controls are not sufficient to address the relevant financial reporting assertions (control objectives). In this circumstance, can management conclude that the identified deficiencies as of the end of 2007 are no longer material weaknesses?

Paragraph 42 of Auditing Standard No. 4, *Reporting on Whether a Previously Reported Material Weakness Continues to Exist*, states:

> Management may conclude that a previously reported material weakness no longer exists because it has been reduced to a significant deficiency. If management does not plan to correct the significant deficiency within a reasonable period of time, the auditor is expected to evaluate whether the remaining significant deficiency could be indicative of a material weakness in internal control over financial reporting.

Paragraphs B32 and B36 of Auditing Standard No. 4 also are required reading on this matter.

This literature clearly conveys the notion that the PCAOB envisioned that circumstances could arise where a deficiency or significant deficiency could continue to exist. This literature is significant because the Board is acknowledging that management can reach a conclusion of this nature. Paragraph 42 also suggests that management needs to have a plan to resolve the significant deficiency. This is not just any significant deficiency – it is a significant deficiency that was once a material weakness.

These circumstances should be rare. They are particularly messy for purposes of public disclosure because the ensuing discussion of the circumstances in the public record is not as clear as one that states the material weakness is remediated. That said, at the end the current year, a *new* evaluation of severity of existing control deficiencies takes place. Just because a material weakness hasn't been completely resolved does not necessarily mean that a material weakness condition continues to exist.

If management goes forward with a conclusion that a material weakness is now a significant deficiency, we recommend the following:

- Management should consider carefully everything done since the end of the previous year and evaluate the achievement of the control objectives or financial reporting assertions that were previously unmet as a result of the material weakness. If this evaluation points to compensating controls, there should be clear and convincing evidence that such controls are functioning effectively in addressing the objectives or assertions in question. Any remaining control deficiencies should be evaluated as to severity and likelihood.
- Management should be careful with a rationale that "even though the financial reporting assertion or control objective is not met, the likelihood of occurrence is less." The standard management must follow is "can we explain our rationale to an objective third party?"
- Management will need to disclose the following for each material weakness reported in the prior year:

  (1) The nature of the material weakness

  (2) The remediation they have done to date

  (3) Their conclusion that the material weakness is now a significant deficiency, with an appropriate explanation as to what this assertion means

  (4) The basis for their conclusion (because disclosure of (3) signals the deficiency previously reported as a material weakness has not been fully remediated)

  (5) The remaining remediation plans and the timing of completion

  Because (3) and (4) are particularly awkward disclosures, we do not believe that many companies will take this approach.

Most companies report against the material weakness and disclose their remediation efforts until the problem is fixed. Given that this "straight-path" approach is easy for investors to understand, management should consult with SEC counsel to get their perspective before taking this alternative "winding path."

112. Is a significant deficiency no longer as important given the SEC's redefinition of the term and focusing of the Section 404 compliance process on identifying material weaknesses?

The SEC has stated that the central purpose of the Section 404 evaluation is to assess whether there is a reasonable possibility of a material misstatement in the financial statements not being prevented or detected on a timely basis by the company's internal control over financial reporting. Management's assessment is, therefore, based on whether any material weaknesses exist as of the end of the fiscal year. The PCAOB also states the following in Auditing Standard No. 5:

> [T]he auditor must plan and perform the audit to obtain competent evidence that is sufficient to obtain reasonable assurance about whether material weaknesses exist as of the date specified in management's assessment.

The question arises as to whether significant deficiencies are less important, given the SEC's and PCAOB's direction. Overall, significant deficiencies remain relevant because the Section 302 executive certification requires management to disclose them to the audit committee and the auditors. The SEC and PCAOB decided

to modify the definitions of "material weakness" and "significant deficiency" to simplify and clarify the authoritative literature and eliminate misunderstandings that were leading some companies and auditors to perform too much work. Accordingly, several important changes were made:

- The definition of a material weakness no longer refers to "a significant deficiency or a combination of significant deficiencies" because neither the SEC nor the PCAOB want management planning the company's assessment process and the auditors designing the audit to search for significant deficiencies. Therefore, the definition of a material weakness now refers to "a control deficiency or a combination of control deficiencies."
- The definition of a material weakness now focuses on "at least a reasonable possibility" in lieu of "more than a remote likelihood." Furthermore, the definition of a significant deficiency now refers to a deficiency that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the company's financial reporting. The message we can draw from these changes is clear: Management and auditors need to focus their line of sight on whether there is at least a reasonable possibility of a material misstatement in the financial statements, which is the level of likelihood and severity for a material weakness to exist under Section 404. The use of the "more than a remote likelihood" threshold in the definitions of a significant deficiency and a material weakness led some companies and auditors to concern themselves with hypothetical situations that either have not occurred or are not likely to occur. That was never the intent of the Commission or the Board. Further, the focus on severity now provides for management to exercise judgment. When control deficiencies surface during the assessment process, management should eliminate consideration of deficiencies where the potential impact is not significant enough to warrant attention.
- The SEC and PCAOB discarded the "at least a de facto significant deficiency" rule applied under Auditing Standard No. 2 to the list of indicators of a material weakness, because some argued the rule took away the ability to conclude that a control deficiency did not even exist in these circumstances. That issue was part of the reason why financial restatements have almost always resulted in a material weakness determination.
- In their respective proposing releases, the SEC and PCAOB clarified that the issue around uncorrected significant deficiencies being a strong indicator of a material weakness is in reality a potential problem with the control environment. This point of view wasn't intended to de-emphasize the importance of a significant deficiency as much as it was intended to clarify why this condition was an indicator of a possible material weakness. In their final releases, the SEC and PCAOB deleted this situation altogether from the list of indicators of a material weakness. However, it still remains an issue auditors could raise in certain circumstances.

When evaluating the severity of identified control deficiencies, the conclusion may arise that the deficiencies comprise one or more significant deficiencies and do not result in a material weakness. That conclusion is an incidental one resulting from evaluating the severity of the deficiencies identified by the assessment process, and is not a result of having planned the review or conducted the assessment to find significant deficiencies. Going forward, when the results of management's Section 404 assessment are evaluated or the results of an audit of internal control over financial reporting are evaluated, the evaluation process is one of determining whether the identified deficiencies are individually, or in the aggregate, a material weakness. The requirement to aggregate related deficiencies when evaluating whether a material weakness exists does not mean that management should plan the assessment or auditors should design their audits to detect significant deficiencies. If a material weakness does not exist, then a determination is made as to whether the identified deficiencies are important enough to warrant attention by personnel responsible for financial reporting. If any of the deficiencies meet this severity test, they are considered to be significant deficiencies and are handled accordingly.

Rather than de-emphasize the significant deficiency classification, the SEC's and PCAOB's changes fine-tune the process to address what's important under Section 404. Management is still required to issue a written representation to auditors that they have disclosed all significant deficiencies in accordance with Section 302 of Sarbanes-Oxley. Auditors are also required to communicate in writing to management and the audit committee any significant deficiencies they identify during the audit.

113. What is meant by the "prudent official test"?

Exchange Act Section 13(b)(7) defines "reasonable assurance" and "reasonable detail" as such level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs. The term is often used to describe the adequacy of books and records pursuant to Section 12 of the Exchange Act, which requires companies filing reports pursuant to Section 15(d) to make and keep books, records and accounts, which, in reasonable detail, accurately and fairly reflect the registrant's transactions and dispositions of assets. Congress adopted the prudent man qualification in order to clarify that the standard for documents and records does not connote an unrealistic degree of exactitude or precision. Therefore, the concept of reasonableness of necessity contemplates the weighing of a number of relevant factors, including the costs of compliance.

When defining a material weakness in its guidance to management, the SEC discussed the implications if a control deficiency would prevent prudent officials in the conduct of their own affairs from concluding that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in accordance with generally accepted accounting principles. In such instances, the SEC notes that the deficiency is at least a significant deficiency. Thus, the securities laws and the SEC guidance refer to the "prudent official test" in the context of defining reasonable assurance, the level of necessary detail of documents and records, and the evaluation of control deficiencies.

We believe that a prudent official is a "reasonable person" (a term defined in case law) who specifically operates within a business context of one who understands the intricacies of the financial reporting process and, through that understanding, is equipped to evaluate the costs and benefits of implementing controls and evaluating control deficiencies in light of the requirements of reliable financial reporting and the needs of investors for fair and transparent financial reports. Therefore, a prudent official is one who is able to evaluate the level of detail and the degree of assurance that would be necessary in the circumstances to determine that transactions are recorded properly.

What is significant about a "prudent official" is not what it is or who it is, but who it isn't. A prudent official is not management. It is a benchmark against which management is evaluated in the eyes of an objective third party, whether that third party is an auditor, a regulator, a judge, the plaintiff's bar or a jury. It suggests one who is serious about fair and transparent financial reporting and is committed, as an SEC official said in a December 2004 speech, to "tell the truth, the whole truth and nothing but the truth."

114. What must management do if there is a "significant deficiency" or a "material weakness" in internal control?

If a "significant deficiency" or a "material weakness" in internal control exists, management must do three things. First, management must communicate this condition in the company's internal controls to the independent public accountant and audit committee. This disclosure is a requirement under Section 302 of Sarbanes-Oxley. Second, management needs to correct the condition within a reasonable period of time while ensuring that financial reports issued during that period of time are reliable. Finally, management must disclose the actions taken to correct the condition, if such actions constitute a change that materially affects (or is reasonably likely to materially affect) internal control over financial reporting. If a material weakness exists as of year-end, it must be disclosed to investors in accordance with Section 404.

When disclosing a material weakness, it should be noted that it should be clear that the control deficiency is described as a material weakness. In 2005, a member of the SEC staff stated that the SEC staff was watching closely the disclosure trends and taking action if they concluded a registrant "prettied up" its disclosures. For example, if a material weakness exists, it must be disclosed as a material weakness and not as an improvement or as something else, such as an "issue" or a "problem." The SEC's motivation is to ensure that registrants use the correct terminology.

115. Which changes to internal control over financial reporting "materially affect" or are "reasonably likely to materially affect" the effectiveness of the company's internal control over financial reporting for purposes of complying with the Sarbanes-Oxley Act?

The SEC has chosen not to provide specific guidance on this question. Examples of changes in the company's operations that might impact the effectiveness of internal controls include significant loss or change of senior management, employee turnover, downsizing, new systems, significant acquisitions, the effects of unexpected catastrophic events and the effect of growth on the adequacy of existing disclosure processes. As discussed in Questions 173 and 176, significant improvements in internal control require disclosure if they materially affect, or are reasonably likely to materially affect, the effectiveness of the company's internal control over financial reporting.

116. What is management's responsibility for changes in internal controls that could affect the adequacy of internal controls after the date of management's assessment?

The SEC's rules for Section 302 executive certifications, as revised for the final Section 404 rules, state that the company must disclose any change in its internal control over financial reporting that occurred during its most recent fiscal quarter that has materially affected, or is reasonably likely to materially affect, the effectiveness of the company's internal control over financial reporting. This requirement suggests a critical need for companies to understand the impact of change on their internal control structure. For example, rapidly growing businesses need to be sensitive to the increased demands of growth on improving the infrastructure supporting internal control over financial reporting.

117. Can management rely on the self-assessments of process owners as the sole basis for rendering the annual internal control report?

The SEC observes in its interpretive guidance to management that self-assessment is a broad term that refers to different types of procedures performed by various parties with different levels of objectivity. For example, one company might require an assessment by the personnel responsible for performing the key controls. Another company might require assessments and tests of controls by members of management who are not responsible for performing the controls. Still another company might require independent tests of self-assessment results by internal audit. Thus, self-assessment activities may be carried out by different individuals with varying degrees of objectivity. The message is that the sufficiency of the evidence derived from self-assessment, for purposes of supporting management's assertions in the internal control report, depends on how it is implemented and the objectivity of those performing the assessments.

We believe that self-assessments, whether by control owners or by process owners or managers who are not directly responsible for executing the control, can be a significant part of the certifying officers' evaluation but should not be the sole basis for their evaluation. Other sources of evidence include effective entity-level analytics and monitoring controls, the results of internal audit testing and other separate independent evaluations performed from time to time.

See our response to Question 144 for further discussion.

118. If pervasive entity-level and monitoring controls are designed and operating effectively, to what extent does management need to evaluate specific controls at the process level?

COSO requires an evaluation at both the entity level and process level. Thus, for significant processes impacting priority financial reporting elements, management needs to evaluate the effectiveness of internal controls at the process level even if entity-level controls are strong. Effectively functioning entity-level controls can support a conclusion to do less work at the process level for insignificant or lower risk processes. In practice, auditors

have often applied these company-level controls as a justification for minimum testing scopes at the process level. If the entity-level controls are not effective, then scopes at the process level are expanded.

As more fully discussed in Question 81, the SEC's interpretive guidance states that some entity-level controls are designed to operate at the process, transaction or application level and might adequately prevent or detect on a timely basis misstatements in one or more financial reporting elements. If these controls – which are often monitoring controls – are effective in reducing financial assertion risks to an acceptable level for one or more significant financial reporting elements, then management may rely on them in lieu of testing transaction processing controls. Therefore, this assessment is made using financial reporting assertions as a context. If the entity-level and monitoring controls provide reasonable assurance that the financial reporting assertions are met and it is determined that those controls are operating effectively, the SEC guidance makes it clear that no further testing is required for those particular assertions.

119. What does it mean that the Section 404 assessment is based on a point in time and why is it important?

A point-in-time assessment is an evaluation of internal control effectiveness as of a specific date, usually at the end of a reporting period, i.e., a year-end date or quarter-end date. A point-in-time assessment is different from an assessment of controls for a period of time, say the three months of a quarter or the 12 months of a year. A benefit to a point-in-time assessment is to give management an opportunity to develop and test controls during the course of a financial period, with sufficient time to correct significant control deficiencies prior to the "point in time" at which they must be evaluated. Notwithstanding this advantage, management must disclose to investors any actions that have materially affected, or are reasonably likely to materially affect, the company's internal control over financial reporting.

From a practical standpoint, the test plans of many companies spread the effort out over a period of time rather than confine it to year-end. So why the emphasis on a point in time? The point-in-time focus was written into the statute, so the SEC had to work within that construct. As much as commenters have expressed concern about the costs of complying with Section 404, the costs would be even greater if the statute had required a *period* assessment in lieu of a *point-in-time* assessment. Under a point-in-time assessment, the auditor's testing is not as extensive and timing can be directed in subsequent years to the fourth quarter, although as a practical matter auditors may spread out their testing over the third and fourth quarters. It is likely the legislators crafting Sarbanes-Oxley understood financial reporting and the auditing process well enough to realize this distinction and structured Section 404 accordingly. Point in time also makes it easier for management to remediate a deficiency.

120. If evaluation and testing are done throughout the year but management's required evaluation and the internal control report are as of year-end, what type of evaluation is necessary as of year-end for management to render the internal control report as of that date?

Management's approach to testing and evaluating controls at year-end is impacted by the strength of the internal controls and the nature and extent of the evaluation and testing during the year. If the controls are strong, the evaluation and testing during the year have been ongoing and comprehensive, and there have been no significant changes in the company's processes, one approach is to have process owners confirm as of year-end that the key controls for which they are responsible are in place and operating effectively. The self-assessments used by the process owners address the key controls documented during the evaluation and tested during the year.

That being said, some refresh testing also may be required at or close to year-end, particularly for critical routine controls, and selected controls over nonroutine and estimation processes. Furthermore, controls executed *at* year-end may require testing *after* year-end.

Validation of Operating Effectiveness ("Testing of Controls")

121. What approaches are recommended for "testing" the effectiveness of internal control over financial reporting?

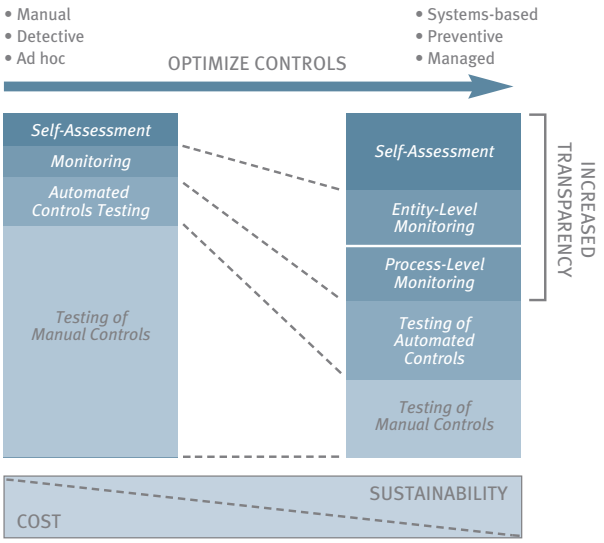
For management to assert that internal control over financial reporting is effective, evaluating design effectiveness and validating operating effectiveness are both required. Validating operating effectiveness is the process of determining that the controls are operating as designed. In its interpretive guidance, the SEC's underlying premise is that management varies the nature, timing and extent of the evaluation methods it implements in response to judgments about risk. Thus, the greater the misstatement risk of a financial reporting element and the higher the risk of control failure, the greater the amount of evidence required. Conversely, the lower the misstatement risk of a financial reporting element and the lower the risk of control failure, the lesser the amount of evidence required. As simple as these principles are, they represent the crux of a risk-based approach to developing a cost-effective test plan.

Examples of characteristics to consider when applying these principles are described below:

- ***Risk of misstatement*** – Characteristics of the financial reporting element that management considers include both the materiality of the financial reporting element and the susceptibility of the underlying account balances, transactions or other supporting information to material misstatement. When considering the latter, the SEC recommends considering such elements as:
  - The judgment involved in determining the recorded amounts
  - The susceptibility to fraud
  - The complexity in the underlying accounting requirements
  - The occurrence of change in the nature or volume of the underlying transactions
  - The extent of exposure to environmental factors (such as technological and/or economic developments)

  Financial reporting elements requiring significant judgment, vulnerable to fraud, requiring complicated calculations, affected by change in the underlying transactions and/or exposed to external environmental factors would generally be assessed as higher risk.
- ***Risk of control failure*** – When considering the likelihood that a control might fail to operate effectively, the Commission's guidance points out that management considers the following factors:
  - The type of control (manual or automated) and the frequency with which it operates
  - The complexity of the control
  - The risk of management override
  - The judgment required to operate the control
  - The competence of the personnel who perform the control or monitor its performance
  - Whether there have been changes in key personnel who either perform the control or monitor its performance
  - The nature and materiality of misstatements that the control is intended to prevent or detect
  - The degree to which the control relies on the effectiveness of other controls (for example, general IT controls); and the evidence of the operation of the control from prior year(s)

The above characteristics are addressed through a balanced test plan consisting of three elements – self-assessment, monitoring (both entity-level and process-level) and independent testing (both automated and manual controls).



As illustrated in the above schematic, there are several forms of validating the operating effectiveness of controls, one of which is independent direct testing of controls. Testing provides the evaluator the greatest confidence as it provides the most direct evidence of operating effectiveness. However, testing is also the most time-consuming of all forms of validation. As of the time this publication went to print, many companies continued to rely excessively on independent direct testing of manual controls. The key to a cost-effective test plan is to *balance* the plan as suggested in the above schematic.

The three approaches to validating operating effectiveness are:

- ***Self-assessment.*** Control owners, or process owners or managers with no direct control responsibility, self-assess the controls for which they are responsible and communicate the results to management. This form of validation enables the certifying officers to confirm operating effectiveness at any time, including year-end and quarter-end. Self-assessments are often completed for all of the company's primary controls, i.e., those controls that are especially critical to the mitigation of risk and the ultimate achievement of one or more financial reporting assertions. The self-assessment process is designed so that it may be conducted at any time, with technology-based solutions providing this flexibility.
- ***Monitoring.*** Monitoring takes place at two levels – the entity level and the process level. Management puts in place entity-level monitoring and analytics that provide direct evidence of control performance at the process level. Process owners put in place monitoring approaches through their direct supervisory activities and metrics on process performance. Monitoring is evaluated in terms of its effectiveness in (1) determining that the controls are operating effectively and (2) identifying material errors and/or omissions not detected by the underlying control processes. Note that the SEC's interpretive guidance refers to "monitoring activities," which are discussed in Question 94. A monitoring activity is a procedure that ensures that a key control is operating effectively.
- ***Independent direct tests of controls.*** Direct tests of controls should be performed at both the entity level and at the process level. Tests at the process level include tests of pervasive process controls and information process controls. Periodic testing of key controls also evaluates the quality of self-assessment and monitoring processes.

These validation approaches are interrelated. For example, process-based self-assessments can be an effective tool to assist management in supporting the conclusion on the effectiveness of controls; however, they do not obviate the need for monitoring and independent testing of controls. If self-assessment results are comprehensive and positive and there are strong entity-level monitoring controls and analytics, management may decide to

alter the nature, extent and timing of independent tests of controls. This assessment depends on many factors, including the criticality of the controls, the exposure to variability, and the volume, complexity and velocity of the transactions flowing through the process. As noted earlier, the SEC states that the extent of independent testing is impacted by the assessment of misstatement risk and control failure risk. The Commission also provides the following observations and assertions in its interpretive guidance:

- Management's judgment about the likelihood that a control fails to operate effectively may be influenced by a highly effective control environment and thereby impact the evidence evaluated for that control. However, a strong control environment would not eliminate the need for evaluation procedures that consider the effective operation of the control in some manner.
- When risk of misstatement and control failure is assessed as high, management's evaluation would ordinarily include evidence obtained from direct testing. Further, management's evaluation would ordinarily consider evidence from a reasonable period of time during the year, including the fiscal year-end. As the assessed risk increases, management can vary the nature of evidence from ongoing monitoring by adjusting the extent of validation through periodic direct testing of the underlying controls and/or adjusting the objectivity of those performing self-assessments. Management can also vary the nature of evidence obtained by adjusting the period of time covered by direct testing.
- For lower risk areas, the SEC's interpretive guidance provides management with significant flexibility in making judgments regarding what constitutes adequate evidence. For example, management may conclude that evidence from ongoing monitoring is sufficient and that no direct testing is required. Ongoing monitoring includes activities that provide information about the operation of controls and may be obtained, for example, through self-assessment procedures and the analysis of performance measures designed to track the operation of controls.
- Management's daily interaction with its controls may provide it with sufficient knowledge about its operation to evaluate the operation of internal control over financial reporting, particularly in smaller companies. For example, ongoing direct knowledge and direct supervision of control operation may contribute to this knowledge from daily interaction. Management should consider the particular facts and circumstances when determining whether or not its daily interaction with controls provides sufficient evidence for the evaluation.

122. Who is responsible for validating operating effectiveness?

Management, with the participation of the company's CEO and CFO, is ultimately responsible for validating the operating effectiveness of controls. Internal auditors, other company personnel or third parties retained by management and under its direction may assist during the validation process so long as management takes responsibility for the work. Management must be satisfied that the testing procedures provide sufficient evidence to support management's assessment that internal control over financial reporting is operating effectively. In addition, management must be satisfied that assisting personnel are sufficiently objective and competent to perform the required testing procedures. Factors management may consider when selecting an evaluator include the evaluator's knowledge of the process, internal controls and accounting (competence), the evaluator's knowledge of the business and industry, limitations of the evaluator's schedule, and the evaluator's ability to perform tests in the future.

123. What is "testing of controls"?

A test of controls is a form of validating controls operation. Evaluators use tests of controls to determine whether selected internal controls were operating effectively during a period of time or as of a point in time. Tests of controls include inquiries of process and control owners, observation of control procedures as they occur, inspection of relevant control documentation using a selected sample of documents, and analysis or reperformance of the operation of a control using a selected sample of transactions. Often a combination of these procedures is used to obtain sufficient evidence regarding the operating effectiveness of a control. There

is a presumption that management's evidence is more reliable if a combination of procedures is used to validate the operation of internal controls.

Internal control over financial reporting is designed to either (a) prevent errors from flowing through the accounting system, or (b) detect and correct on a timely basis those errors that do occur. Consequently, tests of controls address (a) the effectiveness of preventive controls in preventing errors and exceptions, and (b) the nature, volume and disposition of errors and exceptions disclosed by the "detect and correct" controls being tested. These tests are also concerned with how the control was applied, the consistency with which it was applied and by whom it was applied.

Tests of controls follow the evaluation of controls design. In supporting their assertion on internal control over financial reporting, management first evaluates design effectiveness. Management then evaluates operating effectiveness, which requires an evaluation as to whether the key controls, as documented, reduce identified risks to an appropriately low level and provide reasonable assurance that management's assertions inherent in the financial statements are met and that there isn't a reasonable possibility of a material misstatement in the financial statements. Validating operating effectiveness (which includes testing of controls) requires an evaluation as to whether the controls operate as they are designed to operate. Therefore, "controls testing" is the process of determining that a company's internal controls operate in the manner they are supposed to operate.

124. How does management test controls that do not leave a trail of documentary evidence?

The operation of many controls produces documentary evidence, e.g., batch control logs that have been compared with the results of processing, or evidence that items on exception reports have been annotated with the disposition of exceptions. This evidence can be examined at any time. Thus, they can be tested at any time.

Other controls, however, do not leave a trail of documentary evidence and, to a large extent, depend upon the competence and diligence of the person or persons performing the control, e.g., close inspection of goods received prior to acceptance, or aspects of the control environment (such as management's interaction with certain controls). Documentary evidence for certain aspects of the control environment, such as management's daily interaction with certain controls, might not exist – particularly in smaller companies that have neither multiple layers of management nor multiple operating units. For example, ongoing direct knowledge and direct supervision of control operation may contribute to this knowledge from management's daily interaction. In circumstances in which documentary evidence does not exist, and is not expected to exist, testing of controls must be accomplished through visual observation of entity activities and interviews with control owners and other appropriate personnel. Management should consider the particular facts and circumstances when determining whether or not its daily interaction with controls provides sufficient evidence for a Section 404 evaluation.

125. How can inquiries or interviewing be considered "tests" of controls?

Interviews are useful "tests" because a significant number of controls depend on the right people identifying and resolving exceptions. In these cases, as noted in the previous question, there often is little or no evidence that a control is performed. To assess whether the control is operating effectively, it is often necessary to form an opinion as to how well these individuals understand a particular control and the related control objectives and are able to implement the control effectively. Do the control owners know what to look for and how to handle exceptions when they occur? In making appropriate assessments based on interviews, it is often appropriate to cross-check results with several interviewees to determine the consistency of responses received. Inquiries also complement other testing procedures.

Inquiries include formal written inquiries, such as a survey (using technology, for example), and informal oral inquiries, such as an interview. Inquiries alone are generally insufficient to provide conclusive test results for

higher to moderate risk areas. Responses to inquiries must be corroborated through inspecting reports or other documentation germane to the information obtained through the inquiries. Responses to inquiries also must be evaluated as to whether they are consistent with information obtained through other procedures. Note that self-assessment, which we have asserted is a separate form of validation, is also an inquiry technique.

126. What is reperformance?

Reperformance of controls provides a more tangible form of testing than inquiry or observation. The external auditors will likely emphasize this form of testing during the attestation process. Reperformance is sometimes confused with a "walkthrough" to understand how transactions are processed. While a walkthrough is useful during the documentation process and the evaluation of design effectiveness, it ordinarily does not serve as a test of controls except in lower risk areas. Reperformance is the reprocessing of a control procedure applied to a sample of transactions to determine whether the result obtained through the original performance of the procedure is correct.

Inspection techniques, on the other hand, often involve ascertaining whether one or more specific attributes exist as of a particular point within the transaction flow, consistent with the controls design, e.g., appropriate management authorization, matching of vendor statement data against receiver quantities and purchase order price points, etc. Quality of evidence is often a factor in some *inspection tests*. To illustrate, a signature on a voucher is not, in and of itself, persuasive evidence of a careful review of the voucher package before signing. Therefore, *inspection* of the voucher might not be enough. *Reperformance* of the control through checking prices, extensions and additions – a procedure which was to have been completed by the reviewer who signed the voucher – may be necessary to provide more compelling evidence.

Reperformance of the transaction process is different from reperformance of a control over that process and is often a common source of confusion. Reperformance of the process only provides negative assurance that the controls are not malfunctioning, because accurate processing is not necessarily indicative that the controls were all operating effectively. Information can be processed correctly even when controls do not exist. Thus, it is important to design the reperformance test to validate the controls themselves (through testing for attributes, for example) rather than the results of processing.

In some instances, reperformance might not be the most effective test. For example, the best evidence that control owners are comparing batch control totals to batch validation reports may be the *inspection* of a log that documents the results of the comparison plus *observation* of the person preparing the log. If this is a key control, reperformance of the process could miss the control entirely. *Reperforming steps of processes and controls based on a selection of transactions recorded on the books is not a test of completeness.* To test completeness, it is necessary to move upstream to apply inspection, observation and inquiry techniques to test controls at the point of entry, during processing, at interface or handoff points (if any), and over correction and re-entry of errors.

127. When are tests of controls performed?

Tests of controls may be performed at any time. In the initial year of Section 404 compliance, they ideally should be completed prior to the end of the second or third quarter, if possible, so that the external auditor is able to begin his or her review. An update is then performed through the end of the year. See Question 145 for further discussion regarding the update of testing through year-end.

For subsequent years, testing of controls over routine processes may be performed uniformly throughout the year with an update performed through the end of the year. Controls over nonroutine and estimation processes may be performed during the last half or, ideally, the last quarter of the year.

128. What is a test plan?

A test plan is management's plan for testing internal controls. In the plan, management defines the testing approaches, scopes and sample sizes that are required to support the assertions in the internal control report. The plan sets forth the following:

- The responsibility of process owners for determining the operating effectiveness of internal controls for which they are responsible
- The monitoring that management has in place at the entity and process levels
- The nature of the internal controls that will be tested at the entity level (see Question 83) and at the activity or process level, and where and how those controls are documented
- The testing standards and sampling methodologies for each area, including population size, the significance of the population, desired confidence levels, the accuracy required of sample results and other key population characteristics
- The process for reporting exceptions and the criteria for evaluating them
- The actions to take when failure conditions occur; e.g., when a control fails to pass a test
- The person or persons responsible for performing tests of controls
- The frequency with which tests are to be done (which often will mirror the operating frequency of the control, e.g., daily, weekly, monthly or annually)
- The parties to whom test results are reported
- The parties responsible for evaluating test results and reaching a conclusion as to operating effectiveness
- The process for identifying gaps and undertaking remediation to close those gaps, including the individuals responsible
- The extent to which the plan addresses the components of COSO (assuming management uses the COSO framework)

Management or its designee must approve the test plan. For example, the certifying officers or the Section 404 Compliance Steering Committee should approve the plan. Once the plan is finalized and approved, it should be reviewed with the external auditor to obtain any input he or she may have and to maximize the extent of the auditor's reliance on the tests performed under the plan.

A cost-effective test plan focuses on the controls addressing the highest risk of material error in the financial statements and emphasizes testing of the key controls (i.e., the controls on which management has decided to rely) with the greatest risk of performance failure. The characteristics for management to consider when evaluating these two components of "ICFR risk," as defined by the SEC in its interpretive guidance, are summarized in Question 121. The message is that a test plan is not cost-effective if it is designed to test every control, emphasize coverage and ignore control failure risk. Under the SEC's suggested approach, ICFR risk is considered when determining the nature, extent and timing of tests of controls. Through the test plan, management articulates ***what*** to test, ***who*** does the testing, ***when*** to perform testing and ***how*** testing should be done. These decisions are driven by the assessed level of ICFR risk. The higher the risk, the more persuasive the testing evidence needs to be. The lower the risk, the less persuasive the testing evidence needs to be. This risk assessment drives the selection of testing methods available to management for purposes of testing the operating effectiveness of key controls. Both the reduced number of controls and the nature of evidence gathering to support a conclusion on operational effectiveness have the potential to reduce the cost of testing, and are elements to consider when formulating a cost-effective test plan.

Following management's approval, the project team, internal audit or other management personnel (whose responsibilities lie outside of the area tested) execute the tests according to management's plan. The test plan should address the various forms of operating effectiveness validation. Following is an illustrative, high-level example, which is to be considered only as an example and not as a recommendation or standard:

	Nature	Frequency	Extent
Self-assessment	Process/control owners self-assess the controls for which they are responsible using tailored questionnaires	Quarterly	Key controls selected by management; self-assessment can be highly efficient and serve a dual purpose if management requires process owners to submit evidence that controls are operating by attaching documents
Monitoring	Review monitoring information and reports at the entity and process levels, and evaluate actions taken on exceptions, including resolution of exceptions, results of root cause analyses and implementation process improvements	Quarterly or monthly	Representative sample of sufficient size to be satisfied that monitoring is effective and appropriate action taken on exceptions
Testing – Pervasive process controls	Access controls – Develop a customized test plan involving appropriate information technology expertise	Quarterly	Based on evidence available and management's judgment and considering potential opportunities for testing across multiple processes or risks with similar controls
	Other types of pervasive controls (except access controls): inquiry, observation and inspection involving appropriate IT expertise for tests of systems development standards and system change controls	Semiannually or as changes occur	
Testing – Information process controls	Test controls results using inquiry, observation, inspection and reperformance techniques	Periodically as determined by management, e.g., incorporated into internal audit plan	Moderate, representative samples covering an appropriate period

While not intended to be an all-inclusive, comprehensive example, the illustration shows that the test plan needs to consider the three forms of validating controls effectiveness introduced in Question 121 (i.e., self-assessment, monitoring and independent direct testing).

The steps in developing a test plan are as follows:

- ***Determine testing objectives*** – Tests of controls provide evidence about whether controls over financial reporting are operating effectively. For example, to determine that disbursements have been properly authorized, tests of controls may be designed to enable the evaluator to examine a sample of payment vouchers to assess whether authorized company personnel signed the payment voucher before processing. Thus, the objective of testing is to answer two questions:

  - Did the controls perform as designed?

  - Did authorized and competent people execute the controls?

  The test plan should take these objectives into account.

- ***Consider the anti-fraud program and controls*** – The test plan should address testing of the company's anti-fraud program and controls, as defined and documented. The plan should focus on fraud when validating important entity-level controls, when testing key controls over the financial reporting process and when testing controls mitigating the critical assertion risks at the process level.

- ***Define the failure conditions*** – Defining what constitutes a "control failure" up front for each control tested before beginning testing is an effective way for management to direct the testing effort. A "failure condition" in testing is a departure from "acceptable" or "effective" performance of the prescribed control activity. For example, a failure condition may be defined as an error rate in the sample that management is unwilling to accept because it exceeds management's maximum tolerable error rate (the upper error limit, or UEL). Stated another way, a failure condition is an error rate that exceeds an acceptable level. See Question 129 for further discussion.
- ***Define the population*** – In financial reporting, the "population" consists of all of the items constituting an account balance or a class of transactions subject to testing. It is important to articulate the characteristics of the population from which a sample is to be selected in a manner that can be related to specific control objectives. To accomplish this task, the test plan developer should specify the target population as clearly and completely as possible. For example, if the evaluator tests a control designed to ensure all shipments are billed, the appropriate population is the shipped items, not the billed items. In controls testing, the population is also affected by the number of times a particular control is performed. For example, the population is defined by the frequency with which the control is executed – recurring, daily, weekly, monthly, quarterly and annually. The population is also defined by the number of individuals executing a control operation. Therefore, if the same control operation is executed by 10 people on a weekly basis, the test plan developer must consider a population size of 520 operations when determining the required sample size.
- ***Ascertain the test period*** – In ascertaining the test period, the Section 404 compliance team must address the question of whether to apply tests of controls to (1) transactions executed throughout the period (e.g., the entire year), ***or*** (2) during the period from the beginning of the year to an interim date, ***or*** (3) primarily close to or at the end of the year. The answer to this question depends on management's risk assessment, as risks relating to period-end transactions and journal entries are quite different from risks associated with routine transactions processed every day. The answer is also affected by the frequency of the control, i.e., whether the control is performed continuously (recurring), daily, weekly, monthly, quarterly or annually. See Question 130 for further discussion.
- ***Define the sampling unit*** – The *sampling unit* is the item to be tested. It constitutes one item in the population, such as a document, an entry or a line item. For example, if the testing objective is to determine whether disbursements have been authorized and the prescribed control activity requires a duly authorized voucher before processing, the sampling unit might be defined as the voucher. While the point about the sampling unit is somewhat elementary, it must be remembered when developing a test plan that many types of controls do not involve selecting a sample from a population. For example, in some instances, the sampling plan must stipulate the domain where the controls can be observed, e.g., safeguard controls, segregation of duties, etc. The plan may set forth the frequency (daily, weekly, monthly, etc.) with which a particular control is executed, e.g., comparisons, reconciliations, etc. In such instances, the sampling unit may be a completed reconciliation meeting certain predefined criteria.
- ***Select testing method(s)*** – There are four basic testing methods – inquiry, observation, inspection and reperformance. Evidence is more reliable when *consistent evidence* is obtained from a *combination of procedures*. See Question 131 for further discussion.
- ***Determine sampling method*** – Sampling is divided into two categories – *judgmental* and *statistical*. When choosing the sampling methodology and determining sample size, the process owners and Section 404 compliance team leads should consider the following:
  - The level of understanding that management and process owners have of the underlying process and the extent of errors in executing the specific control during the process
  - The criticality of the upstream business process(es) that feed(s) the priority financial reporting elements
  - The extent of reliance on self-assessment and entity-level monitoring
  - The nature of the control process and the underlying transaction data addressed within the control process

  See Questions 132, 133 and 134 for further discussion.

- ***Determine sample size*** – Ultimately, the task falls to management to optimize selected sample sizes against the risk of missing a material weakness that the external auditor might later detect. Management retains the ultimate responsibility to decide the sufficiency of testing for its purposes in supporting the assertions in the internal control report. When deciding sample sizes, there are certain factors management should consider. These are discussed in Question 135.
- ***Finalize formal test plan*** – The test plan articulates the rules of engagement before testing begins. Through the test plan, management defines the nature of the internal controls that will be tested at the entity level and at the activity/process level, and where and how those controls are documented. The plan references the separate documentation of financial reporting elements, assertions and risks to provide the proper context. The test plan also addresses the testing approaches, scopes and sample sizes that are required to support the assertions in the internal control report, and sets forth the actions to take should a test indicate a control is not operating effectively.
- ***Approve test plan*** – Management approves the test plan.

Once the test plan is completed, management should review it with the external auditor.

129. Why is it important to define the failure conditions before beginning testing?

As noted in Question 128, a "failure condition" in testing is a departure from "acceptable" or "effective" performance of the prescribed control activity. For example, a failure condition may be defined as an error rate in the sample that management is unwilling to accept because it exceeds management's maximum tolerable error rate, or upper error limit (UEL). In other words, a failure condition is an error rate that exceeds an acceptable level.

Defining what constitutes a "control failure" up front for each control tested before beginning testing is an effective way for management to direct the testing effort. A "failure condition" in testing is a departure from "acceptable" or "effective" performance of the prescribed control activity. For example, a failure condition may be defined as an error rate in the sample that management is unwilling to accept because it exceeds management's maximum tolerable error rate (or UEL).

"Failure conditions" are ***not*** limited to the rate of error within a population. There are many other controls that must be tested that do not involve selecting a sample from a population, including segregation of duties, control environment attributes, physical safeguards, reconciliations, comparisons, and accounting for numerical sequence and completeness. These controls are often tested through inquiry and observation, and reconciliations can be reperformed. The failure condition relates to whether the controls actually exist as intended (e.g., physical safeguards) or are actually performed as intended (e.g., reconciliations and comparisons). Therefore, in addition to defining a failure condition using error rates, a failure condition may be defined qualitatively in terms of specific conditions. For example, management may designate certain conditions noted during testing that lead the evaluator to conclude that the "reasonable assurance" standard is not achieved. Examples of such "conditions" include:

- Failure to follow up on an exception noted during the company's process
- The absence of critical matters (such as a known fraud) covered in audit committee meeting minutes
- The lack of evidence of effective communication and reinforcement of the company's code of ethics
- The lack of expected physical safeguards
- Gratuitous comments from employees regarding pressure from a senior executive to change reported results or other evidence of management override

In summary, the test plan developer must make a precise statement of what constitutes a "failure condition" so the individuals performing the testing procedures have specific guidelines for identifying deviations from adequate or expected performance. If failure conditions are not predefined, the individuals performing the testing procedures will make up the rules as they go, leading to errors in judgment, decisions to retest when remediation is more appropriate and constant second-guessing by the external auditors, all of which will lead to nonvalue-added activity.

Defining the rules of engagement up front means, going forward, management, evaluators and auditors are all in agreement as to what will be done in specific situations. This is what an effective test plan is about.

Another issue arising if the ground rules are not articulated up front is the risk evaluators will rationalize exceptions and conclude they do not represent deficiencies even though they really are deficiencies. A conclusion that an identified unacceptable exception rate does not represent a control deficiency is appropriate only if evidence beyond what the evaluator initially planned supports that conclusion. Mere rationalization will not make exceptions go away.

To define failure conditions, take the following steps:

(1) Start with the population characteristics or attributes that are to be tested.

(2) Understand specifically "what can go wrong" with respect to the operation of the control. (Note: The risk assessment should source these risks.)

(3) Describe each specific example of "what can go wrong" in operation as an example of a "failure condition."

(4) Recognize in the test design that different failure conditions may require different tests, although use of the same sample may be appropriate.

(5) Understand management's acceptable error rate (the "planned" tolerable error) before beginning testing.

(6) Include the planned tolerable error in management's test plan.

(7) Include multiple conditions for "tests of one" when testing application controls.

For example, suppose a prescribed control requires every package supporting a disbursement to include the following: an invoice, a voucher, a receiving report and a purchase order, all stamped "paid." If the existence of the invoice and receiving report stamped "paid" are necessary to indicate adequate performance of the control, then an exception may be defined as "a disbursement not supported by an invoice and a receiving report stamped 'paid.'" Management must then define the tolerable error rate, which may be one error for every 200 disbursements. The test should be designed to compare the error rate noted in the sample to the tolerable error rate (0.5 percent). If the tolerable error is exceeded, a "failure condition" results. If a small sample is selected, this could mean that one exception would cause the test to fail.

The absence of "failure conditions" noted during testing (i.e., in effect, an error rate below the tolerable error) supports a conclusion of "adequate performance."

130. How does the evaluation team ascertain the test period?

As noted in Question 128, the Section 404 compliance team must address the question of whether to apply tests of controls to (1) transactions executed throughout the period (e.g., the entire year), ***or*** (2) during the period from the beginning of the year to an interim date, ***or*** (3) primarily close to or at the end of the year. In theory, because Section 404 requires a point-in-time assessment as of year-end, some may ask whether management can wait until the end of the year to test. From a practical standpoint, it is recommended to differentiate controls over routine processes from controls over nonroutine and estimation processes by testing the former over the course of the year and testing the latter closer to the end of the year. This strategy provides management the flexibility to remediate control deficiencies prior to year-end in sufficient time to retest the remediated controls to ensure they are operating effectively. It also reduces the risk of surprises. Further, the auditor needs sufficient time to perform the attest work.

There are other reasons to spread out the testing work. The Section 302 certification process is a quarterly reporting process. Internal control over financial reporting is a subset of the disclosure controls and procedures certified by the CEO and CFO every quarter. Testing on an interim basis may identify areas to remediate more timely than waiting until the last quarter to do the work. Spreading the testing out over time also is more efficient and avoids a year-end resource "spike."

A choice to deploy interim testing requires consideration as to the nature, timing and extent of refresh testing necessary to update preliminary evaluations and determine operating effectiveness "as of" the end of the fiscal year. Testing performed earlier in the fiscal year will require more extensive updating closer to the end of the fiscal year. If testing covers an interim period, the evaluator must determine what additional evidence needs to be obtained for the remaining period. Factors to consider when determining the nature, timing and extent of refresh testing include:

- The significance of the risk to the financial reporting assertion(s) it affects
- The significance of the risk(s) mitigated by the specific controls tested prior to the "as -of" date
- The results of the tests performed during the interim period
- The results of similar tests performed in prior years
- The length of the remaining period between the interim period-end and the end of the year (generally should be no more than six months)
- Any changes in controls since the interim testing period
- The existence of a self-assessment program that is linked specifically to the control in question

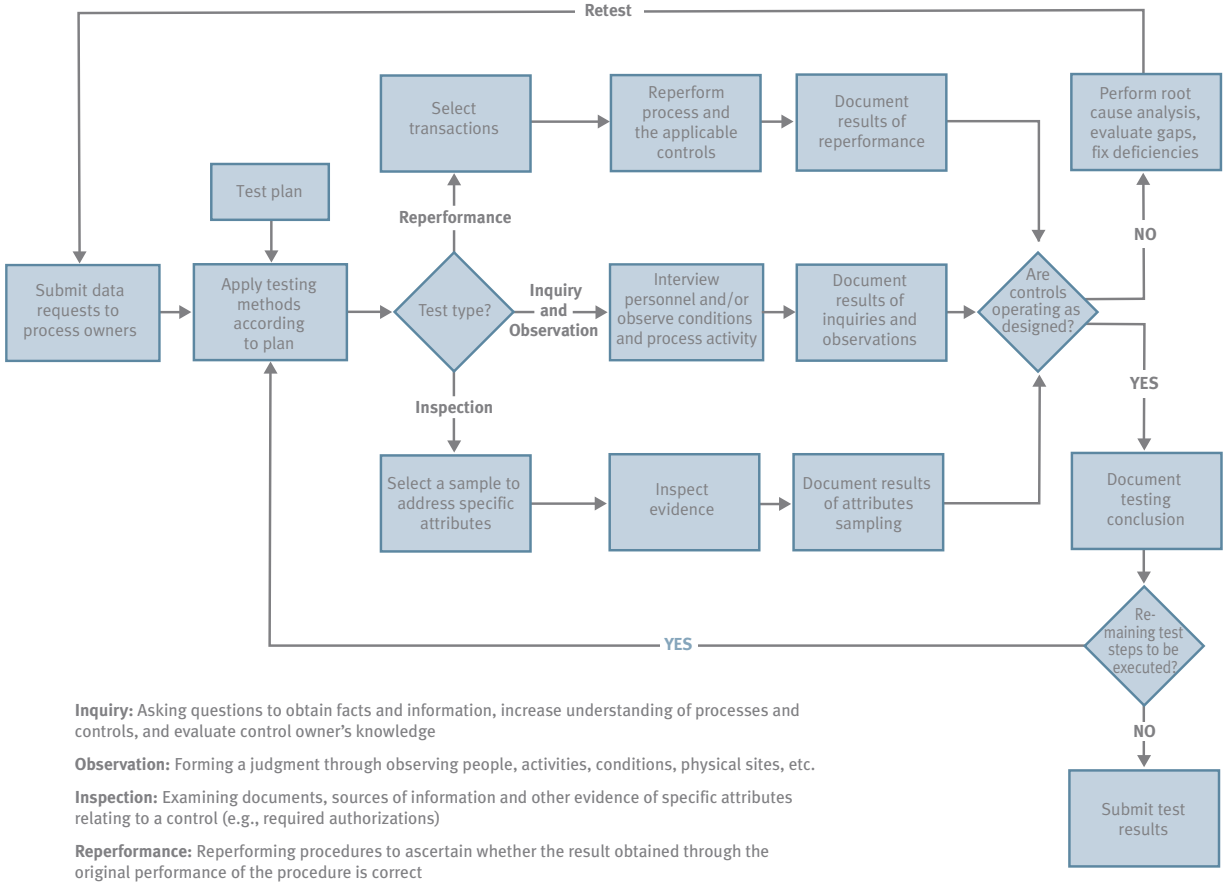
In applying the above guidance in practice, experience indicates that the *controls over routine transactions* are the ones that lend themselves most to interim testing strategies. Since these controls generally require more time to test, it is often more efficient to test them on a preliminary basis. *With respect to controls over pervasive, nonroutine and estimation areas*, because of the nature of these areas and the underlying risks, management should consider the need to perform tests of controls closer to the "as of" date. Examples of these controls include:

- Controls over significant nonroutine transactions
- Controls over accounts or classes of transactions with a high degree of subjectivity or judgment in measurement
- Pervasive controls such as certain IT general controls or controls over the recording of period-end adjustments
- Controls over financial reporting elements exposed to changes in technological, economic or other external environmental developments
- Controls over the risk of management override

From a practical standpoint, testing these controls "closer to the 'as of' date" may mean testing them during the fourth quarter or in conjunction with a hard close as of a preliminary date with appropriate refresh testing at year-end.

131. How does management select testing method(s) to apply in specific circumstances?

There are four basic testing methods: inquiry, observation, inspection and reperformance. Following is an example of how the four methods are applied.



Inquiry: Asking questions to obtain facts and information, increase understanding of processes and controls, and evaluate control owner's knowledge

Observation: Forming a judgment through observing people, activities, conditions, physical sites, etc.

Inspection: Examining documents, sources of information and other evidence of specific attributes relating to a control (e.g., required authorizations)

Reperformance: Reperforming procedures to ascertain whether the result obtained through the original performance of the procedure is correct

Inquiry can be an effective way to corroborate or follow up on evidence gained through the other testing methods. When using inquiry, evaluators should ask open-ended questions, such as "can you tell me what you do?", "how is this done?" and "can you walk me through it?" When using inquiry, evaluators should avoid leading questions that tip the answer, listen carefully, watch for nonverbal cues and apply professional skepticism. Information that responses to inquiries might provide includes:

- The skill and competency of those individuals performing the control
- The precision of the control in preventing or detecting errors or fraud
- The frequency with which the control operates to prevent or detect errors or fraud
- Whether there have been instances of management override with respect to established controls

Effective inquiries lead to further inquiries and to subsequent inspection and observation techniques. Such combination of techniques facilitates testing of control over identifying and correcting errors and re-entering corrected data. Inquiries are also invaluable during a "talkthrough" with process owners, particularly when combined with effective listening and a focus on nonverbal cues. That all said, inquiry, by itself, is inadequate to support management's assessment. Used effectively, inquiry adds considerable insight as a testing technique.

Observation is an effective technique for testing such controls as physical safeguards and segregation of duties as well as noting specific individuals in action as they execute documented control activities.

Inspection is another high level of evidence. For example, sampling for attributes can provide compelling evidence that controls over *routine* transactions are performing as intended. However, inspection must be used with care. A signature on a voucher is not, in and of itself, persuasive evidence of a careful review of a voucher package before signing. Therefore, *inspection* of the voucher might not be enough and *reperformance* of the control procedure (checking prices, extensions and additions) may be necessary.

Reperformance is a higher level of evidence than inquiry. It involves selecting transactions and reperforming the transaction, including reapplication of management's authorization, recording, processing and reporting criteria. The reperformed or recalculated transaction is compared to the reported result. If they agree, there is a presumption that the controls along the process operated effectively.

In summary, evidence is more reliable when it is obtained consistently from a *combination of procedures*. When developing a test plan, the evaluation team needs to consider these points.

132. How does management determine the appropriate sampling method?

As defined by the AICPA Sampling Guide, sampling is "the application of a testing procedure to less than 100 percent of the items within a … class of transactions for the purpose of evaluating some characteristic of … the class." Under Section 404, the context of this definition is reaching a conclusion with respect to the operating effectiveness of internal control over financial reporting. As further explained in Question 143, the key attributes of a control (e.g., manual versus system; frequency of operation; preventive versus detective; routine versus nonroutine) have implications from a risk standpoint and assist the Section 404 compliance team in determining the nature, extent and timing of testing required to evaluate that control. For example, entity-level controls generally require more emphasis on inquiry and observation. Controls that are manual in nature generally may require more extensive testing, i.e., higher sample sizes, than systems-based controls, because they are more susceptible to human failures in operation. The type of underlying transaction subject to a control (either a routine transaction or nonroutine transaction) can also affect the nature, extent and timing of testing.

Sampling is an important aspect to tests of controls because it affects the number of items selected for testing as well as the selection process. It is not necessary to test every single instance in which a control is applied. It is only necessary to test the controls to such an extent that management is satisfied the results of the test provide conclusive evidence to support the assertion that the control is operating effectively. This conclusion need not be reached in isolation. The results of testing may be considered in light of other sources of evidence regarding operating effectiveness, including positive self-assessments received from process owners, the results of entity-level monitoring and the effectiveness of compensating controls as well as historical testing results.

Management must decide the sampling methodologies needed to ensure an efficient approach for demonstrating compliance with Sarbanes-Oxley. When choosing the sampling methodology and determining sample size, management should consider the criticality of the business process(es) which feed the significant financial reporting elements, and the extent of reliance on self-assessment and entity-level monitoring. Other factors to consider when choosing sample size:

- Stability and overall strength of the control environment
- Knowledge of location of errors that have occurred in the past (i.e., known historical exceptions)
- Population size
- Significance of the control to the stated assertion
- Required accuracy of sample results
- Expected error rate

Sampling is divided into two categories – judgmental and statistical. When choosing the sampling methodology and determining sample size, the process owners and Section 404 compliance team leads should consider the following:

- The level of understanding that management and process owners have of the underlying process and the extent of exceptions in the population when the specific control is executed (the greater this understanding, the smaller the sample)
- The criticality of the upstream business process(es) that feed the priority financial reporting elements (the more critical the process, the more important the controls; the more important the controls, the more evidence is needed through testing to provide reasonable assurance they are operating effectively)
- The extent of reliance on self-assessment and entity-level monitoring (the greater the reliance on these sources of evidence, the less evidence is needed through direct testing to provide reasonable assurance the controls are operating effectively)
- The nature of the control process and the underlying transaction data addressed within the control process (e.g., if the control is addressing a process involving unique prenumbered documents or transaction identifiers, such as invoices or receiving reports, then statistically valid samples and conclusions can be effectively applied)

See Questions 133 and 134 for discussion of judgmental and statistical sampling.

133. How is judgmental sampling applied?

As discussed in Question 132, *judgmental* sampling is one of the methods of sampling. This sampling approach involves the use of judgment by management in determining sample sizes based upon the nature and significance of the control. When determining sample sizes and the extent of controls testing on a judgmental basis, management must exercise care. *Judgmental sampling introduces bias, which leads to sampling risk.* In deciding how many items to test, management must consider the risk that the conclusion that a control is operating effectively based on limited testing *may differ* from the conclusion it would have reached if it had tested all operations of the control. Therefore, it is especially risky to select small judgmental samples when there is an inadequate understanding of the process and the expected error rate, i.e., management and process owners don't know what to expect. In fact, the PCAOB staff has stated that nonstatistical samples should be used based on the expectation of "no, or very few, control testing exceptions."

One of the limitations of judgmental sampling is that it is inappropriate to infer testing results using judgmental samples to the population. If the controls are critical to the achievement of the company's stated financial reporting assertions (and to the mitigation of risks to achieving those assertions) and oversight is limited to manual supervision, management should consider more extensive sample sizes and even statistically valid samples for testing purposes in order to formulate more compelling evidence. If there is a critical control relied on versus several compensating controls, then management should expect to test more items for that particular control. As a general rule, the more complex a manual control, the greater the number of items to test. If the frequency of application of manual controls is high (e.g., daily rather than monthly or annually), then as a general rule the test plan should provide for testing more items. However, this is not suggesting a proportionate increase in scope. Generally, when sampling is appropriate and the population of controls to be tested is large, increasing the population size does not proportionately increase the required sample size.

However many items are selected for testing, the Section 404 compliance team should make sure the underlying "thought process" supporting its conclusions is documented and approved by management.

134. How is statistical sampling applied?

As discussed in Question 132, *statistical* sampling is another method of sampling. This sampling technique uses statistics to (1) reduce sampling risk, which is the risk that the sample results are inconsistent with the actual characteristics of the population, and (2) infer results of the sample to the population. If statistical sampling is used, there are several factors to consider:

- The **expected error** is the level of variability (or control exceptions) management anticipates finding in the population.
- The **margin of error** is a measure of sampling error, i.e., it is a measure of the difference between the estimate from the sample and the true population value.
- The **confidence level** is the likelihood that the results obtained from the sample lie within the margin of error rate.
- The **Upper Error Limit (UEL)** is the maximum error rate management is willing to accept (i.e., the tolerable error rate).

Ideally, the margin of error at the stated level of confidence *plus* the expected error should be less than or no greater than the tolerable error rate (UEL). However, this is not always the case as management seeks to balance the cost of testing with the evidence gained from sampling.

Without getting into a technical discussion, statistical sampling involves moving parts. Management should consider holding confidence level constant at a high level, such as 95 percent, to enable more forceful conclusions. High confidence levels are also more appropriate for a critical application or control, particularly when there is an absence of a strong control environment, effective monitoring and other compensating controls. A lower confidence level (such as 90 percent) is often useful only when seeking an indication of the likely population characteristics. Lower confidence levels may be appropriate when a particular control activity functions within a strong control environment, i.e., there is evidence of strong company-level or monitoring controls, strong pervasive controls (including general IT controls) along with a comprehensive self-assessment approach.

Following is an illustrative process for determining sample size, when using statistical sampling:

- For each type of control, management and the process owner define the presumed expected error rate. This rate is the level of variability (or rate of control exceptions) management and the process owners anticipate finding in the population. The expected error rate should be based on factual assessments by management and the process owners who are knowledgeable of the process and the related control objectives, design and performance. This means that management and the process owners need to apply their knowledge of the process.
- Management defines the tolerable error for all control frequencies. The tolerable error is not the same as the true error rate. The goal is to determine, given a 95 percent confidence interval, whether there is a 95 percent chance that the "true" population error rate will not exceed the tolerable error rate management selects. Management's tolerable error is sometimes described as the UEL.
- When applying sampling tables, *sample sizes may vary for controls depending on the extent of management reliance*. For example, a lower maximum tolerable error might be expected for controls on which management is placing a high degree of reliance for purposes of achieving a given financial reporting assertion. To illustrate, a 3 percent maximum tolerable error rate may be selected for lower reliance controls and a 2 percent or 1.5 percent rate for higher reliance critical controls. These choices influence sample size.

When determining sample size using statistical sampling, the Section 404 project team should involve appropriate quantitative expertise. One of the primary issues management faces in sampling is the risk that the project team will conclude through testing that controls are operating effectively and the external auditors will then perform their review (using a different sample and/or sample size) and detect a problem not found by the project team. Involving appropriate skills in applying and interpreting the statistics as well as in executing the tests of the sample will reduce sampling risk.

135. How does management determine sample size?

There is no "one size fits all" when deciding the most appropriate test plan to apply. Considerable judgment must be brought to bear by the project team and management when considering a company's facts and circumstances. For example, our response to Question 104 introduces the Internal Controls Capability Maturity Continuum. When a company's internal controls are at the "initial" (ad hoc) stage for a critical process, the company will often take steps to improve these controls so they are more repeating and better defined. In these circumstances, it is difficult to know for sure that the processes are "in control" without the use of statistical techniques to infer test results to the population with a reasonable level of confidence. Because these environments lack process definition and are often in a state of change, self-assessment techniques are not as effective and entity-level monitoring often doesn't exist. These environments are often characterized by manual and detective controls.

The following guidance should be considered when validating the operating effectiveness of manual "detect and correct" controls:

- If these controls are critical to the achievement of stated financial reporting assertions and oversight is limited to manual supervision, management should consider more extensive sample sizes for testing purposes.
- With respect to testing controls requiring manual oversight or involvement: The more frequently a manual control operates and/or the more important the control, the more extensive the testing.
- If the frequency of application of the manual controls is high (e.g., hourly rather than monthly or annually), then as a general rule the test plan should provide that more items be tested.
- If there is a single control relied on versus a number of compensating controls, then management should expect to test more items for that particular control.
- As a general rule, the more complex a manual control, the greater the number of items to test.

If there is a more stable control environment where the internal controls are functioning at the "defined" and "managed" stages (as defined in Question 104), we often see the emergence of more preventive and systems-based controls. At this level of capability, self-assessment techniques are more effective and monitoring procedures are more likely to be in place, particularly at the "managed" stage. At these higher levels of capability, management may conclude that less comprehensive judgmental sampling techniques, such as representative sampling, might be appropriate. Further, given the additional sources of evidence as to operational effectiveness that are often available at these higher levels of capability, management may choose to test fewer items. The following guidance should be considered:

- The compliance team should test more extensively the controls that support the effectiveness of other controls in these environments (i.e., controls on which other controls depend). This includes selected attributes of the control environment and specific IT general controls processes, such as security administration and change management. Tests of IT general controls ensure the continuous effective operation of automated controls and controls dependent on IT functionality.
- For an automated control, the number of items that should be tested is generally minimal (one to a few items) assuming IT general controls have been tested and found to be effective.

Thus, management's test plan is often influenced by the maturity of the company's controls, as illustrated using the Capability Maturity Continuum introduced in Question 104. Ultimately, management must balance the cost of higher sample sizes against the risk of missing a material weakness that the external auditor later detects.

As noted previously, management retains the ultimate responsibility to decide the sufficiency of testing. Because of the lack of clear criteria as to the number of items to test, input and feedback from the independent accountant should be obtained before commencing execution of the test plan to maximize the extent of the auditor's use of the work of others.

136. How is the sample selected from the population?

There are a variety of methods for selecting a sample. Regardless of the method used, it is important to select locations or business units in such a way that the sample is expected to be representative of the entire population. It is also important to select samples according to the test plan. Sample biases can occur in many ways. For example, sample bias occurs when the number of items selected for the sample is too low, the time period for testing is insufficient in duration, the population targeted is biased in some way, or the items selected are chosen based on deliberate choice rather than through using a random process. Random selection guards against bias, so it should be used whenever possible. It is also important to check the quality of the information in the population from which the sample is drawn. If the quality is poor, sampling may not be justified.

Following are alternative selection methods:

Unrestricted random numbers. This method, in which each item in the population has an equal chance of being selected, is very common. When it is used, the items in the population must be numbered or listed in a complete and accurate record.

Intervals. In this method, there is a uniform interval between each item selected after a random start. It is applied when selecting items randomly is burdensome. It works fine when there is not a pattern in the population that will bias the sample. If there are items missing in the population, they must be identified.

Stratifications. The population is segregated into two or more classes, with each class sampled separately. This method is appropriate when there is considerable variation in the population and increased reliability in sampling results arises from breaking the population down into homogeneous groups of comparable items.

Cluster and Multistage. When using the cluster method, the population is formed into groups and all items within selected groups are examined in their entirety. When using the multistage approach, sampling is applied to several levels, e.g., a sample is taken from several locations and another sample is taken from the sampled items. This approach is applied when random sampling is burdensome or not possible, because the population is dispersed geographically. Cluster sampling increases exposure to sampling error. Multistage sampling requires complex calculations.

137. How does management finalize the formal test plan?

As we stated in previous questions, the test plan articulates the rules of engagement before testing begins. There are several reasons why this is important:

- Management does not want evaluators "making it up as they go."
- Loosely defined test plans open management up for "second-guessing" by the external auditors when dealing with exceptions.
- Evaluators need to know when to (a) root cause exceptions, remediate processes and retest, versus (b) select an expanded sample size and retest.
- The issue of interim testing and year-end updates requires clarification.
- Process owners need guidance on supporting their self-assessments.

Through the test plan, management defines the nature of the internal controls that will be tested at the entity level and at the activity/process level, and where and how those controls are documented. The plan should reference the separate documentation of significant financial reporting elements, assertions and risks to provide the proper context. The test plan addresses the testing approaches, scopes and sample sizes that are required to support the assertions in the internal control report. The plan also sets forth the actions to take should a test indicate a control is not operating effectively. Following is a summary of the essential elements of a test plan:

Validation approach – Self-assessment, monitoring and/or independent testing

Nature/description of the test – Describe nature of the control or transaction subject to validation and testing

Applicable control significance – Primary versus secondary control

Applicable control significance/type – Manual control or system control; preventive control or detective control

Frequency/timing of the control/test – Year-end, quarter-end, month-end, daily or continuous

Other elements of the test plan include:

- The person or persons responsible to perform tests of controls
- The frequency with which tests are to be performed (which often will mirror the operating frequency of the control, i.e., daily, weekly, monthly or annually)
- The parties to whom test results are reported
- The parties responsible for evaluating test results and reaching a conclusion as to operating effectiveness
- A description of the specific actions to take if a control fails
- The process for identifying gaps and undertaking remediation to close those gaps, including the individuals responsible
- The extent to which the plan addresses the components of COSO (assuming management uses the COSO framework)

138. How are testing results documented?

While there are no prescribed documentation requirements, the evaluator needs to know the nature of exceptions, their frequency and the way in which the process or control owner reconciles and documents their disposition. It is also critical to establish the testing documentation protocols and obtain agreement with management and the external auditors, assuming management intends the auditor to use the testing results in planning his or her audit. Simply covering format and columnar headings is not enough. Agreement is also necessary as to the level of detail when documenting the results of testing. One possible suggestion is to complete several tests as a "pilot" and invite the external auditor to critique the completed documentation as to sufficiency for his or her purposes during the attestation process. While there are no prescribed documentation requirements, the evaluator needs to document: the nature of testing procedures; the nature of exceptions, their frequency and the way in which the process or control owner reconciles and documents their disposition; and errors and deviations noted. Documentation must be sufficiently granular to facilitate "over-testing" by the external auditor if the auditor needs to do so to rely on the test results.

Following are illustrative examples of documentation points to use when designing a form that facilitates the documentation process:

Method of selecting the sample. Document the selection procedure used and how it was applied.

Name and title of control owners interviewed. Document the results of inquiries of the "owner" of the control (the person who is accountable for its operation), including the questions asked (may be in the form of a template with questions and responses, *including items inspected and observed as a result of the inquiry).*

Description of visual observations. Describe what was observed, e.g., "observed materials being counted in the receiving department, which was physically segregated from the remainder of the plant."

Identification of the control documents examined. Record sufficient information so the external accountant can retrieve the documents, if necessary, to reperform selected tests.

Description of nature and frequency of exceptions and how they are resolved. A demonstrated knowledge of exceptions by the control owner and the manner by which they are corrected provides evidence that the control owner understands the control and how it operates. If the control procedure never detects an error or exception, questions arise as to whether (a) the control owner understands the control and is performing it, or (b) the technique is merely a processing procedure and not really a control.

Description of procedures for resolving exceptions. The evaluator should determine from the control owner how he or she corrects the errors and submits the corrected data back to processing.

Document reperformance work. Describe the work performed in sufficient detail so that the external auditor can review and reperform the test.

Summarize results of tests of judgmental samples. For judgmental samples, it is inappropriate to make an inference to the population as a whole. The evaluator may state: "We tested N items and noted Y exceptions." Alternatively, the evaluator may state: "We tested N items and noted Y exceptions and that the error rate in the items selected is less than management's stated tolerable error rate."

Summarize results of tests of statistical samples. For statistical samples, the evaluator should exercise care to prepare the summary of testing results consistent with the design of the sample and interpret the sample results consistent with the underlying statistics. It is often key to involve appropriate quantitative expertise to properly frame the summary of results in a statistically valid manner.

An assessment of operating effectiveness. The evaluator must conclude whether the control is operating effectively.

139. How are testing results evaluated?

The results of each test must be evaluated separately. If there are "failure conditions," it is important to understand why these conditions exist. These conditions could require remediation and retesting. Alternatively, they could require expansion of sample size. However, sample size should be expanded only when the test plan requires it and satisfactory results are expected; otherwise, the retesting is a waste of time. When evaluating sample results, remember that exceptions taint the use of small judgmental samples.

When exceptions to or deviations from the control design occur, the evaluator should understand the reasons for the exception or deviation. The evaluator should collaborate with the process owner to consider whether:

- The error rate noted in the sample exceeds the predefined acceptable error rate planned for the test (i.e., management's tolerable error rate).
- An exception noted for a small judgmental sample is potentially a problem.
- The identified error(s) is (are) inadvertent or intentional.
- The control is automated (in the presence of effective general IT controls, there is a presumption that an automated application control will always perform as designed).
- A failure of an automated control requires input from a technology expert to understand the implications.
- The degree of intervention by process personnel contributes to the exception or deviation.
- Management became aware of the exception or deviation on a timely basis.
- Management responds to the exception or deviation in a timely manner (if management was aware of it).
- The root cause of the exception or deviation is understood.
- Remediation is necessary.

When analyzing the test results, the evaluator must apply the definition of "failure conditions," as set forth in the test plan. It is important that the test plan describe what evaluators are supposed to do when a "failure condition" is noted. For example, evaluators should understand the following:

- ***What constitutes effective and ineffective control operating performance;*** e.g., the evaluator should understand whether risks to achieving stated assertions are mitigated, whether stated assertions are achieved, the quantitative standard (tolerable error) and the qualitative standard ("reasonable assurance").

- ***The sampling approach used and the nature of errors identified,*** proper interpretation of testing results is key.
- ***Implications of control failures to management's assertion of "effective control operation,"*** the need for remediation and the need for additional testing.
- ***Approach to communicating and remediating control deficiencies***

A "failure condition" that cannot be remediated and tested in time prior to the "as of" date constitutes a control deficiency. Management should review control deficiencies and formulate a conclusion as to their severity. There will be times when the results of testing aren't clear. In such situations, judgment is necessary.

All controls deemed compliant with the stated design should be assessed as "effective," i.e., the controls provide "reasonable assurance" that there is no risk of material misstatements to the financial statements because the identified assertion risks are mitigated and the stated financial reporting assertions are achieved. For any controls deemed not to be in compliance with the stated design (i.e., a failure condition), the evaluator should consider:

- The nature of the failure, i.e., is it due to a poorly designed control (a *design deficiency* not detected during the earlier evaluation of design effectiveness)? Is it due to a properly designed control not operating as designed? Or is it due to the person performing the control not possessing the necessary authority or qualifications to perform the control effectively?
- The existence of compensating controls (and the need for additional testing of those controls). See Question 107.
- Qualitative factors, e.g., whether management override occurred.

When the evaluator observes an unacceptable deviation when testing control performance and there is not an adequate explanation for that deviation, it should generally be concluded that the control is "ineffective." The circumstances will be rare where a conclusion is reached that a control is operating effectively when there is a "greater than insignificant" error rate. Our expectation is that the external auditor is likely to concur rarely, if ever, with a conclusion on effectiveness in situations where there are a significant number of errors. For each ineffective control, an action plan should be developed to remediate the deficiency as soon as practicable. The remediation plan should allow sufficient time for validation by management and the external auditor prior to year-end.

The overall responsibility for assessment of control effectiveness ultimately lies with management personnel, who must be satisfied that the testing approach, scope and sample size used in testing a control are sufficient to support a conclusion that the control is operating as intended. Management should evaluate the testing results evaluators report. Management is responsible for deciding what to do to correct control deficiencies.

140. How does management decide which controls to test?

There are several areas management and the project team will want to address before developing a test plan. Validating operational effectiveness without a clear understanding as to which controls are the most critical ones is a blueprint for allocating substantially more resources than necessary to controls testing.

It is not necessary to test every control. The SEC's interpretive guidance does not require that every control within a process be identified and documented to accomplish the purpose of complying with Section 404. Once management identifies the controls that adequately address the risks of material misstatement in the financial statements, it is unnecessary to include additional controls within the scope of management's evaluation. Implicit in identifying the important controls is the need to evaluate the design of the selected controls in terms of their effectiveness in mitigating the critical financial reporting risks. That process provides the context for deciding the controls to test.

The Top-Down Approach

A top-down approach starts with entity-level controls. Management need only select those controls that address the most critical financial reporting assertions. Once those controls are selected, management must then evaluate the effectiveness of their design. The selection process is an important management decision because it addresses what experience has shown to be the most significant cost driver of Section 404 compliance – the number of key controls to evaluate and test. If management's understanding of the control environment is sufficient and that understanding is documented in reasonable detail, as required by the SEC, then it is more likely that the application of the top-down approach will result in selecting the control set that is the most effective in mitigating financial reporting assertion risks. A deficient understanding of the control environment will lead to a lack of transparency that will likely result in failure to select the optimum number of controls.

As noted in our response to Question 81, there are three categories of entity-level controls:

(1) Controls with an important, but indirect, effect on the likelihood a misstatement will be detected or prevented – many controls in the control environment fall into this category

(2) Controls that monitor the effectiveness of other controls, allowing reduction in controls testing

(3) Controls designed to operate at a sufficient level of precision to prevent or detect misstatements

The *absence* of the first category of entity-level controls – the controls having an indirect effect on significant financial reporting elements – *increases* the risk of control failure. The *existence* of the second and third categories of entity-level controls *reduces* the scope of testing process-level controls. These dynamics are why entity-level controls are considered first when selecting the key controls.

After considering the impact of entity-level controls, if additional evidence is necessary to provide reasonable assurance that a financial reporting assertion is met, other necessary controls must be identified and evaluated. With respect to identifying these additional key controls, management should consider the process-level monitoring controls used to manage the important processes affecting financial reporting and select only those controls that reduce to an acceptable level the risk of a material misstatement to the financial statements.

The Filtering Process

The process of "filtering" controls identifies the primary or critical controls on which management relies to mitigate the relevant assertion risks and achieve one or more financial reporting assertions for each significant financial reporting element. Filtering requires careful thought and judgment. In documenting the critical processes and controls, most accelerated filers have already identified many controls related to the financial reporting assertions and the risks germane to those assertions. The tool that management uses to document these controls should provide a basis for selecting the controls to test.

Filtering is important because it narrows down the population of controls to the ones that matter, making the linkage of individual controls with the significant assertions to which they relate a more manageable task. Filtering also increases the efficiency of testing, because without a systematic approach to filtering, companies will be testing more controls than necessary. In fact, the sheer volume of controls to test may influence management to select smaller sample sizes than may be appropriate in the circumstances. If more controls than necessary are being tested, significant nonvalue-added activity may be driven off of the need to understand the reason for exceptions for controls that aren't really important. If evaluation teams rationalize away testing results on the basis that the control wasn't really important in the first place, there wasn't adequate filtering in the selection process.

As noted above, management is only concerned with the controls over significant processes affecting financial reporting. One way to filter controls is to classify the documented controls as primary, secondary and tertiary (see Question 143 for further discussion of these labels of control importance) and focus most of the testing on the primary controls, with some testing of the secondary controls.

Experience has shown that an overwhelming number of controls are often identified during the documentation process. Sometimes the first cut at identifying the "primary" controls falls well short of the goal of narrowing down the control set to the vital few. In such instances, these controls may be further segregated as "critical" or "significant." The idea is to narrow down management's detailed testing to all critical controls. In this approach, "critical controls" are defined as follows:

> The ***first*** subset of primary controls, these controls have a pervasive impact on financial reporting (segregation of duties, system and data access, change controls, physical safeguards, authorizations, input controls, reconciliations, review process, etc.) and have the most direct impact on achieving financial statement assertions and mitigating significant assertion risks. Upon failure of a critical control, there is a reasonable possibility of a material misstatement in the financial statements because no other control has been identified within ***any*** process to prevent or detect the misstatement. Failure of a critical control would affect the ability of management to achieve the company's financial reporting objectives.

"Significant controls" are defined as follows:

> The ***second*** subset of key controls, significant reliance is placed upon the effective design and operation of these controls. Upon failure of a significant control, the risk of occurrence of an undesired activity would not be mitigated regardless of other controls identified within the process; however, compensating controls may exist in other downstream processes to mitigate the risk of occurrence of a material misstatement.

There may be primary controls that, by definition, are neither critical nor significant. These remaining primary controls provide assurance regarding the achievement of certain objectives as well as mitigate the risk of an unanticipated outcome within a process. However, failure of such controls does not preclude the process from achieving its financial reporting objectives. These controls include supplementary financial controls and operational controls.

What's the message? The selection of "primary" controls may not result in the identification of the "key" controls from a testing standpoint without a concerted effort to focus solely on the areas where material financial reporting errors or fraud could occur. This is the crux of the matter, as everything else is secondary. "Filtering" is needed to accomplish this objective.

Some of the factors considered by management during the filtering process include selecting:

- ***Controls that are especially critical to the mitigation of financial assertion risk and the ultimate achievement of one or more financial reporting assertions for each significant account balance, class of transactions and disclosure that is considered a priority financial reporting element.*** The objective is to concentrate testing on the key controls that address the assertions relating to the "high-risk" financial elements. When a single control addresses several assertion risks, its importance increases.
- ***Controls on which other controls are dependent.*** If the effectiveness of a primary control is dependent upon the effective performance of one or more other controls, those other controls are also primary controls. Controls at the process level are dependent on the control environment and general IT controls. For example, the extent of reliance upon a key report used as part of an important reconciliation control procedure may be dependent upon the effectiveness of controls over the IT application system that generates the report. They may also be dependent on IT functionality, which in turn is dependent on the general IT controls. Validation of these controls on which the effectiveness of other controls depend may also involve some direct testing. For another example, when monitoring controls are relied upon, it is important to evaluate the IT processes generating the information that makes effective monitoring possible.
- ***Controls that address each component of internal control.*** If management decides to use the COSO Internal Control – Integrated Framework, testing must be directed to address adequately each of the five components of COSO – control environment, risk assessment, control activities, information/communication and monitoring.

- ***Controls that have the most direct impact on mitigating a risk and achieving an assertion that the company is controlling the flow of financial reporting transactions and information.*** These are the controls that management and process owners would agree are the company's "primary line of defense" to reducing a risk of a material misstatement to an acceptable level and achieving a higher risk financial reporting assertion. Thus, they are the controls that the company looks at first to ensure they are operating effectively before considering all other controls. An example is the use of management approvals to address the risk of unauthorized transactions. Another example is the use of wall-to-wall physical inventories or periodic cycle counting to satisfy the "existence of inventory" assertion. Still another consideration is the proximity of a control to the point within a critical process at which there is a reasonable possibility errors or fraud could occur.
- ***Controls that compensate for controls having a significant risk that they might not operate effectively (which the SEC refers to as "control failure risk").*** Factors that management should consider when evaluating the risk of control failure include:
  - The complexity of the control
  - Whether the control is manual or systems-based, i.e., controls that rely on the competence and performance of an individual may be more prone to breakdowns and error
  - Whether there have been changes in the volume or nature of transactions that might affect controls design or operating effectiveness
  - Whether there have been changes in processes, key personnel, systems or other factors that may affect the performance of internal control
  - Whether there have been changes to controls design
  - The degree to which the control relies on the effectiveness of other controls, e.g., the control environment
  - Whether there have been changes in key personnel who perform the control or monitor its performance

  If one or more of these factors apply to the primary controls designated by management in a critical financial reporting area, there may be a need for compensating controls.
- ***Controls that have a pervasive impact on financial reporting,*** such as authorization and limit controls in volatile areas, segregation of incompatible duties in significant areas, restriction of process system and data access, establishment of physical safeguards over significant assets and processing areas, and implementation of process and systems change controls.
- ***Controls over nonroutine and estimation processes.*** These controls are the manual and automated controls over estimates and period-end adjustments. They often address the greatest risks in the financial reporting process and are most susceptible to management override. Therefore, the tests required to evaluate the operating effectiveness of these controls may not be as reliable as in other areas.

Filtering recognizes that it is not necessary to test every single control when evaluating operating effectiveness. An analogy is that filtering is a targeted "rifle approach" to testing operating effectiveness versus an unfocused "shotgun approach." A top-down, risk-based approach to selecting controls for testing lays a foundation for articulating management's rationale for what is important in supporting its assertions on the effectiveness of internal controls. It is a practical approach because testing requires a great deal of time and resources.

A top-down, risk-based approach to filtering leads the project team to methodically evaluate the financial reporting assertions for each priority financial reporting element and, applying the previously discussed criteria, decide on the key controls to test. While this takes time, it is a preferable approach to testing every control or too many controls. Where necessary, experts in specific control areas (specific process owners, IT management, for example) should be involved in this selection process. What should be avoided is a mechanical approach in which controls are selected for testing off of a comprehensive checklist without regard to importance. The time invested up front in terms of critical thinking about the relevant financial reporting assertions and the related risks and key

controls that address those assertions and risks is a one-time investment. Through a reduced control set, it is possible to design a cost-effective test plan that will save the company a substantial amount of time and costs over the course of the entire testing process, not only during the initial annual assessment but also in the years to come.

141. How does management decide the extent of testing?

Question 140 addresses how a company selects only those controls that are the most critical and significant. Questions 121 and 128 focus on developing the most efficient plan to test controls. This question addresses the quality and persuasiveness of the evidence needed to support a conclusion that the controls are operating effectively.

When determining how to test a particular control, the underlying thought process is risk-based. The SEC's interpretive guidance asserts that management varies the nature, timing and extent of the evaluation methods it implements in response to judgments about risk. The greater the misstatement risk of a financial reporting element and the higher the risk of control failure, the greater the amount of evidence required to support a conclusion that a control is operating effectively. Conversely, the lower the misstatement risk of a financial reporting element and the lower the risk of control failure, the less persuasive the evidence needs to be. Therefore, when evaluating the required amount, or persuasiveness, of the evidence, management must focus on both the risk of misstatement and the risk of control failure.

With respect to the risk of misstatement, the characteristics of the financial reporting element that management considers include both the materiality of the financial reporting element and the susceptibility of the underlying account balances, transactions or other supporting information to material misstatement. When considering the latter, the SEC's interpretive guidance provides several factors to consider. These and other factors are discussed in our response to Question 51.

With respect to the risk of control failure, when considering the likelihood that a control might fail to operate effectively, the SEC's guidance points out the pertinent factors for management to consider. These are discussed in our response to Question 100.

The SEC also observes:

> Financial reporting elements that involve related party transactions, critical accounting policies, and related critical accounting estimates, generally would be assessed as having a higher misstatement risk. Further, when the controls related to these financial reporting elements are subject to the risk of management override, involve significant judgment, or are complex, they should generally be assessed as having higher [internal control over financial reporting] risk.

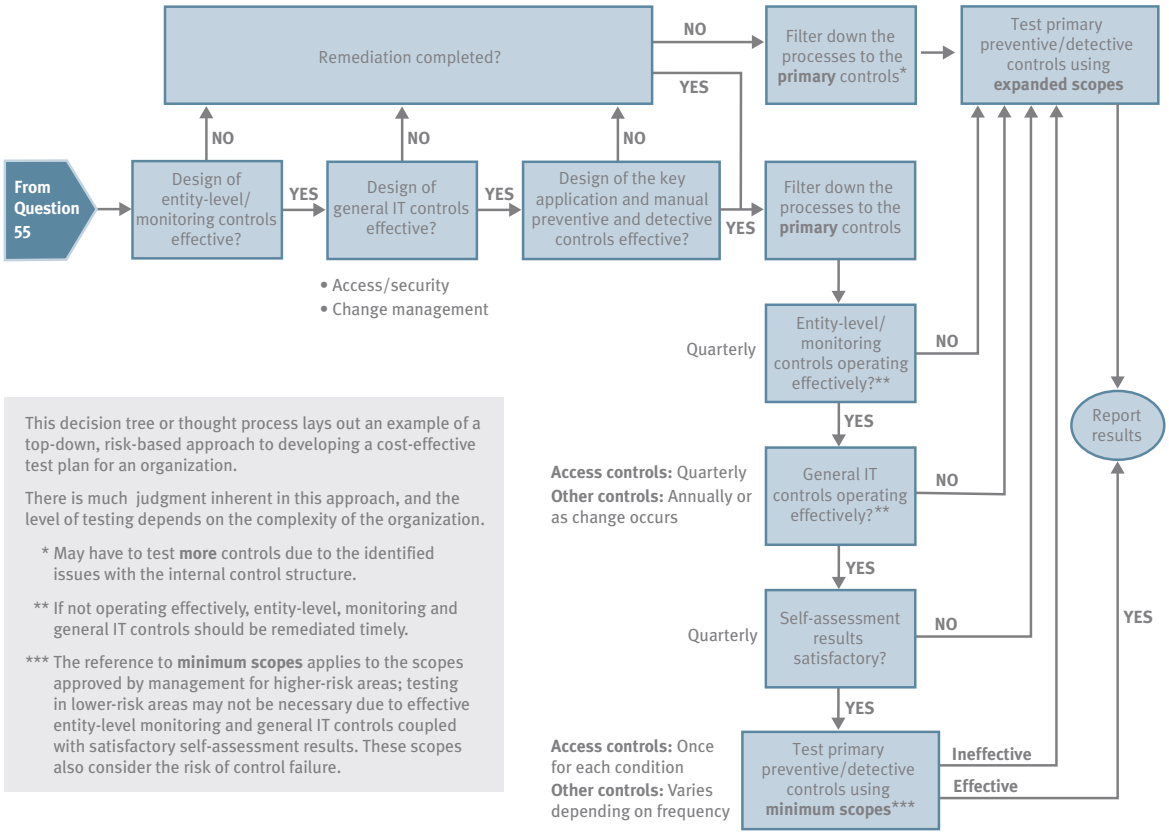
The SEC's commentary clearly highlights the importance of focusing on these higher risk areas. The SEC followed the above discussion with the following assertion:

> When a combination of controls is required to adequately address the risks of a financial reporting element, management should analyze the risk characteristics of each control … [The reason this analysis is necessary] is because the controls associated with a given financial reporting element may not necessarily share the same risk characteristics.

The example the Commission provides on page 27 of its interpretive guidance to illustrate the above assertion clearly reinforces the view that not all tests of controls carry equal weight. The basic premise is that management ordinarily focuses its evaluation on those areas of internal control over financial reporting that pose the highest risk to reliable financial statements. The evaluation procedures that management uses should be tailored to its risk assessment, including the risk of control failure. Management's assessment of risk should consider the relative strengths and weaknesses of the control environment, which may influence management's judgments about the risks of failure for particular controls.

To illustrate, the company should generally *first* assess entity-level controls that have both a direct and an indirect impact on the significant financial reporting elements, *then* assess the impact of general IT controls, and *then* assess the preventive/detective controls at the process level using the established testing guidelines set forth in the test plan.

The following schematic completes the illustrative thought process introduced in the response to Question 55, which identified the processes in which the evaluation team has sourced the greatest risks of material misstatements to the significant financial reporting elements. If entity-level controls (as discussed in our response to Question 81), including monitoring, are ineffective, testing scopes will increase. For example, if there is a weak company-level control environment that cannot be remediated in a timely manner, more testing will be needed at the process level. If the company can remediate deficiencies in the control environment (or in any other critical entity-level controls) on a timely basis, it may stick to the established minimum testing guidelines, as set forth in the test plan approved by management. Test plans often presume that such entity-level controls are operating effectively.



General IT controls are those underlying IT-related controls, such as those related to security administration and change management controls on which other process-level controls depend (see Question 85). If these IT controls are ineffective, there could be instances where management might be unable to rely on monitoring and automated controls, and aggressive remediation might be required. Management should validate effective operation of these controls as soon as possible after concluding on the effectiveness of their design and be prepared to answer the question, "Is there sufficient evidential matter supporting a conclusion that the general IT controls are operating effectively?" If there are deficiencies in change controls and security that cannot be

remediated, more testing will be needed to provide persuasive evidence at the process level. These deficiencies could also result in a "hard stop" to the external audit if significant, e.g., the environment is highly automated in processing a significant volume of transactions for in-scope business processes.

At the process level, it is presumed that tests of controls would address a mix of preventive and detective controls. A control structure that is 100 percent detective is not a sustainable control structure and will encounter issues when significant changes in the business occur. If there are unacceptable testing exceptions, management must investigate the root causes and, in many cases, will need to redesign the control. The redesigned controls are then retested. An alternative is not to do a root cause analysis and test the control again using an expanded scope. If testing is expanded and more errors are found, management will clearly need to find the cause of the error, fix it and retest the new control(s).

142. Why are control descriptions important and how does management know they are adequate?

The SEC's interpretive guidance does not require that every control within a process be identified and documented to accomplish the purpose of complying with Section 404. Once management identifies the controls that adequately address the risk of material misstatement in the financial statements, it is unnecessary to include additional controls within management's evaluation. However, once the key controls are identified, they must be described in a robust fashion. Implicit in identifying the important controls is the need to evaluate the design of the selected controls in terms of their effectiveness in mitigating the identified financial reporting risks.

Before controls can be tested, management and the individuals responsible for testing need to know how they operate. Thus, the project team needs to satisfy itself that descriptions are adequately documented for each primary or key control. The control description should clarify how the controls design provides reasonable assurance that a misstatement in a financial reporting element that could result in a material misstatement in the financial statements would be prevented or detected on a timely basis.

When preparing this controls documentation, the project team should think of a control as a "process" rather than a "technique." A process is a set of related activities that prevents errors or omissions from happening, or detects and corrects them in a timely manner. To simply refer to a control without identifying the person or group responsible for the control or understanding how the control addresses errors, omissions and fraud does not provide a sufficient basis for designing effective tests of operation.

For example:

- Inadequate description: Cycle counts are used.

  Adequate description: Inventory management personnel periodically conduct cycle counts with an objective of systematically covering the entire inventory over a 12-month period. The cycle-counting process covers all locations. Counts are complete. The physical counts are posted immediately to the perpetual records and compared to recorded amounts. Any differences noted are used to process an adjustment to the general ledger. The plant controller approves the adjustment. Significant book-to-physical adjustments, as identified by the plant controller, are investigated to determine the items causing the adjustment and the root causes so that appropriate process improvements can be made.

- Inadequate description: A "was-is" report is used to manage price changes.

  Adequate description: The marketing department reviews an IT-generated "was-is" list, and changes are reconciled to the price change authorization signed by the VP of marketing. If a price change – either an increase or a decrease – was not input to the master price list on a timely basis, such changes are subsequently billed/credited to the customer.

143. How should the Section 404 compliance team classify individual control techniques so that the team, as well as the independent auditor, can more effectively plan the required tests of controls?

There are several ways Section 404 compliance teams can classify individual control techniques to facilitate evaluation of controls design effectiveness and the formulation of test plans to evaluate controls operating effectiveness. These are identified below:

Manual versus system-based controls – *Manual controls* predominantly depend upon the manual execution by one or more individuals, whereas *automated* controls predominantly rely upon programmed applications or IT functionality to execute a step or perhaps prevent a transaction from occurring without human interaction. There are also *system-dependent manual controls*, e.g., controls that are manual (comparing one thing to another) but what is being compared is system-generated and not independently collaborated; therefore, the manual control is dependent on the reliability of system processing.

Why: Manual controls are more susceptible to failure and require more time and effort to test than automated controls. A control structure built primarily on manual controls is not sustainable under stress and change conditions. As transaction volumes increase and with increasingly complex calculations, systems-based controls are often more reliable than people-based controls because they are less prone to mistakes than human beings, *if designed, operated, maintained and secured effectively*.

Preventive versus detective controls – *Preventive controls*, either people-based or systems-based, are designed to prevent errors or omissions from occurring and are generally positioned at the source of the risk within a business process. *Detective controls* are processes, either people-based or systems-based, that are designed to detect and correct an error, or detect and report fraud, within a reasonable period of time, to ensure achievement of a stated objective (e.g., begin the next transaction processing cycle, close the books, prepare final financial reports, etc.).

Why: An effective control structure is built on a mix of preventive and detective controls. A control structure built on detective controls is not sustainable under stress and change conditions. A shift toward an anticipatory, proactive approach to controlling risk requires greater use of preventive controls than the reactive "find and fix" approach embodied in a detective control.

Relevant COSO element – Controls can be classified according to the five COSO elements, as described in Question 40.

Why: It is desirable to address all five components of the COSO framework. Because most control techniques at the process level are classified as either "control activities" or "monitoring," it is acceptable to address the other three components using an overall memorandum in lieu of a risk and control matrix.

Control frequency – Controls may be classified according to frequency of application, e.g., continuous, daily, weekly, monthly, quarterly and annually.

Why: Testing scopes vary according to the frequency by which the control technique is applied.

Control importance – Controls may be classified as primary, secondary and tertiary. These are defined below:

- ***Primary controls*** are the critical activities or tasks performed by management or other personnel that are especially critical to the mitigation of financial reporting risks and have the most direct impact on the ultimate achievement of one or more financial reporting assertions for each significant account balance, class of transactions and disclosure that is considered a priority financial reporting element. These controls are the ones that managers and process owners primarily rely on; therefore, they must be designed effectively and must operate as designed. Primary controls provide reasonable assurance regarding the achievement of certain objectives, as well as reduce the risk of an unanticipated outcome to an acceptable level. If these controls fail, there are usually no other controls in place to compensate for the failure.

- ***Secondary controls*** are documented controls that contribute significantly to the mitigation of risk and the ultimate achievement of one or more financial reporting assertions, but are not considered as important as primary controls by management and process owners. While these controls are significant, there are compensating controls that also assist in achieving the assertions. If these controls fail, there are other controls in place to compensate for the failure.
- ***Tertiary controls*** are other documented controls that are neither primary nor secondary; i.e., they are not particularly important to the mitigation of risk and the achievement of financial reporting assertions. Therefore, management and process owners do not place reliance on them. The SEC does not require documentation of these controls for purposes of Section 404 compliance.

When companies segregate their control population in this or a similar manner, some only provide the primary controls to the external auditor. The objective is to provide the auditor with only the key controls on which management has chosen to rely, rather than place the auditor in a position of having to wade through controls that the company has already taken out of scope.

Application of the above definitions is illustrated in Question 140.

Why: Companies often test too many controls and, therefore, there is undue emphasis on selecting small sample sizes. There is not enough emphasis on filtering down the documented controls to the vital critical or significant controls that need to be tested to enable more thorough testing of fewer controls. Filtering the population of controls down to the vital few that matter is critical to evaluating controls design effectiveness and efficient testing of controls operating effectiveness. For example, the focus of testing should be directed to the primary controls, particularly if the primary controls are so critical there are no compensating controls should the primary control fail to operate as intended. Secondary controls may also be tested in tandem with testing other controls.

Controls over routine processes versus controls over nonroutine processes – *Controls over routine processes* are the manual and automated controls over day-to-day transaction flows. *Controls over nonroutine processes* are the manual and automated controls over estimation transactions and period-end adjustments; these controls often address the greatest risks in the financial reporting process and are most susceptible to management override. In addition, the SEC's interpretive guidance states that "financial reporting elements that involve related party transactions, critical accounting policies, and related critical accounting estimates, generally would be assessed as having a higher misstatement risk." The Commission also states that "when the controls related to these financial reporting elements are subject to the risk of management override, involve significant judgment, or are complex, they should generally be assessed as having higher … risk."

Why: Controls over routine process may be tested throughout the year with some refresh testing toward the end of the year. Controls over nonroutine processes are more appropriately tested closer to the end of the year.

Controls addressing fraud versus controls addressing unintentional errors – Fraud is unlike inadvertent error. It is intentional, unrelated to actual transactions, not random, covered up and often facilitated through collusion with intent to deceive. Therefore, it must be considered differently than inadvertent error. That said, there are many controls that serve a dual purpose in addressing both fraud and inadvertent error. Classifying controls in this manner will ensure that controls over fraud have been considered explicitly in the Section 404 evaluation.

Why: The SEC and PCAOB have made it clear that risks and controls must be addressed with respect to ***both*** intentional and inadvertent errors. The intent was to make fraud risk explicit in the assessment of risk and in formulating a conclusion as to the design effectiveness and operating effectiveness of internal control over financial reporting.

144. Is testing by process owners acceptable for purposes of supporting management's assertion?

Yes, at least partially. There are two related questions when evaluating the degree of reliance on testing by process owners. First, there is the question of objectivity, i.e., are the process owners responsible for the execution of the controls tested? This question is discussed further below. Second, what evidence must the process owners have to support their assessments on an ongoing basis? Would inquiry, observation and inspection be enough? All three of these techniques are integral to effective supervision and are included in the testing techniques listed in our response to Question 123. What's left is the reperformance technique, which many process owners may believe is not necessary due to their day-to-day involvement with the process and the monitoring controls they already have in place.

That said, testing by process owners alone is ordinarily not a sufficient body of evidence for management to base a conclusion in higher risk areas. More evidence is needed through formal self-assessment reporting from the process owners, entity-level monitoring and analytics, and independent tests of controls by internal audit or other parties who are free of bias and can evaluate test results in an impartial manner. Note that the external auditors will not rely on management's use of process-owner testing in higher risk areas.

The SEC guidance to management explicitly acknowledges the use of self-assessment techniques. Going forward, we believe that many registrants will use self-assessment as *one* source of evidence in supporting management's assertion regarding the effectiveness of internal control over financial reporting. The term, "self-assessment," is often used to describe circumstances where company personnel evaluate the controls for which they are responsible and communicate the results of their self-review to management. For purposes of discussion, "company personnel" may or may not be process or control owners.

A robust self-assessment approach is always process-based, and involves several key components, including the (a) identification of the most important controls, (b) identification of the owners of those controls, (c) predetermination of questions approved by management, (d) rigorous deployment of questions and appropriate follow-up with control owners, and (e) resolution of exceptions and open matters on a timely basis. Self-assessment may be enhanced to a higher form of evidence if the personnel responsible for conducting the assessments are also required to test a minimum sample of items before formulating their conclusions on operating effectiveness. If performed by process owners, these self-applied tests augment the inquiry, observation and inspection techniques the process owners often use as they supervise and monitor the activities for which they are responsible on a day-to-day basis to assess whether controls are functioning properly. Coupled with periodic reviews by internal audit to evaluate the quality of the overall process, a self-assessment program might be sufficient evidence for lower risk areas. If higher levels of management personnel armed with effective monitoring controls also are involved, the quality of the evidence resulting from the program may be further enhanced.

Our response to Question 189 discusses the design of a self-assessment program. The matter of objectivity is an important consideration when designing a self-assessment program and determining the extent of reliance on the results of that program. The SEC's interpretive guidance to management states:

> Self-assessment … can refer to different types of procedures performed by individuals with varying degrees of objectivity. It includes assessments made by the personnel who operate the control as well as members of management who are not responsible for operating the control. The evidence provided by self-assessment activities depends on the personnel involved and the manner in which the activities are conducted. For example, evidence from self-assessments performed by personnel responsible for operating the control generally provides less evidence due to the evaluator's lower degree of objectivity.

The SEC's guidance suggests strongly that management can increase the value of the evidence from the self-assessment process by deploying personnel who are more objective. This point is discussed further in our response to Question 117.

Self-assessment should be an integral part of the body of evidence arising from management's assessment process. There is no cookie-cutter approach, and each case is evaluated on a "facts and circumstances" basis.

For example, consider the following questions:

- Do the process owners understand how to test controls (i.e., are they competent)? Have the process owners received adequate training on how to evaluate test results?
- Are the process owners testing their own work or the work of control owners who work for them?
- How does management know that quality testing is performed? Who sets the testing scopes?
- Are the process owners evaluating and testing key controls which are complex in application?
- Are any of the self-assessed key controls addressing higher risk areas from a financial reporting standpoint?
- Are the process owners testing remediated controls?
- What is management's risk appetite around the level of process owner testing versus independent direct testing by internal audit or other objective evaluators?

These and other questions lead management to evaluate the appropriate mix of process owner testing, entity-level monitoring and independent testing to put in place as part of a cost-effective test plan supporting management's assertion in the annual internal control report. Process owner testing coupled with reported process owner self-assessments provide management with a strong base of evidence to use when planning the nature, timing and extent of independent testing required. Ultimately, the decision as to the appropriate mix of evidence is management's to make and defend.

145. With respect to the period between the date management completes its preliminary evaluation of operating effectiveness and year-end, what must management do to update its evaluation?

Management should complete the preliminary evaluation on a timely basis so that the external auditor can evaluate the evidence supporting management's preliminary assertion on internal control. The purpose of the suggested approach outlined in our response to Question 57 is to support the development of the body of evidence in the initial year of Section 404 compliance to enable the external audit to begin while the necessary remediation and repair take place.

Thus, the period between the date management completes its evaluation (say the end of the second or third quarter) and year-end (the date as of which management must assert the effectiveness of internal control) is an important issue to consider. Changes may have occurred and other issues may have arisen that might have affected the internal control structure since the date of management's preliminary evaluation. If self-assessment is used at year-end and monitoring controls are strong, the refresh testing required at year-end may be reduced to a minimum. However, for the critical controls over the priority financial reporting elements, the evaluator may want to perform some refresh testing. Whether that testing takes place as of or after year-end or during a period before but close to year-end is largely dependent on management's confidence in the control structure and the effectiveness of monitoring.

Refresh testing updates interim tests of operating effectiveness to obtain additional evidence to support assertions as of the report date. On the other hand, the purpose of retesting remediated controls is to formulate a conclusion regarding the effective operation of those controls for a sufficient period of time prior to year-end. If the testing results are satisfactory, management should document the resolution of each exception and that the control has been improved. If the testing results are not satisfactory, the unresolved deficiencies along with other control deficiencies that have not been remediated must be evaluated in terms of whether there are other compensating controls in place and found to be operating effectively. If compensating controls do not exist, then management must evaluate the severity of the deficiencies.

At year-end, management must also assess whether there have been changes in internal controls, or in factors that affect the performance of internal controls, subsequent to the interim testing period. Such changes would invalidate or otherwise impact the results of tests of controls performed at an earlier point in time in the year. For example, the impact of significant changes in processes, personnel and application systems that occur subsequent to the interim date and affect the control environment needs to be evaluated and, as a result, additional tests of controls will be necessary. Such changes could also affect the adequacy of controls design effectiveness and require an update of that assessment. Another example would be changes to address control deficiencies identified as part of the ongoing assessment process. A preventive control previously considered effective may prove to be ineffective if unexpected errors emerge and are detected downstream by compensating controls (see Question 107). In all of these circumstances, these changes require an update in testing. Further, some controls may function only at year-end; thus, it may only be feasible to test them at or even after year-end.

An updated review is also an opportunity for management to begin putting in place its process for ongoing evaluations of changes in internal control that must be performed on a quarterly basis starting in the year after the initial year of compliance.

The use of technology can provide a self-assessment solution to refreshing the second- or third-quarter body of evidence and position the company for ongoing periodic self-assessments. Through technology, self-assessment can be done at any time. For example, one calendar-year reporting company deployed self-assessment around December 15 to ensure there are no surprises when it requires its process owners to self-assess their controls and report the results as of December 31. Independent testing is also applied to risky areas during the fourth quarter.

In addition, management should consider strengthening its entity-level monitoring and analytics with the objective of using them on an ongoing basis to support the quarterly evaluation process. The use of self-assessment technology and the entity-level monitoring techniques during the last quarter of the initial annual assessment can serve a dual purpose – first, to achieve the objective of updating the preliminary first-year evaluation to year-end without having to perform extensive additional refresh testing and, second, to provide a "dry run" of management's approach for conducting periodic evaluations during the second year and beyond.

In the second year and beyond, the process that companies should consider having in place on an ongoing basis might include the following:

- A technology solution to put a cascading and process-based self-assessment approach in place.
- Adequate entity-level monitoring controls and process analytics, so a problem in the financial controls would be detected in a timely fashion.
- Periodic independent tests of controls by internal audit and/or risk control specialists, with emphasis on higher risk areas.

Tests of controls by internal audit would also be designed to evaluate the quality and reliability of the self-assessment process and the integrity of the reports that make entity-level monitoring possible, as well as to perform direct tests of controls. See Questions 186 through 197 for a discussion of the second year and beyond.

146. What should management do when exceptions are identified?

When exceptions are identified, they must be evaluated carefully. When small minimum judgmental sample sizes are used, exceptions can taint the ability to rely on the test results. Even one exception can be an issue depending on the facts and circumstances.

A control with an observed deviation rate that is clearly significant is not an effective control. The correct perspective is to look for controls for which the deviation rate, if any, is negligible. Management must be satisfied that the testing approach, scope and sample size used in testing a control are sufficient to support a conclusion that the control is operating as intended without a greater than insignificant error rate.

When testing operating effectiveness, exceptions or deviations to the control may occur. When evaluating the reasons for the exceptions or deviations, the project team should consider whether:

- The control is automated (in the presence of effective general controls, there is a presumption that an automated application control is expected to always perform as designed).
- The degree of intervention by entity personnel contributes to the exception or deviation.
- Management became aware of the exception or deviation on a timely basis.
- Management responded to the exception or deviation in a timely manner (if management was aware of it).

Regardless of the reasons for the exceptions or deviations, numerous or repeated instances may constitute a control deficiency that is potentially at least a significant deficiency unless other compensating controls are identified and found to be operating effectively. When the project team tests control performance and observes a deviation rate that is not negligible, management cannot rationalize the exceptions away and conclude the control is effective. However, management may consider expanding the testing scope and sample size to determine whether the results of the initial test are conclusive.

147. How is monitoring evaluated?

Monitoring takes place at both the entity and process levels. Entity-level monitoring includes analytics and metrics. As noted in Question 81, monitoring at the entity-level includes controls to monitor results of operations and controls to monitor other controls. According to the SEC, the latter type of monitoring controls includes activities of the internal audit function, activities of the audit committee and self-assessment programs. "Monitoring activities" assess the quality of internal control performance over time. These activities involve assessing the design and operation of controls on a timely basis and taking necessary corrective actions. The process is accomplished through ongoing monitoring activities, separate evaluations by internal audit or personnel performing similar functions, or a combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of an entity and include regular management and supervisory review activities.

Following are a few examples of monitoring activities:

- Independent testing of controls by objective and competent internal auditors or risk control specialists to ascertain whether selected controls are performing as intended.
- Predictive tests by the finance function provide an effective means of evaluating the results of process performance. For example, interest expense is calculated based upon number of days of outstanding debt, and weighted-average interest rates provide a means to determine whether reported interest expense is reasonable.
- Exception reports, such as the ones provided by an ERP system when the appropriate controls are configured correctly, provide IT management with an indication as to the effectiveness of specific internal controls (e.g., authorization controls, limit controls, change controls, etc.).
- Audit reports issued by internal audit confirming compliance with established policies and providing assurance that specific controls are operating as intended and process measures are reliable, etc. These reports may utilize points of focus obtained from the COSO framework and customized by the evaluation team to evaluate the control environment and other internal control components. They are effective in detecting errors timely if the audit results are communicated timely, elevated to the appropriate level of management and acted upon in sufficient time before the fiscal year end.
- Budgetary controls provide management an effective mechanism for monitoring operating results, particularly when the budget is based upon specific factors such as volume, price and mix, enabling the determination of meaningful variances for further analysis and investigation. These controls facilitate preparation of P&L attribution reports summarizing how the organization makes or loses money. This kind of reporting discipline enables management to understand what is going on in the business and to initiate investigations when

things don't look right. When focused at a level of precision that is less than material and applied routinely in a timely manner, these controls can be effective in monitoring lower to moderate risk financial reporting elements, particularly when they are proven to be effective over time in detecting errors before financial reports are released.

- Results of key performance indicators (KPIs) are evaluated by management with the objective of reconciling operating and financial information using knowledge of the business. These process metrics may address relevant key factors, such as number of shipments during the last week of each reporting period, sales volume versus plan and prior year, store sales per cash register, SG&A spending accountability reports, etc.
- Supervisory reviews of the execution of process activities and controls confirm adherence to established policies and procedures. For example, a supervisor might review closely the control activities performed by new employees, the results of new process activities and the performance of activities in areas where problems have occurred in the past or where customer or supplier complaints have been received, in addition to performing spot checks in routine and stable areas.
- The audit committee evaluates periodically the process of handling confidential, anonymous submissions from employees on sensitive matters and reviews background information on and qualifications of selected new hires in key management positions and, in particular, those positions affecting financial reporting.
- Event reports summarize the number of incidents or near misses, e.g., the number of instances of errors, down time, limit violations, etc. These reports spawn investigations to identify the root cause of reported events.

These are just a few examples.

At the process level, process owners are generally supervisors or managers of individuals or departments responsible for performing specific control activities. In certain circumstances (such as for small companies), members of executive management may also be process owners due to their daily interaction with specific controls. In their role, process owners often use inquiry, observation and inspection techniques to satisfy themselves during the supervisory process that the controls are functioning properly. There may also be reports that enable them to evaluate the effectiveness of the process. For example, suspense reports and aging of items in suspense provide an indication as to the effectiveness of the process.

According to COSO, monitoring can be achieved either by obtaining direct evidence of the operation of specific controls or by testing results of control processes. An evaluation of monitoring effectiveness would include review of the integrity of the metrics, information and reports used during the monitoring process. That review can include an evaluation of general IT controls and the IT functionality on which specific controls depend. The evaluation should consider the actions taken by management on exceptions, including assessment of the resolution of exceptions and determination of root causes and action taken to correct errors and improve processes. An evaluation of monitoring should be performed quarterly or monthly as determined by management's test plan.

If process owners are reviewing and approving journal entries prepared by someone they supervise, they ordinarily should evidence the process. For example, assume a supervisor checks a journal entry listing on a screen prior to posting. The supervisor may evidence his or her review in different ways, such as (a) document approval electronically, noting name and date, provided the person preparing the journal entry can't also approve it, (b) annotate the required review on a predetermined checklist that includes other "sign-off procedures," or (c) print, sign and file the listing noting the review. The means of evidencing the review also serves as the medium by which the review process is periodically monitored by internal audit or others.

The extent of monitoring tests should reflect a representative sample of a sufficient size to include exceptions to be satisfied with appropriate follow-up by management. A key aspect of monitoring at the process level relates to the actions taken by the control process owner when any exceptions are encountered. These actions should include identifying the root cause(s) of the exceptions, correcting the exceptions and ensuring appropriate process improvements or other necessary actions are taken to avoid the occurrence of future exceptions.

148. How are pervasive process controls tested?

Pervasive process controls, as discussed and illustrated in Question 93, can have an indirect impact on the operating effectiveness of information process controls. They include company- or entity-level controls such as establishing and communicating objectives and assigning key tasks to people with the requisite knowledge and skills. They also include entitywide controls such as authorization and approval controls, limit controls, performance measures, segregation of incompatible duties, physical safeguards, restricting process system and data access, and redundant/backup capabilities.

The so-called pervasive process controls apply to all categories of control objectives, including operational effectiveness and efficiency, and compliance with applicable laws and regulations. These controls span across business processes, and ensure authorization and control over process changes (e.g., are they authorized, tested and effectively implemented?), segregation of incompatible duties (e.g., authorization, custody and record keeping), and integrity of programs and data that support execution of specific controls activities and monitoring.

On an annual basis or as changes occur, management should use inquiry, observation and inspection to validate pervasive controls designed to communicate objectives, establish authority and assign duties, create physical safeguards, apply process and systems development standards, and implement process change controls. On a semiannual or quarterly basis, management should test the pervasive controls designed to implement change and access control functions. A customized plan for testing process and systems development standards, process change controls and access controls should be developed involving appropriate technology risk expertise. The nature and extent of testing and ultimate determination of the operating effectiveness of pervasive controls is based upon the evidence available and management's judgment.

149. How are information process controls tested?

Information process controls, as discussed and illustrated in Question 93, are the manual and application controls that apply to any process generating financial and/or operating information, and provide assurance that information is reliable for use in decision-making. "Reliability" means relevant, complete, accurate and timely.

Process owners should self-assess their controls and report results to management. Self-assessment results should cascade upward to the disclosure committee and/or the certifying officers.

However, self-assessment is not enough. Management should also periodically test specific information process controls. Testing should be designed to provide assurances as to the quality of control self-assessments. Increased frequency of testing will allow earlier detection of any control deficiencies and implementation of process improvements to prevent future errors.

Management should design tests of controls to focus on a combination of tests, including inquiry, inspection, observation and reperformance. Examples of tests include the following activities:

- Obtain samples of processed transactions and evaluate attributes or amounts for purposes of inferring whether controls are operating effectively. More extensive samples are required for manual controls whereas a "test of one" (see Question 150) may be sufficient for application controls provided there are strong general IT controls in place.
- Perform reasonableness tests using either internal or external data.
- Compare accounting balances with budgets and prior periods and, if possible, with industry peers.
- Review reconciliations prepared by others and evaluate the appropriate disposition of reconciling items.
- Review the nature and magnitude of items on exception reports on a sample or comprehensive basis and evaluate whether the resolution/disposition of the individual exceptions by others was appropriate.

- Evaluate the differences that result from independent verification of balances by others (e.g., by confirmations from counterparties, physical observation and monthly statements received from vendors), and evaluate the appropriate disposition of these differences.
- Evaluate process metrics related to activity levels or the time, cost and quality of process activities.

150. How are IT controls tested?

See Question 85 for our approach to breaking down IT considerations during an assessment of internal control over financial reporting. We recommend considering IT controls together with the manual controls in an integrated fashion within a process, i.e., test the IT controls in a manner similar to the controls in other process areas. Whether controls are manual or automated or both, the relevant financial reporting assertions must be addressed and the appropriate combination of inquiry, inspection, observation, and reapplication and/or reperformance testing techniques must be applied to formulate a conclusion related to operating effectiveness. Adequate documentation of the testing should also be developed.

At the IT entity level (see Question 85), we expect most of the testing to be related to inquiries, inspection and observation techniques. Reperformance and reapplication techniques cannot typically be accomplished for many of these types of controls.

For the processes in the general IT controls area and for application and data owner controls (as discussed in Question 85), there is a need for all four types of testing, including reperformance and/or reapplication. These are processes in which key controls can and should be tested similar to other processes. Process flows and risk and control matrices should be referenced and considered when selecting the types of tests needed. With respect to timing, some external auditors may assert that pervasive controls such as IT general controls should be tested near the "as of" date. In the initial annual assessment, however, management should complete the testing of these controls as early as possible in the overall process because the results of these tests can drive potentially significant remediation efforts and could directly impact the nature and extent of testing of application controls. In such instances, some update testing near the "as of" date also may be appropriate to support management's assertion.

With respect to *testing application-specific processes*, if the general IT controls are designed adequately and are operating effectively, programmed controls consistently operate – either consistently correctly or consistently incorrectly. Therefore, there are two areas to consider:

- ***Embedded programmed controls:*** This program logic includes reasonableness checks, error checking, matching routines, error and exception reporting, complex calculations, critical management report integrity, etc. The evaluation team *must test each condition*. A "condition" relates to a step in the program logic, i.e., if a routine matches a vendor against the approved vendor list, there are at least two conditions (they match, they don't match). These tests are dependent on the effectiveness of application change controls.
- ***Other programmed controls:*** These types of controls include interfaces, segregation of duties, access controls for critical transactions and data. They must be considered separately since they represent processes that are more dynamic in nature and depend on a proper functioning of the associated process activities.

When testing application-specific controls, there ordinarily is no need for a large sample if the general IT controls are designed and operating effectively. For example, evaluation teams may perform a "test of one" covering all conditions. However, in order to justify such a low scope it is possible the external auditor could require a detailed review of the application logic to form a baseline conclusion that the program logic is consistent with management's assertion. In such instances, this is an initial year issue and management may choose to prioritize applications for this purpose and evaluate input and output controls for some applications. Once the baseline is established in the initial annual assessment, the company can focus on change controls and the impact of changes in key application systems.

The response to this question is more fully discussed in Protiviti's companion publication, *Guide to the Sarbanes-Oxley Act: IT Risks and Controls*, which outlines an overall approach for integrating the consideration of IT risks and controls into the Section 404 compliance project.

151. How much testing should management perform relative to the testing the external auditor performs?

Management's responsibility is to support the assertion in the annual internal control report. As explained in Question 121, a balanced approach to accumulating the necessary evidence is sufficient. Management is not required to perform independent direct tests in the same areas tested by the external auditor. Management is also not required to use the same sample sizes as the external auditor in the areas management decides to test. That said, management needs to evaluate the sample sizes needed to provide a high level of assurance that the key controls are operating effectively, particularly in the higher risk areas. See Question 135 for factors management should consider when evaluating sample sizes.

152. What should the Section 404 compliance team do if a significant level of exceptions is encountered during testing?

Exceptions should be expected in testing. The compliance team should evaluate each type of exception to understand the nature of exceptions encountered during testing. The number of exceptions should also be considered, as discussed in Question 153. If the nature of exceptions and number of exceptions are not an issue in terms of evaluating the effectiveness of the control in accordance with the parameters set forth in the test plan (see Questions 128 and 129), the test is completed.

If the nature of exceptions and number of exceptions are an issue, there are several options:

- The compliance team can select a second sample that is expanded in size and retest the control. Retesting in this manner can be expensive because the second test can also generate an unacceptable level of exceptions.
- The compliance team can evaluate the root cause of the exceptions, define the necessary remediation in control design and/or operation, determine that the remediation takes place and then retest the remediated control.
- The compliance team can determine whether there are other controls that address the control objective and, if there are, test those controls to determine whether they are operating effectively and can serve as compensating controls. However, even if other controls are in place and operating effectively, the company must carefully consider whether follow-up is necessary with respect to the initial key control tested because that control was selected as part of the controls design on which management is relying to satisfy a specific financial reporting assertion. The validation process cannot be trivialized by testing controls until the evaluator finds controls that work. Compensating controls may not be considered when evaluating whether a control deficiency exists (see Question 107).

The above points support the assertion in our response to Question 129 that the rules of engagement should be defined up front in the test plan.

153. How many exceptions are acceptable before a control deficiency is deemed to exist?

The answer to this question ultimately depends on the answer to two implied questions:

- What level of error *do we expect* in the population?
- What level of error *are we willing to accept* in the population?

We can draw several observations from this point of view:

- A control operation that occurs with numerous or repeated exceptions is not an effectively operating control.
- When small minimum judgmental sample sizes are used, *any number* of exceptions can present an issue. In such instances, management needs to consider drawing another sample that is expanded in size to obtain

more compelling evidence the control is operating effectively or take remedial action and retest the control again.

- Generally, the test plan should set a standard for a high level of operating effectiveness. For example, what level of effectiveness would management normally expect in any significant business activity? Would management accept a 2 percent defect rate in its products shipped to customers? No competitive business would accept that level of defects. The same point holds true for any significant business activity representing a repeatable, defined process, particularly a process that significantly affects one or more significant financial reporting elements.
- When sample results are on the margin, management should ask the two questions noted above. When considering these questions, it is important to recognize that a test of a sample of items is only an attempt to support an expectation about the level of error that actually exists in the population. When management and process owners select a control as part of the control design that achieves a financial reporting assertion, it is presumed the control is operating effectively. The objective of testing is to validate that presumption. If the sample includes errors, it will be difficult to prove to the external auditor that the control is effective. Therefore, if testing results are marginal, management should consider drawing an expanded sample to retest the control and obtain more conclusive evidence it is operating effectively.
- A "reasonable person" test can be applied to the question of "how many exceptions are acceptable" before a control deficiency is deemed to exist. In other words, what would a reasonable person conclude after evaluating the number of exceptions arising from a given test? If the answer isn't clear, another test or remediation may be warranted.
- Management should caution Section 404 compliance teams and process owners about "rationalizing away" exceptions. If that kind of bias takes place, the quality of testing results will be compromised, which increases the risk of significant deficiencies (or worse) arising from the attestation process. For example, when the auditor reviews the company's testing working papers, he or she could reject the conclusions reached based on the company's documented testing results. The auditor could also perform his or her own test and arrive at different results leading to a conclusion the control is not operating effectively.
- Finally, it is difficult for Section 404 compliance teams to conclusively state the "acceptable number" of exceptions when there are compensating controls. If the documented controls design includes compensating controls, management may consider that fact when evaluating test results. On the other hand, if there is an absence of compensating controls, that raises the criticality of the control being tested. Section 404 compliance teams should generally avoid considering compensating controls when evaluating exceptions for an individual control. See Question 107.

The above points illustrate the considerable judgment coming into play when evaluating test results. They underscore the importance of defining the rules of engagement up front in the test plan, including defining a "failure condition" as discussed in Question 129.

154. What if the external auditor's testing results differ from management's results?

Management needs to be aware of the possibility of this occurring. If it does occur, management should seek to understand the facts and compare the auditor's tests of controls to the company's tests supporting the year-end assertion that the controls in question are operating effectively. If the external auditor identifies an error through substantive tests of balances that is material to the financial statements and is not due to an error in judgment, he or she may assert that the error is due to a material weakness in internal control. This situation may cause management to reassess its testing approach in certain areas.

155. Should the external auditor participate during management's testing process?

As a general rule, this participation rarely occurs and is unnecessary if management and the auditor are in agreement on the test plan and the format for documenting testing results.

Remediation

156. If control deficiencies or gaps are identified, how should we remediate them?

When the evaluation team faces control deficiencies or gaps, the team must evaluate the nature of the identified deficiencies and decide the deficiencies requiring correction. With respect to the deficiencies requiring correction, the evaluation team must design and implement a solution. When designing a solution, the team should address the nature of the deficiencies. For example, *for design deficiencies*, the team should decide and document design improvements. *For operating deficiencies*, the team should make recommendations on providing the necessary authority or deploying the appropriate competencies to improve performance. When implementing solutions, the team should execute the following steps: Build and test design improvements, roll out design improvements, update policies and procedures, provide training and measure performance.

157. Assume a company identifies a material weakness in internal control and remedies that deficiency during the year it is required to comply with Section 404 under the SEC's rules. How soon before the end of the fiscal year must the deficiency be corrected?

This issue can be summed up with the following two questions:

- If a company has a material weakness, how long does the "fix" need to operate effectively to enable management to conclude that a material weakness doesn't exist as of year-end?
- If management is able to conclude that a material weakness doesn't exist as of year-end, what period of time does the auditor need to attest to management's assertion?

As noted in Question 109, the determination of whether a deficiency is a material weakness rests with management and its auditors. The issue posed by this question adds yet another dimension by focusing on the time frame in which a "fix" must operate effectively to overcome the "taint" of the control deficiency. It is an issue that will likely be a "facts and circumstances" call, where management will want to consult with the company's independent accountant. Consultation is important because the audit firms have formulated policies as to the minimum time frame for a control to be in operation. In general, a shorter period might be required if the remediated control is performed more frequently, is nonjudgmental in nature, is automated or is an integral part of several compensating controls on which management is relying with respect to a material transaction. On the other hand, if the control is performed less frequently, is judgmental in nature, is manual or is the sole control on which management is relying with respect to a material transaction, a longer period would be required. See also our response to Question 158.

The real message is that if a company has a material weakness, management should get it fixed sooner rather than later to avoid a situation in which there is insufficient time to demonstrate effective operation of a remedy.

A certifying officer may be able to conclude, for purposes of the certification and the internal control report, that a material weakness has been sufficiently corrected "as of" the end of the relevant fiscal period to permit a conclusion that internal control is effective. However, the company should consider whether the prior existence of the material weakness generated material errors or omissions in previous reports, including interim reports. Furthermore, the company should consider whether the existence of a material weakness during the fiscal period is a matter that should be disclosed to investors. The existence of a material weakness and its remediation could very well constitute a material change in internal control over financial reporting.

158. Since this Section 404 project requires a point-in-time review, for how long do remediated controls need to be in place and in operation to be considered effective?

Management should ensure the new controls are in place for a sufficient period of time to permit testing of operating effectiveness. The time period must be adequate to enable both management and the auditor to obtain sufficient evidence of the controls' effective operation. For controls over routine processes that are

applied continuously or daily, a period of four to six weeks should suffice. For controls operating on a weekly or monthly basis, a couple of months should be adequate. *The goal* is to assess the operating effectiveness of such remediated controls between the time they were implemented and year-end. The major audit firms have adopted policies on the minimum time frame within which to accomplish that goal, so consultation with the auditor is advised.

Special Circumstances and Situations

159. How does management evaluate the company's internal control with respect to unconsolidated investments accounted for under the equity method?

Assume Company A, an issuer with listed stock, owns 25 percent of Company B, a private company, and accounts for its investment using the equity method. If Company B's statements are audited, the management of Company A should focus on ensuring the company's investments in this unconsolidated entity are properly accounted for in accordance with generally accepted accounting principles, based upon the available audited information and the timing of that information relative to year-end. This view from a consolidation perspective is a practical one as investors rarely have the level of influence to require transparency related to internal controls of investee companies.

The SEC staff has pointed out that investee companies accounted for under the equity method are not consolidated on a line-by-line basis in the investor's financial statements. Therefore, the investee company's controls over the recording of transactions into the investee's accounts are not part of the issuer's internal control structure. In making this point, the staff makes 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.

If the investee's financial statements are audited, the investor should have processes and controls in place in the closing and consolidation process to obtain and use relevant information to account for the investment using the equity method. These processes and controls would focus on:

- The selection of accounting methods for equity investments, including the recognition of earnings and losses using the equity method.
- Obtaining audited or unaudited financial information for use in recording the equity pickup of the investor company's prorata share of income or loss. For example, the investor might require, at least annually, audited financial statements to "true up" the equity pickup recorded based on unaudited or other information.
- Consistent application of the estimation processes necessary to cover the gap between the investor company's reporting date and the date of the most recent set of financial information from the investee company. The financial reporting objective is to ensure that 12 months of equity pickup is recorded during each annual period.
- Proper treatment of dividends, if any, as a reduction of the investment.
- Obtaining the necessary information to determine whether an impairment has occurred and to ensure the appropriate involvement of management in reaching a conclusion as to the need for an impairment write-down. These asset impairments are rare in practice.

160. How are material acquisitions occurring during the fiscal year handled for purposes of determining the scope of the Section 404 assessment?

The SEC provides relief on the issue of acquired entities of such size and/or complexity whereby it is impossible for the acquiring entity's management to complete an assessment of their internal control over financial reporting during the period between the consummation date and the acquiring company's fiscal year-end.

While the SEC staff indicated it is expected that the acquiring entity's management would ordinarily include in its scope the controls at all consolidated entities, they acknowledged that it might not always be possible to conduct an assessment of an acquired entity's internal control over financial reporting in sufficient time to incorporate the results in the internal control report filed for the year during which the acquisition took place.

The effect of the SEC staff's position is as follows: If there is an acquisition during the year, the acquiring entity's management may evaluate the facts and circumstances to determine whether there is sufficient time and/or resources to consummate the assessment of internal control over financial reporting for the acquired entity in accordance with the appropriate assessment scope on a consolidated basis. If management decides to exclude the acquired business from its report on internal control over financial reporting, the staff would not object so long as there is adequate disclosure. With respect to adequacy of disclosure, the SEC staff expects the following:

(a) Management must refer in the internal control report to a discussion in the registrant's Form 10-K or 10-KSB regarding the scope of the assessment, noting that management excluded the acquired business from management's report on internal control over financial reporting.

(b) If the reference in (a) is made, management must clearly identify the acquired business excluded and indicate the significance of the acquired business to the acquiring company's consolidated financial statements.

(c) Notwithstanding management's exclusion of an acquired entity's internal controls from its annual assessment, the company must disclose any material change to its internal control over financial reporting due to the acquisition in accordance with Exchange Act Rule 13a-15(d) or 15d-15(d), whichever applies.

The staff places limits on the period of time during which management may exclude the acquisition from the assessment of internal control over financial reporting. The period in which management may omit an assessment on a consolidated basis of an acquired entity's internal control over financial reporting may not extend beyond one year from the date of acquisition. Furthermore, an assessment may not be omitted from more than one annual management report on internal control over financial reporting.

Based on discussions with the SEC staff, the overriding principle they are using in applying their guidance is that management can exclude a newly acquired business from only one internal control report. Rather than the timing (12 months), the key is the sufficiency of the time available for management to evaluate the internal controls of the newly acquired business after closing the transaction. Therefore, a practical approach for applying this guidance is to view the close of the fiscal year as the benchmark for looking back one year. Management should apply its "best efforts" to integrate the internal controls of the newly acquired business into the current year Section 404 assessment. If that is not possible based on the facts and circumstances, including the size and complexity of the acquisition and the available time and resources, the internal control over financial reporting for the newly acquired division or unit can be excluded from the internal control assessment for that fiscal year, but not for the subsequent year.

With respect to reverse mergers (the acquisition of an operating company by an empty public shell corporation with the operating company being the surviving entity), the SEC staff has indicated these transactions generally do not qualify for an acquisition exclusion. The message is that the SEC's rules were not intended to apply to such transactions.

Note that the reporting company must have appropriate controls over the acquisition accounting in the year of acquisition. For example, the accounting and reporting must consider the determination of any acquisition-date contingencies, and the apportionment of the purchase price to tangible assets and liabilities, intangibles other than goodwill, and goodwill. While these matters are largely related to expertise in applying generally accepted accounting principles to acquisitions, they are, nonetheless, internal control considerations.

161. What is the impact of excluded acquisitions on management's executive certification under Section 302?

As discussed in Question 160, the SEC provides relief to issuers with respect to acquired entities of such size and complexity that it is impossible for management to complete an assessment of their internal control

over financial reporting during the period between the acquisition consummation date and the issuer's fiscal year-end. The question arises as to the impact of this Section 404 scope exclusion on management's executive certification responsibilities under Section 302.

Item 4, *Controls and Procedures*, in Form 10-Q should include disclosure that indicates the following (assuming the acquired entity is material):

- The acquisition was recently consummated during the current fiscal year.
- The company is taking a period of time to incorporate the acquired entity into its evaluation of internal control over financial reporting.
- Other than the above, management is not aware of any material change to the company's internal control over financial reporting.

Note that the SEC staff indicated in its guidance with respect to the exclusion that the issuer must disclose in its annual internal control report the acquired business excluded and the significance of the acquired business to the issuer's consolidated financial statements. Accordingly, we recommend that management consider disclosing in the Item 4 quarterly disclosures the relative size of the acquired entity to the issuer. We have seen examples of such disclosure when the relative size of the acquisition was material to the issuer and the issuer had issued an internal control report in the prior year.

We often receive questions with respect to management's disclosure responsibility if and when the company identifies any issues affecting the acquired entity's control environment that could mean exposure to a material misstatement, which in turn leads to a change that either materially affects or could potentially materially affect the issuer's internal control over financial reporting. In such instances, management would have an obligation to report these matters publicly – regardless of whether the acquired entity is "in scope" or "out of scope" during the year of acquisition. While the SEC allowed management more time to evaluate the internal controls of an acquired entity, the Commission did not allow issuers to blindly ignore material matters of which management is aware.

162. How does management apply the SEC's exclusion for material acquisitions when they occur early in the fiscal year?

Assume Company A, a calendar-year company, acquires Entity X in a transaction that closes on January 1, 2007. Assume further that Entity X is material to Company A's consolidated financial position and results of operations. This situation is particularly interesting, given that Company A is just one day shy of being required to include Entity X in scope during 2007. A literal read of the SEC exclusion suggests that management of Company A has the prerogative to exclude Entity X from the Section 404 compliance scope for the year ended December 31, 2007.

For all acquisitions occurring early in a fiscal year, we recommend that management consider two questions, before deciding to use the exclusion.

The first question is whether investors will raise questions regarding the length of time before the acquired entity is finally addressed from a Section 404 standpoint. This question suggests that management of Company A should consider the difficulty and cost of a "reasonable and best effort" to include Entity X in scope for 2007 Section 404 compliance purposes versus the potential message to investors with respect to not including it. For example, assume that Entity X is not a particularly complex operation or will be integrated rapidly into Company A's core processes. In such instances, management should consider carefully the option of including the acquisition in scope during 2007 and consult with the external auditors and audit committee.

We believe that the market appears to be accepting that an exclusion of a material acquisition is all about alleviating the burden of including the acquisition in scope during the year the transaction is consummated. Such burdens can be disruptive to an organization if the acquired entity is large and complex. For example,

when considering whether to take advantage of the SEC's exclusion, management should consider such factors as the following:

- The overall impact of the acquisition on the acquirer's control environment
- Whether the acquired entity is already Section 404 compliant
- Whether the acquisition is complex (e.g., does it involve many locations and legacy systems or include significantly different processes and controls than the acquirer's other operations)
- The existence of other business initiatives and directives that consume and limit available company resources
- The size of the acquired entity relative to the acquiring company's consolidated financial statements (For example, one company decided to include an acquired entity in the Section 404 compliance scope for the year of acquisition because that entity comprised 80 percent of the consolidated financial position and results of operations.)

The most important point to keep in mind is that the certifying officers should not sign the Section 404 opinion, inclusive of the acquired entity, until they are satisfied the available evidence enables them to do so.

The second question is whether there are merger integration plans which, if implemented, would taint an exemption. In other words, would an aggressive integration plan taint the exclusion by year-end if it eliminates the acquired company's processes by folding the required processing activities into the reporting entity's processes? Assume the acquired entity's period-end financial close process is eliminated and replaced with the reporting entity's period-end financial close process, such that the relevant control environment is the reporting entity's and not the acquired entity's. The question in such instances is whether the external auditor will accept the continued exclusion of the acquired entity's upstream business processes that "feed" the period-end financial reporting process. To illustrate, integration activities that might taint the exemption include merging of financial reporting systems or merging of nonstandard processes such as inventory management. On the other hand, integration activities that might not taint the exemption include (a) physically merging certain locations, (b) merging of certain standard processes such as payroll and (c) implementing changes to the authorization and approval policies of the acquired entity, or certain organizational reporting changes, to conform them to the policies of the reporting entity. The message is that, to avoid the tainting of the exclusion, the integration plans cannot place management and the external auditor in the position of having difficulty differentiating what is excluded from what isn't excluded.

Whatever is decided with respect to taking the exclusion, management should not forget their disclosure responsibilities. As explained in our responses to Questions 160 and 161, the Section 302 certification around disclosure controls and procedures and the disclosure of material changes to internal control over financial reporting applies to an acquired entity, effective immediately, in the quarter the acquisition is consummated. This would include a material weakness (from the vantage point of the reporting entity, or Company A in the illustrative example provided earlier) that is discovered at the acquired entity prior to completion of the review of the acquired entity's internal control structure.

163. How are divestitures of significant entities (or net assets) and discontinued operations considered for purposes of evaluating internal control over financial reporting?

The scope of the evaluation of internal control over financial reporting includes entities that were acquired on or before the date of management's assessment. This scope would include operations that are accounted for as discontinued operations on the date of management's assessment. To illustrate, assume a company divests itself of a subsidiary or a major facility and the divestiture is consummated outright as of the date of sale without any pending contingencies, and a gain or loss on the sale and all related liabilities, if any, are recorded at that time. In that case, there are no controls to evaluate because the company has divested itself of the subsidiary or facility and there are no operations, work out activities or controls in existence as of the year-end assessment date. However, if the sale is not consummated by year-end and the company retains rights and title to specific assets

and is obligated for related liabilities, the subsidiary or facility must be considered for purposes of inclusion within the scope of the Section 404 evaluation.

Discontinued operations are different from an outright sale or divestiture of facilities, entities or net assets. The expected loss is recorded as of the date of management's decision to discontinue and any expected operating losses through the date of final disposition are accrued. Any expected income from discontinued operations through the date of disposition are recorded in the period in which they are realized. The net assets are consolidated on a one-line basis on the balance sheet and the related operations are one-lined on the income statement to exclude them from continuing operations. Thus, discontinued operations accounting separates the operations of a discontinued location or unit from continuing operations so investors can evaluate separately the operations of continuing significance and understand the magnitude and impact of discontinued operations. There is also a significant amount of information that is required to account for discontinued operations. For example, there are estimates to be made to properly reflect the economics as of the date of management's decision to discontinue. Actuals are compared to estimates every quarter; differences are recorded and prior estimates are updated.

Discontinued operations, therefore, must be considered for purposes of determining the Section 404 project scope if the sale is not consummated as of the year-end assessment date. In these situations, management should evaluate the discontinued operations as a separate unit like all other locations and units in terms of their significance to consolidated operations. If significant, management should document the processes and controls in place to ensure that the discontinued operations are properly accounted for. The key factors driving the nature and extent of work to be done on the processes and controls related to discontinued operations include (a) the length of time it will take to execute management's plan of discontinuance, (b) whether the assets continue to operate as of year-end, and (c) the timing of the ultimate consummation of sale. If the sale were to close *before* the date of management's assessment, the discontinued operations need not be included within the scope of the Section 404 assessment. If the sale were to close *after* the assessment date, the discontinued operations would fall within the scope of the Section 404 assessment.

As discontinued operations often function until a willing buyer is found, the unit continues to generate revenues, costs and expenses, just like any unit that is part of continuing operations. Thus, there are controls in place related to these operations. On the other hand, if facilities are shut down and there are no operations, the focus of the controls is limited to the development of information needed to account for the gain or loss as of the decision date plus the accrual of related liabilities (e.g., severance costs).

164. What are some of the considerations with respect to an entity spun off from a Section 404 compliant company to form a standalone public company?

First and foremost, there is the question as to when the spun-off entity must first comply with Section 404. As discussed in Question 26, the Commission's rules provide all newly public companies, regardless of size, with a transition period that prevents them from having to comply with the Section 404 requirements in the first annual report that they file after becoming an Exchange Act reporting company. The transition period applies to a company that has become public through a registered exchange offer or that otherwise has become subject to the Exchange Act reporting requirements. Thus, a spun-off company need not comply with Section 404 until it files its second annual report.

For purposes of complying with Section 404, it would be a mistake to assume that the same scope and approach previously followed under the direction of the former parent would continue to apply now that the entity is a standalone company. The Section 404 scope needs to be reconsidered. Following are examples of matters requiring consideration:

- First and foremost, materiality needs to be reconsidered in view of the company no longer being a segment of a larger company. Often, there are surprising scope changes as changes in materiality are considered.
- If there are IT changes requiring special emphasis (e.g., system or data center conversions), the company's Section 404 compliance approach may be affected.

- As employees transition from parent company systems and processes, they may generally assume that processes and the control environment remain unchanged – as a result, they may neglect segregation of duties, effects of significant IT changes and the impact of changes in the decentralization or centralization of entity activities that can have scope implications.
- In circumstances where "support agreements" are in place, the spun-off entity continues to remain on the technical infrastructure of the parent while the entity's personnel work on establishing the entity's operations independent of the parent. These agreements can also impact Section 404 scope if they impact financial reporting, because such arrangements are similar in substance to outsourced processes. When such contracts exist, it is important that they be structured on an arms-length basis at inception and that they clarify the responsibilities and accountabilities between the former parent and the spun-off entity. See Question 86 for consideration relating to outsourced processes.
- The company may find that the external auditor will not rely on entity-level or monitoring controls, or the control environment, with respect to areas in which there are significant changes.
- If there are international locations, these may have been ignored in conjunction with the former parent company scope, as the focus may have been on centralized activities and one or two high-risk areas. Therefore, international locations may not have received much attention in the past. This can lead to the discovery of some significant problem areas.

One of the biggest challenges in a spin-off is overcoming the tendency to assume that the new entity will be strong in areas in which the former parent was strong and will have the same problems the former parent had. To illustrate, following are examples of matters requiring consideration:

- There is a risk of losing focus on the execution of critical controls. For example, as key employees assume different positions or undertake different activities in the new entity, a loss of focus on control ownership and accountability may result. Thus, employees who previously played a key role in Section 404 compliance can become so busy with the job of becoming a new public company (i.e., building infrastructure, refining processes, addressing governance matters, asserting finance leadership, etc.), they neglect to give sufficient attention to the necessary preparations for the compliance process.
- Entity-level controls, and the related documentation, must be evaluated carefully to consider the appropriate governance and legal requirements the new entity must now address as a standalone company. For example, the composition of the board of directors and its subcommittees must be considered. A human resources infrastructure, a code of ethics, a whistleblower hotline, among other things, may need to be established, because they were previously managed by the former parent.
- The financial reporting process must be refined to address public reporting and incorporate appropriate disclosure controls and procedures, as these processes and controls were previously managed by the parent.

As stated earlier, the good news is that a spun-off entity is considered a newly public company by the SEC.

165. How does a lag in reporting of the financial results by certain foreign subsidiaries for financial reporting purposes affect the assessment of internal control over financial reporting?

Many companies with global operations have a lag in reporting the financial results of certain foreign subsidiaries for financial reporting purposes. For example, the SEC staff used an example of a 30-day lag to illustrate the circumstances, i.e., an entity with a December 31 year-end may consolidate the operations of certain foreign subsidiaries reporting annual results for the period ended November 30 on a consistent basis year-to-year. The staff is of the view that this difference in period ends is also acceptable in relation to the assessment of internal control over financial reporting. Reporting lags are also common for certain investments accounted for on the equity method.

166. How are certain entities consolidated based on characteristics other than voting control, including certain variable interest entities and entities accounted for via proportionate consolidation, handled for purposes of determining the scope of the Section 404 assessment?

The SEC typically expects management's report on internal control over financial reporting to address the controls at *all* consolidated entities, irrespective of the basis for consolidation. However, there may be situations where an entity was in existence prior to December 15, 2003, and is consolidated by virtue of FASB Interpretation No. 46 (revised December 2003), *Consolidation of Variable Interest Entities: An Interpretation of ARB No. 51.* That interpretation in the authoritative literature requires that companies 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 these instances where the reporting company 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.

In these situations, the SEC staff is of the view that management should disclose the following, either in the internal control report or elsewhere in the body of the annual report:

- The company has not evaluated the internal controls of the entity (or entities) in question and the conclusion regarding the effectiveness of the registrant's internal control over financial reporting does not extend to the internal controls of the entity (or entities) in question.
- Total assets, net assets, revenues and net income that result from consolidation of the entity (or entities) whose internal controls have not been assessed.
- Management has been unable to assess the effectiveness of internal control at the entity (or entities) included in the consolidated financial statements due to the fact that the registrant does not have the ability to dictate or modify the controls of the entity (or entities) and does not have the ability, in practice, to assess those controls.

167. If controls are replaced or eliminated during the period before the end of the year, must the evaluation team test them?

No. If management implements changes prior to the end of the year to make controls more efficient and effective or to address control deficiencies, the superseded controls need not be tested. These superseded controls will not exist as of the end of the year and therefore are irrelevant. However, management should ensure the new controls are in place for a sufficient period of time to permit testing of operating effectiveness. See Questions 130 and 158 for discussion regarding a "sufficient period of time." In addition, the SEC requires public disclosure of any change in internal control that has materially affected, or is reasonably likely to materially affect, internal control over financial reporting.

168. Do the SEC's Executive Compensation Disclosure and Analysis rules fall within the scope of the Section 404 compliance process?

Section 404 would not be affected by these rules since they require disclosures outside of the financial statements. The scope of Section 404 compliance pertains to the financial statements only. Therefore, Section 404 is only relevant to these new disclosures insofar as the data required to prepare the Compensation Disclosure and Analysis (CD&A) is properly accounted for and disclosed in the financial statements. However, the new CD&A disclosures would fall under the scope of Section 302, because that section of Sarbanes-Oxley requires management to certify to the disclosure controls and procedures over all of the information included in periodic

reports – including information outside the financial statements. The SEC staff has noted that the company's proxy materials and other public disclosures also fall within the scope of Section 302. As companies comply with the new CD&A rules, this area will certainly attract the spotlight. For example, at the time this publication went to print, the SEC staff had sent letters to several hundred publicly traded companies in a broad cross section of industries requesting more information or clarification regarding their CD&A disclosures so that investors could better compare compensation practices of different companies. While it is apparent that the Commission seeks to increase the transparency of compensation practices by driving consistent application of its rules, we do not believe that these important disclosures fall specifically under Section 404 from the lender.

169. Is monitoring of debt compliance within the scope of Section 404 compliance?

Periodically, companies monitor whether they are in compliance with their positive and negative loan covenants. For example, they use information included in the annual financial statements to calculate various ratios and management submits a letter to the lenders confirming the company is in compliance. This annual loan compliance reporting process typically takes place several months after year-end and may include the need for a loan compliance letter from the external auditor to supplement management's compliance certification. If a condition of default exists, the condition is evaluated in terms of the specified grace period and the process of curing the default condition is closely monitored and the necessary waivers are obtained.

While the loan covenant reporting cycle itself probably would not fall within the scope of Section 404 compliance, the process of evaluating timely the effects of loan compliance can have an impact on balance sheet classification and the adequacy of financial disclosures. If loan compliance calculations are wrong, the financial statements and related disclosures may be wrong. Undisclosed noncompliance also could result in restated financial statements. If the financial statements are not fairly presented in accordance with generally accepted accounting principles as a result of incorrect loan compliance calculations or untimely monitoring of loan compliance, the external auditor may conclude that a material weakness or significant deficiency exists. Thus, it is important that issues arising from management's quarterly and annual monitoring of compliance be elevated in a timely manner to those responsible for financial reporting. The Section 404 compliance scope would ordinarily include the effectiveness of monitoring controls over the preliminary assessments and internal communications ensuring the fair presentation of disclosures in the financial statements regarding loan compliance matters, including any issues disclosed by management in fulfilling its periodic annual and quarterly reporting responsibilities to the trustee. These monitoring controls ensure reliability of financial reporting with respect to debt classification and related disclosures.

Reporting

170. How should management formulate conclusions with respect to internal control over financial reporting?

Now that the evaluations of the design and operational effectiveness of internal controls are complete, management is ready to develop an overall conclusion with respect to internal controls. This overall conclusion should consider:

- The body of evidence accumulated during the evaluation
- The results of the entity-level control assessment
- The results of the assessment of general IT controls
- The results of controls design evaluations at the process level
- The results of controls testing at the process level

- The results of monitoring activities and monitoring controls
- The identified control gaps, and the significance and pervasiveness of their impact on financial reporting
- The evidence of satisfactory resolution of the identified gaps
- Consultations with appropriate parties, including the disclosure committee, audit committee, outside experts (such as a "Section 404 Advisor") and the independent public accountant

Based on these considerations, management formulates its overall conclusions with respect to the effectiveness of internal control over financial reporting.

171. What should be communicated to executive management, project sponsors and the board?

One of the most important objectives of internal control reporting is to ensure the related reporting requirements of Section 302 are met. These matters are discussed in Question 204. In addition, as management formulates its overall conclusions, it will want to communicate with the audit committee. Another important point for the project team is continuous communication with project sponsors and executive management at key project milestones and checkpoints.

172. What is the internal control report?

Management must file an internal control report with its annual report, stating:

- Management's responsibilities to establish and maintain adequate internal control over financial reporting for the company
- The framework used by management as criteria for evaluating the effectiveness of internal control over financial reporting
- Management's conclusion on the effectiveness of the company's internal control over financial reporting at year-end (i.e., a point-in-time assessment), including disclosure of any material weakness in the company's internal control identified by management
- The company's independent public accountant who audited the financial statements included in the annual report also has attested to and reported on management's evaluation of internal control over financial reporting

The final rules provide a threshold for concluding that a company's internal control over financial reporting is effective by stating that management is not permitted to conclude that the company's internal control over financial reporting is effective if there are one or more material weaknesses in such internal controls.

The SEC requires that management state a direct conclusion about effectiveness. That said:

- The use of subjective phrases like "very effective" should be avoided.
- Negative assurance statements are not acceptable; e.g., "nothing came to management's attention to suggest that the company's internal control over financial reporting is not effective."
- Management is not permitted to conclude internal control over financial reporting is effective if there are one or more material weaknesses.

Management also may not qualify the internal control report. According to the SEC staff, management cannot make statements like "the company's controls and procedures are effective except to the extent that certain problems have been identified or express similar qualified conclusions." The staff points out that management must take those problems into account when concluding whether the company's internal control over financial reporting is effective.

173. When management identifies a control deficiency that is deemed to be a material weakness in internal control over financial reporting, must the company disclose the weakness in its public reports even though the weakness may be corrected prior to the end of the year? If so, when is this requirement effective?

Regulation S-K Item 308(c) requires companies to disclose any change (which would ordinarily include a change to correct a material weakness) in the company's internal control over financial reporting that occurred during the company's last fiscal quarter that has materially affected (or is reasonably likely to materially affect) the company's internal control over financial reporting. Regulation S-K Item 308(c) is currently effective and required by Form 10-Q. In the context of disclosing any such changes, a company may conclude that it is prudent to describe any material weaknesses (or potential material weaknesses) that gave rise to the change.

The SEC staff has noted that they 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 company's initial compliance with Section 404. However, the staff would not object if a registrant chose not to disclose changes made in preparation for the registrant's first management report on internal control over financial reporting. That said, consistent with the point of view expressed in the previous paragraph, the SEC staff reiterated that if a registrant has identified a material weakness, it should carefully consider whether that fact should be disclosed, including changes made in response to the material weakness.

After the issuance of the registrant's first management report on internal control over financial reporting, pursuant to Item 308 of Regulations S-K or S-B, the SEC staff points out that registrants are required to identify and disclose any material changes in its 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 is a common example) "if it materially affected the registrant's internal control over financial reporting."

174. If the Section 404 compliance team determines at year-end that there are control deficiencies deemed to be significant deficiencies in internal control over financial reporting, are there circumstances requiring public disclosure of these deficiencies in connection with the filing of the internal control report?

The SEC staff has pointed out that a registrant must identify and publicly disclose all material weaknesses. If management identifies a significant deficiency, it is not obligated to publicly disclose the existence or nature of the significant deficiency. However, the SEC staff has pointed out the following: If management identifies a significant deficiency that, when combined with other control 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 deficiency. Furthermore, 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.

175. What constitutes a change in internal control over financial reporting and how is materiality considered for purposes of evaluating the effects of such changes?

Changes in internal control over financial reporting generally fall into the following categories:

- Design and implementation of new or modified controls to address new risks or new accounting pronouncements
- Improvements of existing controls (see Question 176)
- Changes related to the acquisition of a business (see Questions 160, 161 and 162)

- Changes in the existing business which could affect the performance of established internal controls, e.g., turnover of key personnel responsible for financial reporting, corporate restructuring, installation of new IT systems, major modifications of existing IT systems, etc.
- Newly identified deficiencies in design or operating effectiveness, particularly if they constitute a material weakness
- Remediation of previously identified deficiencies, particularly if they are material weaknesses (see Question 177)

If any of the above changes occur, the question arises as to whether the change has a material effect on internal control over financial reporting and, therefore, warrants disclosure. While we recommend that companies consult with legal counsel on such questions, we have never seen an instance where an identified material weakness was not regarded as a change having a material effect on internal control over financial reporting.

In general, the goal of Sections 404 and 302 is transparency. As a rule, if companies aren't sure whether a change materially affects internal control over financial reporting, it is wise to err on the side of more disclosure rather than less disclosure and disclose the change. With respect to considering materiality, the SEC staff stated the following in guidance published as a response to a frequently asked question:

> 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 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.

In summary, information is material for disclosure purposes if it would have affected the manner of an investor's decision-making when he/she made an investment decision, i.e., the decision-making process. However, it is not necessary that the information would have caused the investor to change his/her decision, i.e., the substantive outcome.

176. Must management disclose improvements of internal controls?

An improvement of internal control over financial reporting is an enhancement to existing controls that were previously considered effective. With respect to such improvements, they must be disclosed if they have a material effect, or are reasonably likely to have a material effect, on internal control over financial reporting. The SEC staff has indicated the following in response to a frequently asked question:

- Generally they "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."
- The staff "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, 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 report and annual report. This disclosure "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."

177. Must management disclose the company's remediation efforts related to a material weakness?

Management may disclose the company's efforts to remediate the identified material weakness(es) in Item 9A of Form 10-K, Item 15 of Form 20-F, or General Instruction B of Form 40-F. In its guidance to management, the SEC states the following:

> Because of the significance of the disclosure requirements surrounding material weaknesses beyond specifically stating that the material weaknesses exist, companies should also consider including the following in their disclosures:
>
> - The nature of any material weaknesses,
> - Its impact on financial reporting and its [internal control over financial reporting], and
> - Management's current plans, if any, or actions already undertaken, for remediating the material weakness.

As the SEC states, "the goal underlying all disclosure in this area is to provide an investor with disclosure and analysis that goes beyond the mere existence of a material weakness." Therefore, some financial statement users have expressed a need to understand the status of management's remediation efforts concerning previously reported material weaknesses. This need has surfaced from the user community during the SEC roundtables on the Section 404 implementation process as well as in comment letters submitted to the SEC. In its interpretive guidance to management, the SEC recommends that "companies … consider providing disclosure that allows investors to understand the cause of the control deficiency and to assess the potential impact of each particular material weakness." This recommendation is driven by the point of view that not all material weaknesses are alike.

178. What are the form and content of the internal control report?

The rules do not specify the exact content of the annual internal control report, because the SEC is of the view that doing so would "result in boilerplate responses of little value." The SEC believes management should tailor the report to the company's circumstances.

179. Where is the internal control report included in Form 10-K?

Although the final rules do not specify where management's internal control report must appear in the company's annual report, the SEC indicated that the report should be in close proximity to the corresponding attestation report issued by the company's independent accountant. Generally, the SEC expects that many companies will choose to place the internal control report and attestation report near the MD&A disclosure or in a portion of the document immediately preceding the financial statements.

180. Can the results of the assessment of internal control over financial reporting affect the company's executive certifications under Sections 302 and 906?

There may be implications for requirements related to the executive certifications. For example, the assessment may identify significant deficiencies and material weaknesses in internal control that require disclosure to the auditor and audit committee in order to not render the certification under Section 302 inaccurate. These findings may arise during the assessment even though management may have sufficient time to remediate the deficiencies by year-end. The same is true with respect to any instances of fraud involving anyone who has a significant role in internal control over financial reporting. In addition, the company must disclose to investors any change in the company's internal control over financial reporting that occurred during the issuer's most recent fiscal quarter that has materially affected, or is reasonably likely to materially affect, the company's internal control over financial reporting.

181. What impact would a conclusion that the internal controls are ineffective have on the company?

A study released in May of 2006 by Lord & Benoit reported that shareholders benefit when companies have effective internal control over financial reporting. To illustrate, for the period from March 31, 2004 to March 31, 2006, the Russell 3000 share index increased by 17.7 percent. The Lord & Benoit study found that companies reporting no material weaknesses for either 2004 or 2005 enjoyed a 27.7 percent increase in share price. Companies reporting material weaknesses in 2004 but no material weaknesses in 2005 experienced a 25.7 percent increase in share price. However, companies reporting material weaknesses in both 2004 and 2005 suffered a 5.7 percent *decline* in share price. Therefore, the companies that reported that their internal control over financial reporting was ineffective both years experienced poorer performance in their stock price relative to the companies that did not.

182. What happens if there is a significant event affecting internal control over financial reporting following the end of the year but before the internal control report is released?

Whenever a significant change affecting internal control over financial reporting occurs after year-end but before including the financial statements with a filing with the SEC, management should first consider whether the change is material. For example, implementing a new ERP system to consolidate existing systems into one is likely to be a material change in internal control over financial reporting. Repairing a control deficiency that is a material weakness also is a material change.

If the change is material, management must determine whether it requires disclosure in the internal control report, the first quarter Form 10-Q or both. For example, if key personnel responsible for a critical area were to leave unexpectedly or critical data files were irretrievably lost due to a sudden catastrophic event, then management might conclude that the event constitutes a material adverse change in internal control over financial reporting, and require either modification or disclosure in the internal control report because it affects a condition existing as of the balance sheet date. Alternatively, management might decide a change involves an improvement in internal controls (e.g., implementation of a new system or remediation of a material weakness). Such changes may be ones that materially affect, or are reasonably likely to materially affect, internal control over financial reporting, and ordinarily require disclosure in conjunction with the first quarter Form 10-Q.

These matters should be discussed with the external auditor and audit committee.

183. What happens if a company completes its Section 404 assessment and files an unqualified internal control report, and subsequently restates its financial statements for the applicable period?

We will use the following scenario to address this question. Assume Company A, a calendar-year reporting company and an accelerated filer, has completed its Section 404 assessment for 2004, 2005 and 2006, and has filed its internal control reports for all three years with a conclusion that internal control over financial reporting is designed and operating effectively (i.e., there are no material weaknesses). The external auditor also issues in the attestation reports for each of the three years in the period ended December 31, 2006 an unqualified opinion that internal control over financial reporting is effective. Assume further that sometime during calendar year 2007, Company A issues restated financial statements affecting the reported results for 2005 and 2006. The restatement is attributable to a material weakness that existed during the 2005 and 2006 reporting periods but was not detected either by management or by the external auditor.

Several questions arise. For example:

- ***Will the SEC require management to reissue the 2005 and 2006 internal control reports?***

  When a material misstatement in previously issued financial statements is discovered and a company is required to restate those financial statements, the SEC's interpretive guidance states that "while there is no requirement for management to reassess or revise its [previous years'] conclusion[s] related to the effectiveness of [internal control over financial reporting], management should consider whether its original disclosures are

still appropriate." If the prior year disclosures are no longer appropriate, the Commission states that management "should modify or supplement its original disclosure to include any other material information that is necessary for such disclosures not to be misleading in light of the restatement."

In effect, an internal control report is similar to the financial statements in that it includes assertions, both expressed and implied, that are subject to change whenever there is a discovery of contrary evidence after its release to the public. The SEC states that a restatement of previously issued financial statements to reflect the correction of a misstatement is a situation that warrants an evaluation as to whether a material weakness in internal control over financial reporting exists. If the restatement is attributable to a material weakness existing during 2005 and 2006, Company A's management may have no choice but to reissue its assessment of internal control over financial reporting for those years because its original assessment may have been incorrect. Therefore, once management reports an error in previously reported financial statements and a determination is made that a material weakness existed during the prior period(s), the internal control reports indicating internal control over financial reporting as being effective as of the end of the respective reporting period(s) also may require reissuance to explain that internal control over financial reporting was not effective and, if appropriate, the material weaknesses have since been corrected. In addition, because a company is required to disclose any change in internal control over financial reporting that has materially affected, or is reasonably likely to materially affect, internal control over financial reporting, management likely would want to include appropriate disclosure in the next Section 302 executive certification regarding any changes made in response to the material weakness as part of its restatement.

To illustrate, one FORTUNE 50 company issued an unqualified internal control report for 2004 in its annual report on Form 10-K filed in March 2005. In May 2005, the company concluded that an issue with respect to the derivative accounting in a finance subsidiary required restatement of its consolidated financial statements for the previous four years. In addition, the company concluded that the issue constituted a material weakness. The company:

- Issued an 8-K reporting the matter and that the prior-year statements could not be relied upon
- Reissued an amended Form 10-K restating the prior four years and the prior four year quarters
- Issued a revised internal control report and audit opinion in the amended 2004 filing asserting that internal control over financial reporting was not effective due to the discovered material weakness

- ***Will the external auditor be required to reissue its 2005 and 2006 attestation reports on internal control over financial reporting?***

  Yes. As illustrated in the above example, the auditor reissues the audit opinion whenever there is a discovery of contrary evidence after the original opinion is released to the public. Once management's assessment has been revised, the auditor's attestation will obviously no longer be applicable and would likewise require revision.

- ***What position will the SEC take with respect to the various 302 certifications filed during the period(s) the material weaknesses existed? Will the Commission require them to be revisited or reissued?***

  As with the issues around reassessing previously issued internal control reports, the SEC's interpretive guidance also points to similar considerations with respect to the certifying officers' assertions regarding the effectiveness of disclosure controls and procedures in prior year executive certifications issued in accordance with Section 302. To restate its financial statements, Company A would need to file a Form 10-K/A. Rule 12b-15 requires the company to include new 302 and 906 certifications with the Form 10-K/A. In the above illustrative example, the FORTUNE 50 company did not revise prior-year Section 302 executive certifications. One possible explanation as to why the company did not issue revised certifications is that the restatement did not cause changes in the company's internal control over financial reporting in the prior periods. However, we are aware of circumstances where the SEC staff has required restatement of prior Section 302 executive certifications issued during the year because of a disclosure of the existence of material weaknesses at year-end. Because every situation is different, legal counsel should advise management according to the facts and circumstances in each case.

- ***In civil and/or criminal proceedings, will prosecutorial authorities (SEC, Department of Justice, etc.) take advantage of management's issuance of "false" (1) internal control reports for 2005 and 2006, and (2) 302 certifications during both years (and any other periods) a material weakness existed?***

  Obviously, this is a question for legal counsel. Whether criminal or civil liability will result from the false certifications depends on the circumstances under which the mistake arose, the extent of the mistake and various other factors. If, for example, a certifying officer willfully files a false 302 certification, it could subject the officer and/or the company to criminal liability. Willful violation of the Exchange Act is a felony that is punishable by fine and imprisonment. It also could be the subject of civil liability as the SEC could pursue a civil enforcement action against the officer, the company or both. A false 302 certification also may expose both the company and the certifying officer to criminal liability under a variety of other statutes.

  In terms of civil liability, the act of filing new 302 and 906 certifications creates additional factual predicates on which governmental authorities and/or private plaintiffs may premise complaints for false and misleading information. For example, it is common to see class action suits alleging defendant companies "lacked adequate internal controls and as a result, issued misleading financial statements, causing the stock price to be artificially inflated."

184. What documentation does management need to support the assertions in the internal control report?

During the Section 404 compliance process, much documentation occurs. For example, the Section 404 compliance team should document management's approach and the basis for management's decisions, including the processes, procedures and due diligence management completed in executing its responsibilities and supporting its conclusions. In addition, there should be sufficient documentation of the rationale and framework for identifying significant financial reporting elements, selecting key controls, determining multilocation scoping, setting testing scopes, and addressing exceptions. The compliance team's documentation also should indicate who is involved in making decisions and should maintain minutes and memoranda to record key decisions made. All of this documentation evidences management's assessment process.

As an illustration, the project documentation might include, among other things:

- From Set the Foundation and Phase I (see Question 57)
  - Analysis of financial reporting elements to select the priority elements;
  - Decomposition of the reporting entity into locations and units and business processes, and supporting analysis selecting the control units and the significant processes feeding the priority financial reporting elements;
  - Support for the assessment of entity-level controls;
  - Support for the assessment of general IT controls;
  - Support for the evaluation of the anti-fraud program and controls, including the specific controls designed to prevent or detect fraud, who performs them and the related segregation of duties; and
  - Process maps or equivalent documentation evidencing the period-end financial reporting process and identification of the points at which material misstatements due to error or fraud could occur.
- From Phase II (see Question 57)
  - Process maps or equivalent documentation evidencing how significant transactions are initiated, authorized, recorded, processed and reported, and identification of the points at which material misstatements due to error or fraud could occur;
  - Evidence of design of key controls over all relevant assertions related to all significant accounts and disclosures, including supporting rationale for selection of key controls;
  - Linkage of key controls to financial reporting assertions;

- Evidence the five components of COSO (including the control environment and entity-level controls) are addressed;
- Controls in place that address the identified risks of material misstatements due to error or fraud that could occur;
- Controls in place that safeguard assets;
- The results of management's evaluation of controls design effectiveness;
- Management's test plan; and
- The results of management's interim tests of controls operating effectiveness.

• From Phase III and IV (see Question 57)

- The results of management's evaluation of control deficiencies and communications of findings to the auditor and audit committee; and
- The results of management's retesting of remediated controls and refresh tests to update preliminary conclusions regarding controls operating effectiveness.

While not necessarily all-inclusive, this list illustrates the substantial amount of documentation developed during the Section 404 compliance process.

In addition, the documentation should evidence testing of the following controls:

- Entity-level controls, including the control environment, controls over the period-end financial reporting process and monitoring controls that function at the process, transaction and application level
- Process-level controls over initiating, authorizing, recording, processing and reporting significant accounts and disclosures and related assertions inherent in financial reporting (including application controls embedded within the critical processes)
- Controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles
- Anti-fraud programs and controls (i.e., controls related to the prevention and detection of fraud)
- Controls, including general IT controls, on which other controls are dependent
- Controls over significant nonroutine transactions
- Controls over significant estimation transactions

The compliance team's controls design documentation also must address these controls.

We recommend that an overall high-level document be prepared to evidence management's assessment process. The SEC's interpretive guidance provides the following example:

> [M]anagement may document its overall strategy in a comprehensive memorandum that establishes the evaluation approach, the evaluation procedures, the basis for management's conclusions about the effectiveness of controls related to the financial reporting elements and the entity-level and other pervasive elements that are important to management's assessment of [internal control over financial reporting]. If management determines the evidential matter within the company's books and records is sufficient to provide reasonable support for its assessment, it may determine that it is not necessary to separately maintain copies of the evidence it evaluates.

This memorandum should describe the steps of the process and refer to the project documents and work products. Examples of the project documents and work products may be attached to the overall memorandum as exhibits. The memorandum should describe the results of the design effectiveness work and the control testing work, including the identification and disposition of control deficiencies. The high-level memorandum also should be global in focus. For example, it might list by process the number of key controls, the number of

controls deemed "effective" and "ineffective" based on the initial testing, the number of "ineffective" controls remediated and retested, the number of controls for which a preliminary conclusion was reached requiring refresh testing, the controls for which refresh testing is completed, and the final conclusions.

The overall memorandum should accomplish four very important objectives:

- First, it should support the assertion to be included in the internal control report.
- Second, the certifying officers need some overall documentation to enable them to walk through the work done. Wading through the details is not the most effective way to help these senior executives gain confidence that the work done is complete and responsive to the requirements.
- Third, the memorandum can serve as a tool for providing transparency to the auditors and the audit committee as to management's assessment process.
- Finally, it should assist the auditor in leveraging management's assessment process and controls documentation in using the work of others.

185. How long must management retain the documentation supporting the assertions in the internal control report?

Although the instructions to Regulation S-K, Item 308, require a company to "maintain evidential matter, including documentation, to provide reasonable support for management's assessment of the effectiveness of the [company's] internal control over financial reporting," the instructions do not prescribe a minimum time period. The Sarbanes-Oxley Act and the rules issued by the SEC require the independent auditors to maintain, for seven years after the conclusion of the audit, all "records relevant to the audit or review, including workpapers and other documents that form the basis of the audit or review, and memoranda, correspondence, communications, other documents, and records (including electronic records), which (1) are created, sent or received in connection with the audit or review, and (2) contain conclusions, opinions, analyses, or financial data related to the audit or review."

It would stand to reason that comparable documents prepared by the company could be deemed relevant to any future investigation into the company's audit processes and, therefore, should be retained by the company for seven years as well. For example, company documentation might include, among other things: the selection of significant financial reporting elements and the critical processes affecting those elements; the documentation of risks and key controls supporting the assessment of controls design effectiveness; and the nature, timing and extent of tests of controls operation, as articulated in the test plan, and management's execution of the test plan, as evidenced in the "working papers" (e.g., the testing working papers, the technology tool documentation, etc.). In addition, pursuant to Rule 12b-11(d) under the Exchange Act, a company must keep all manually signed documents filed with or furnished to the SEC (including the certifications) for five years.

Needless to say, this question is one requiring input from legal counsel. Given the tenor of the times, no retention policy should be adopted and no steps should be taken without consulting counsel.

Another area related to the question of documentation retention deals specifically with the retention of documents and documentation by process owners to facilitate reperformance testing by auditors. We believe that the duration of retaining that type of documentation need not be as long as the working papers and related documentation described above once the auditor's tests are completed. We are aware of one company adopting a sufficient period of time to cover the certification period and the outside auditor review period as well as provide a period of time as a sufficient "cushion." The breadth of Section 404 (including the number of controls evaluated) and the number of systems involved make this kind of retention period for "second level" documentation a challenge. Because of the impact of auditor efficiency and sign-off, and the fact that there may not be a compelling business need to retain this evidential matter for long periods of time, the external auditor's expectations will probably be the driver of practice with respect to this level of documentation.

In some industries, there are laws and regulations that require retention of specific documents. These laws and regulations also must be considered when evaluating the company's documentation retention policy. Again, legal counsel needs to weigh in on the document retention issue. The general counsel also should be involved in addressing these questions.

Moving Beyond the Initial Year Assessment

186. Why should certifying officers care about the Sarbanes-Oxley Section 404 compliance structure going forward after the first internal control report is filed?

CEOs and CFOs are required – on a quarterly basis – to represent three things:

(1) They are responsible for establishing and maintaining internal control over financial reporting.

(2) They have designed internal control over financial reporting, or caused such internal control over financial reporting to be designed under their supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles.

(3) They have disclosed any change that has materially affected, or is reasonably likely to materially affect, internal control over financial reporting.

Thus, the certifying officers have two concerns with respect to Section 404. First, they need assurance that the controls design remains effective. Second, they don't want a material weakness to emerge. As a result, CEOs and CFOs should continue to closely monitor developments regarding internal control over financial reporting on a periodic basis.

187. What are the elements of an effective Sarbanes-Oxley Section 404 compliance structure after the initial annual assessment is completed?

Certifying officers should take the following steps in preparing their organizations for moving beyond the initial year of Section 404 compliance:

- ***Pay attention to "tone at the top."*** It starts with your personal involvement and commitment. Overtly support a strong control environment through, among other things, the code of conduct, audit committee oversight, an effective process for handling confidential and anonymous complaints, clear policies for assigning authority and responsibility, effective human resource policies and practices, and an organizational structure and management style that is conducive to an open and transparent internal control environment. Speak out about ethics, internal control and personal integrity in company meetings. Let the organization know ethical violations will not be tolerated.
- ***Reinforce responsibility and accountability through establishment of a self-assessment process.*** If you already have a self-assessment process, make sure it is effective and is linked to specific business processes and your key controls. If you don't have a self-assessment process, design one and conduct it periodically. Provide guidance to your process owners as to what is expected of them in supporting the assessments they submit. Let them know internal audit will periodically review the basis for their assessments. Engage your operating unit managers by making them privy to self-assessment results and request their participation when following up on matters requiring remediation.
- ***Implement a change-recognition process.*** When certifying officers have confidence that disclosure controls and internal control over financial reporting are functioning as intended, and processes are improved as necessary when changes occur in the business, they will be able to focus on the disclosure implications of change. This is where their focus should be. A formal change-recognition process is needed to identify emerging risks, issues and developments in a timely manner for action and disclosure on a quarterly basis.

- ***Maintain a Sarbanes-Oxley PMO or steering committee.*** Continue to view Section 404 compliance as a major effort requiring sufficient resources and project management discipline to hold the appropriate personnel accountable, complete all project tasks in a timely manner, and bring the project to successful completion on time and on budget.
- ***Consider establishing a risk control specialists group to support process owners with remediation, design changes and documentation updates during times of change and to perform testing of operating effectiveness.*** Decide whether to (1) embed the risk control specialists within operations, or (2) establish an independent risk control function either reporting to a C-suite executive or housed within the internal audit department.
- ***Define the ongoing Sarbanes-Oxley role of the internal audit department.*** Focus internal audit's role on evaluating management's assessment process, performing testing in selected areas and reporting results. Define the function's role consistent with its other responsibilities (e.g., conduct operational and compliance audits in critical risk areas), its capabilities and its available capacity.
- ***Formalize a reporting and elevation process that will support management's continuing responsibilities under Section 302 and initiate timely remediation of significant deficiencies.*** Management must disclose significant deficiencies and material weaknesses to the audit committee and external auditors on a timely basis. Management also must make sure a process is in place to report and elevate significant deficiencies and potentially significant deficiencies to the disclosure committee and to other designated management as soon as practicable.
- ***Understand who is taking charge of identifying and controlling the unique risks introduced by IT.*** Don't underestimate the importance of managing IT-related risks. The complexity of technology makes these risks more critical. Confirm that the chief information officer is engaged continuously in the process of evaluating internal control over financial reporting. Also, be sure your software solution for managing compliance satisfies your needs going forward.
- ***Insist on getting value from your first-year investment.*** Once the first internal control report is filed, ask your people to mine the value of the increased transparency into your business processes that the Section 404 compliance documentation provides. Look for opportunities to improve the quality of the internal control structure and the upstream business processes. If you don't get results, your people aren't looking hard enough.

"Life after the first year" cannot begin until the aforementioned steps are taken to lay a strong foundation for ongoing compliance. Because they necessitate advance preparation in the first year, some companies have already begun to focus on these steps to ensure that the investments they are currently making will pay off in the future.

188. How are the process owners engaged going forward?

Process owners should be held accountable for the effective functioning of internal controls for which they are responsible. Through an effective self-assessment process, accountability is reinforced by requiring process owners to respond to questions regarding specific controls for which they are responsible, creating a transparent "chain of accountability" for internal control over financial reporting. The Section 404 compliance process lays the foundation for an effective self-assessment process by providing insights as to the key controls and the owners of those controls.

The SEC has taken the position that entity-level controls include "controls to monitor other controls, including … self-assessment programs." Because "process owners" are the men and women closest to the critical control points within the organization, they are best positioned to know what's working and what isn't, when changes are occurring in the process, and the impact of systems and other pervasive changes on the controls within the process. Process owners both execute controls and supervise and monitor the owners of controls, and ultimately are responsible for assessing the design and the performance of controls.

What does this mean to certifying officers? If you don't have a self-assessment process, implement one. If you have a self-assessment process already in place, improve it. Make it more robust by linking it to the key controls

identified by the Section 404 compliance process and including it as an integral part of the disclosure process and continuous monitoring required by Section 302 reporting. *Look at self-assessment as a management tool that drives the "tone at the top" down to the process owners.*

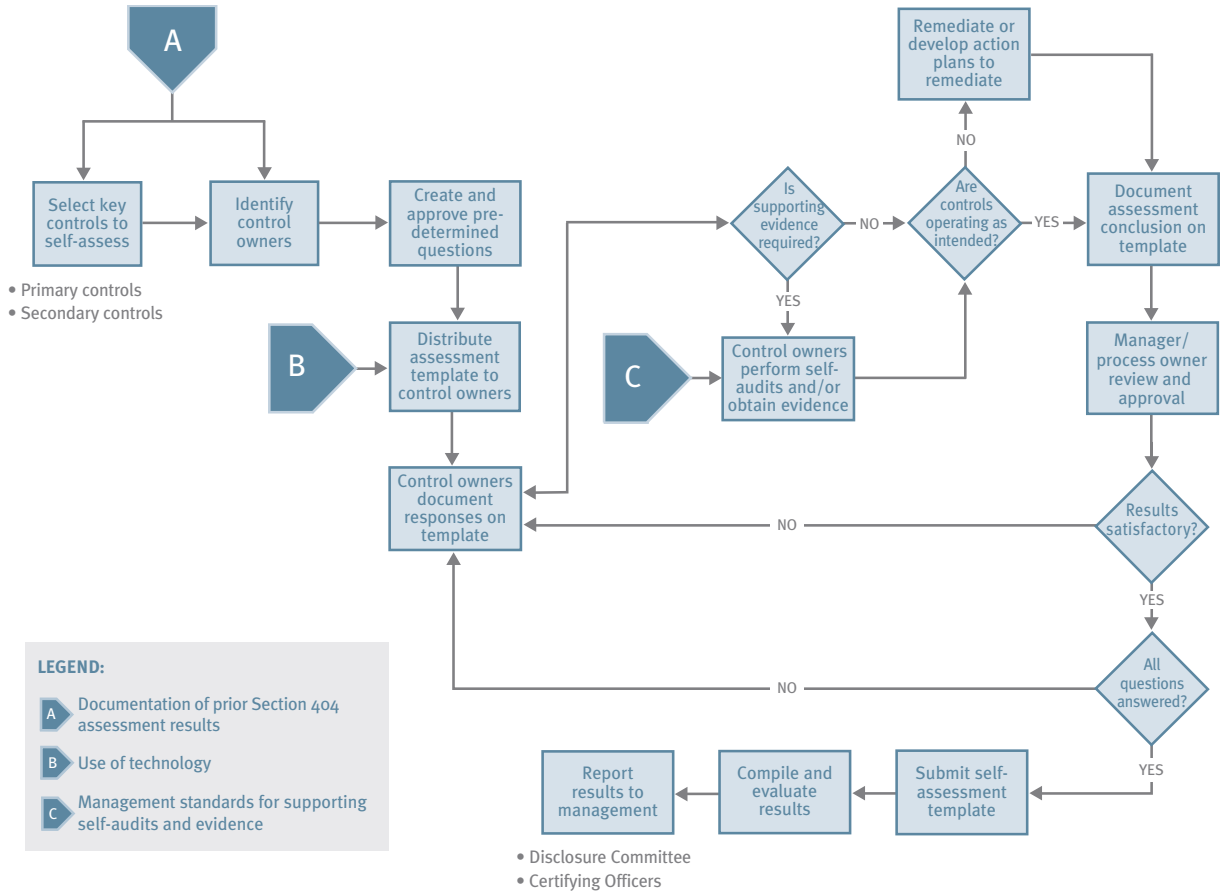
189. How does a self-assessment program work going forward?

The self-assessment process involves several key components:

- The key controls have been identified.
- The owners of those controls are known.
- Predetermined questions are approved by management.
- The process involves rigorous deployment of questions and follow-up with owners.
- The process may be applied at the entity and process levels.
- Self-assessment results are communicated to management.
- Exceptions and open matters are resolved in a timely manner.

Process and control owners often use inquiry, observation and inspection techniques as they supervise and monitor the activities for which they are responsible to assess whether the controls are functioning properly. They also may use reports to evaluate the effectiveness of the process, e.g., accounts receivable items in suspense reports and aging of items in suspense provide an indication as to the effectiveness of the processing of billings, cash collections and adjustments. These activities provide the basis for periodic self-assessments. They may be augmented by additional self-audits by the process owners as prescribed by the self-assessment process.

Self-assessment involves the following steps:



The effectiveness of self-assessment is evaluated in terms of two things: the quality and reliability of the assurances the process provides to certifying officers and the identification of issues for timely follow-up and necessary remediation. For example, self-assessments performed by personnel responsible for operating the control generally provide less evidence due to the evaluator's lower degree of objectivity. Self-assessments performed by members of management or process owners who are not responsible for operating the control generally provide more reliable evidence. In addition, internal audit can test selected controls to evaluate the quality of self-assessment results.

The above approach is not to be confused with the "backup certifications" often required to support the quarterly executive certifications. The above approach is process-based, where backup certifications merely mirror the executive certification representations and do not necessarily provide assurance that better information will be furnished to management for timely action and disclosure. Rather than a "chain of certifications," the above approach creates a "chain of accountability" arising from the clear linkage to the key controls on which management relies for purposes of Section 404 compliance.

While self-assessments can be performed for the primary and critical controls, they cannot be relied upon as the *sole evidence* supporting management's conclusions on higher risk areas regarding internal control over financial reporting. Therefore, self-assessment may complement other testing approaches to provide certifying officers assurance that the key controls are operating effectively as of a point in time (e.g., at year-end or quarter-end) for higher risk areas. There also is the question of objectivity when designing self-assessment programs. This question is discussed in our response to Question 144.

190. Why do process owners need support going forward?

Companies are investing many hours of effort in the first year and incurring significant costs. Going forward, it is unrealistic to expect the process owners to shoulder the burden of Section 404 compliance by themselves. If there are significant changes, it is inconceivable how they will get the job done without some support. It is imperative, therefore, that companies protect their initial-year investment by supporting process owners and ensuring ongoing compliance.

Management also must maintain up-to-date compliance documentation. The good news is that the documentation arising from the prior year may be rolled forward if there are no changes in policies, processes, people and systems. That said, who will keep this documentation up to date going forward? Who will assess the impact of changes in processes and systems, redesign controls in response to change and update the related controls documentation for changes made? Who will remediate deficiencies when necessary? Do process owners know how to do these things? Who will coach, assist and evaluate them? An appropriate organizational structure that facilitates compliance must provide answers to these questions, because process owners are neither auditors nor experts in documentation and remediation. They need help and support going forward after Year One.

191. What are alternative structures for supporting process owners in complying with Sarbanes-Oxley Section 404 after the initial annual assessment?

The matter of organizational structure is important. For purposes of ongoing compliance with Section 404, there are at least two important aspects affecting structure. The first is the issue of managing gaps and overlaps. The second is establishing the appropriate transitional organizational structure.

Managing Gaps and Overlaps

An organizational structure that drives effective internal control over financial reporting is predicated on a sharp delineation of roles and responsibilities. The question of "ownership" is oftentimes obscured by the "command and control" hierarchy of most organizations because that structure has always placed strong emphasis on managing silos. For example, the "procure to pay" process is executed by the purchasing, receiving, accounts payable and treasury (cash disbursements) functions. Not only do these functions operate at different levels of the organization, there are critical interfaces or "touch points" among these functions that make the "procure to pay"

process work. There must be effective controls over these interfaces, as well as owners of these controls who are accountable for their effective operation.

Certifying officers can benefit from clarifying accountability at all levels and for all key financial reporting processes within the organization. While Section 404 compliance should drive this definition, the ultimate litmus test occurs when management deploys a self-assessment process. To make self-assessment happen in a Section 404 compliance environment, every key control must have a name by it. Gaps (such as when there is no one responsible for executing a control) should be eliminated and overlaps (such as when there are too many multiple owners of a control) minimized. This kind of clarity is not easy to achieve. Therefore, many companies face situations in which process ownership must be clarified, particularly at the interface points within processes.

Because Section 404 compliance demands attention to execution, it is important to understand that the process ownership aspects of identifying processes and the controls within processes is a significant change management issue. The exercise of assigning accountability for results can result in redrawing the scope of control responsibilities that previously existed for specific individuals. Thus, it is critical that companies consider carefully the transitional organizational structure following the first year of compliance to facilitate process owner understanding and acceptance of the scope of their respective responsibilities. Such responsibilities include appropriately testing and self-assessing internal controls to provide assurance that they are operating effectively as designed. Desirably, process owners should be accountable for the effectiveness of process design, empowered to make decisions affecting the process and responsible for monitoring process performance.

Establish the Appropriate Transitional Organizational Structure

Certifying officers need an organizational structure that facilitates ongoing compliance with Sarbanes-Oxley Sections 302 and 404. This structure should emphasize the internal audit function, a group of risk control specialists or both. For example, assume an organization contemplates a lot of changes, and the skill sets, capacity and charter of the internal audit function are not conducive to providing the assistance that process owners need with respect to documenting controls, evaluating change, assessing controls design, testing controls operation and remediation. In such instances, certifying officers should consider creating a risk control function or engaging risk control specialists. A risk control group does not execute processes and controls. It may report to and be embedded within the entity's operations. Alternatively, it may be independent of operations, reporting to the chief financial officer, the chief compliance officer or the chief risk officer. In fact, the change management aspects of eliminating gaps and minimizing overlaps suggest a need for risk control specialists to support process owners over a sufficient period of time as they assume responsibility for the ongoing operation of specific controls after the initial year internal control report is filed. Another factor management may choose to consider is the impact on the appearance of objectivity of the internal audit function. The appearance of objectivity is enhanced when internal audit has a direct line of reporting to the audit committee.

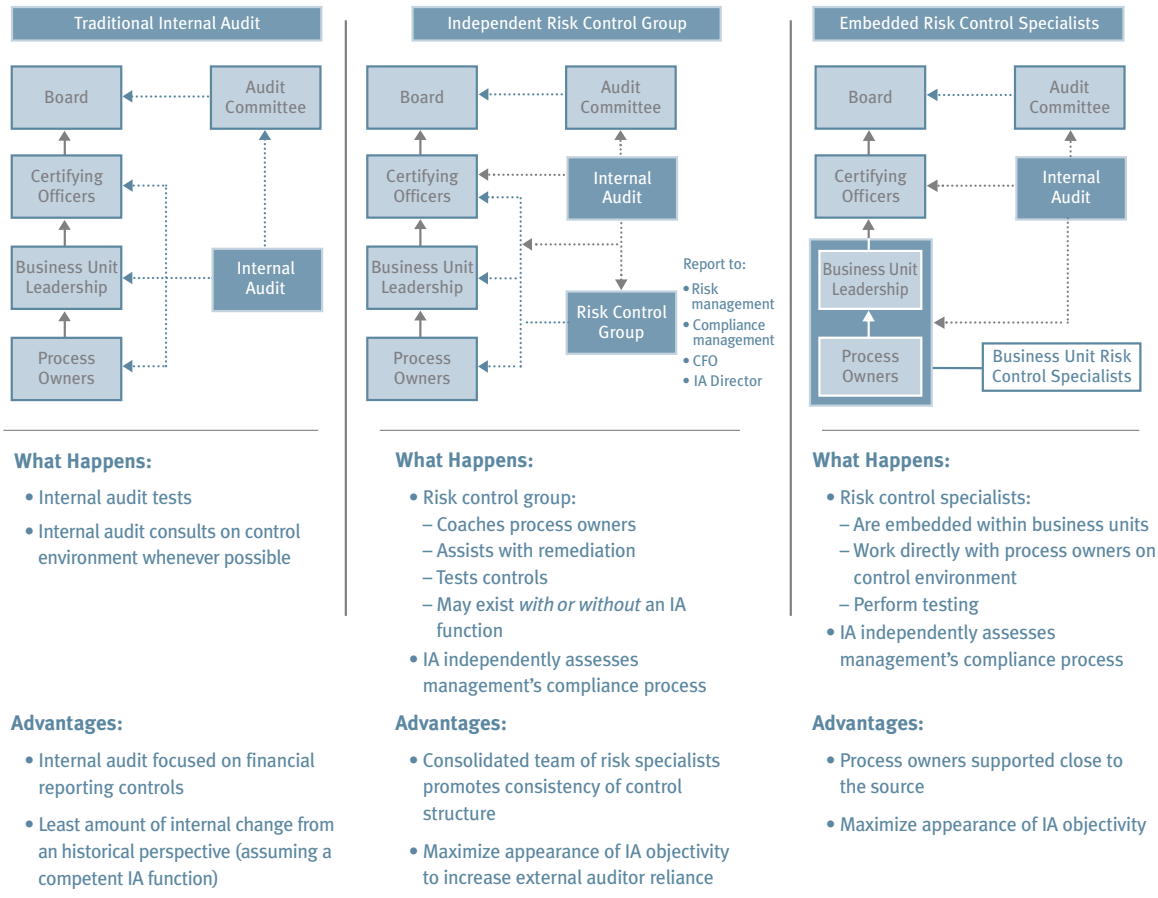
If not much change is contemplated and internal audit has the requisite process, risk and control skill sets, as well as the available capacity, the function may be deployed (and, if necessary, expanded) and its charter aligned to provide process owners the assistance they need in lieu of deploying a separate risk control group. If it is desired to deploy risk control specialists, such specialists may be organized as a separate division within the internal audit function, reporting to the chief audit executive, or integrated across the organization. In any event, the internal audit function should align its audit plan with whatever Sarbanes-Oxley compliance-related monitoring role management has designated for it to fulfill.

Whether embedded or independent, whether reporting to a C-level executive or whether housed within internal audit, risk control specialists play a vital role. Through their knowledge of risk, Sarbanes-Oxley requirements and business processes, they ensure consistent compliance enterprisewide and evaluate the risk at critical interface points between business functions. They infuse process innovations on a periodic basis. They facilitate the identification of metrics that will drive efficiency and effectiveness. In specialty areas like technology, supply chain, commodity trading and treasury, they have access to organizations with which they may co-source personnel with expertise that is not deployed daily in most organizations. Most importantly,

they give the process owners assistance from someone they respect, which is vital in the early transitional stage as process owners assume new and expanded responsibilities for controls and compliance.

In summary, we suggest three organizational structures that facilitate ongoing compliance with Sections 404 and 302:

Alternative Sarbanes-Oxley Compliance Structures



There are several factors certifying officers should consider as they evaluate the appropriate transitional organizational structure going forward. Following are five:

(1) The need to clarify roles and responsibilities of, among others, process owners, operating unit managers and, depending on the selected structure, internal auditors and risk control specialists. As noted earlier, clarity of roles and responsibilities is essential to achieve accountability for results.

(2) As the underlying business processes are simplified, focused and automated, there will be greater emphasis on preventive controls (versus detective controls), systems-based controls (versus manual controls) and monitoring. The state of maturity of the company's processes (meaning the extent to which they are defined and managed) will drive the nature of the skills needed. For example, business processes that rely heavily on automated controls will require less testing. However, testing in these environments demands more emphasis on technology-related skills that are not required with respect to processes that rely on manual controls. What's the point? The more efficient and effective the organization's processes, the more they will depend on preventive and automated controls. Consequently, less testing will be necessary and compliance costs will decline over time.

(3) The extent of change expected within the industry should be considered, e.g., regulatory, consolidation and other developments. The more change, the more help process owners will need.

(4) A highly competent and objective risk control group (either within internal audit or separate) and a strong internal audit department are functions whose work the external auditor can rely on to a greater extent than on work performed by others within the company. Going forward, this is an important factor as companies look for ways to reduce net audit costs while maintaining audit effectiveness.

(5) The choice of using internal audit and risk control specialist(s) to advise and coach process owners and perform testing is based upon:

- The assigned role and responsibilities of process owners
- The capabilities of process owners
- The capacity and cost of deploying process owners
- The capabilities, capacity and cost of deploying internal audit

If the needs of the organization require expansion of these skill sets, hiring all of the necessary skills may be expensive, particularly in areas of specialized skills such as IT. Therefore, co-sourcing may provide an attractive option to management.

Following is an illustrative summary of the components of infrastructure for ongoing compliance along with examples of illustrative questions when defining the components of infrastructure needed:

Examples of Components of Infrastructure for Ongoing Compliance (Not Intended to Be All-Inclusive)

Examples of Illustrative Questions When Defining the Components of Infrastructure Needed (Not Intended to be All-Inclusive)

Is there a self-assessment process and is it effective?	• How do you know? • How far down the organization? • Is it continuous, quarterly or ad hoc? • Who performs the assessments? • To whom are results reported?
Are process owners required to support their assessments?	• If so, what guidance is provided? • Are managers/process owners involved to increase objectivity?
Are there constraints in deploying process owners and/or internal audit?	• What are their capabilities? • What is their capacity? • What infrastructure needs to be in place to support the effort? • What is the cost?
What is the evolving role of the internal audit function with respect to Sarbanes-Oxley compliance?	• What is the organization's view with respect to preserving the appearance of objectivity? • If separate risk control specialists group, what is role of internal audit?
Are risk control specialists needed to assist process owners with testing and other activities?	• If so, where should they be positioned within the organization? • How do you staff and measure performance?

In summary, after the first-year Section 404 assessment is completed, certifying officers face three realities. First, if there is a significant breakdown in internal control over financial reporting, the company could receive an adverse opinion from the auditor on its internal control. Second, the entity's process owners have a business to run and, due to the day-to-day demands of executing the processes of the business, will be unable to carry the entire compliance load during periods of significant change. Third, there are change management issues that reinforce the need to support process owners, at least on a transitional basis over a period of time following the first year of compliance. Certifying officers need an effective organizational structure that provides them with confidence that what is supposed to be done with respect to ongoing Sections 302 and 404 compliance is, in fact, being done and reduces the risk of personal exposure going forward.

192. How does the maturity of a company's business processes affect the sustainability of its internal control structure?

Many companies have work to do with respect to improving their underlying business and accounting processes so they are sound and sustainable. Going forward, external auditors may press hard for process improvements that will lead to a more sustainable internal control structure during times of change. Continued reliance by management on ad hoc, manual processes will be challenged, particularly in environments involving a significant volume of transactions.

The stakes are high in ensuring there are no material weaknesses because if there is just one, management must assert that internal control over financial reporting is ineffective and the external auditor must issue an adverse opinion. Unfortunately, many material weaknesses do not get reported to management until it is too late to fix them. In many instances management didn't know they existed. This is often due to the lack of maturity of the company's processes. See Question 104 for discussion of the capability maturity model.

Control deficiencies arising from ad hoc processes are often rooted in an overemphasis on manual and detective controls. This captures the essence of what we see in the control deficiencies noted in SEC filings. Companies are reporting material weaknesses (and, in some instances, even significant deficiencies) in internal control over financial reporting, are providing updates on the status of their control-improvement efforts and are disclosing risk factors related to uncertainties in the internal control structure. See Question 238 for further discussion of examples of material weaknesses disclosed.

These dynamics suggest a need for companies to evaluate their key business processes not only to assess control design effectiveness but also to assess process maturity as a measure of sustainability. Companies should not stand pat with their existing processes just because they passed the Section 404 assessment test in the initial years of compliance. If processes are heavily dependent on manual and detective controls and on human intervention, the company's internal control structure may not be sustainable during periods of change. Management should target such processes strategically for improvement and for increased scrutiny by internal audit or risk control specialists. While we see many companies remediating their control deficiencies with short-term solutions, we also see them planning for longer-term improvement in key processes that support financial reporting.

193. How do companies "find the value" from Section 404 going forward?

With respect to Section 404 compliance, certifying officers should ask for value returned just like they do for any other investment or expenditure. Sections 302 and 404 provide the "launching pad" to improve the quality of both upstream business processes and the internal control structure and enhance entity-level monitoring of the financial reporting process. Sarbanes-Oxley compels public companies to assess weaknesses in their business processes, including their controls over processing information. Because the financial reporting processes for many companies are dependent on people and detective controls, and are sometimes inadequately defined, there are potentially strong sources of value extending beyond compliance. For example, there is a significant opportunity to "build in" (versus "inspect in") quality, compress time and reduce costs within the organization's processes while simultaneously reducing its financial reporting risks to an acceptable level.

With improved financial reporting, companies also can augment the governance process by managing reputation and other business risks to protect and enhance enterprise value. Companies with documented processes can compare and benchmark their processes to improve efficiency; articulate clearer job descriptions; better train their people; design improved metrics; eliminate nonessentials; and simplify, focus and automate manual activities. Finally, the reduced risk of material weaknesses results in a corresponding reduced risk of a drag on stock price performance (see Question 181).

194. After the initial annual assessment, how does management conduct the quarterly evaluations of those elements of internal control over financial reporting that are a subset of disclosure controls and procedures?

The SEC's final Section 404 rules state that a quarterly evaluation of internal control over financial reporting is not required. However, the rules in place starting in August 2002 requiring quarterly evaluations of disclosure controls and procedures and disclosure of the certifying officers' conclusion regarding the effectiveness of those controls and procedures have not been substantively changed since their adoption. In the final Section 404 rules, the SEC states that "these evaluation and disclosure requirements will continue to apply to disclosure controls and procedures, including the elements of internal control over financial reporting that are subsumed within disclosure controls and procedures."

How should management review these elements of internal control over financial reporting on a quarterly basis? The key controls identified during the initial annual assessment provide the basis for conducting quarterly evaluations going forward. Web-based technology can support monitoring of self-assessments by process owners who report as of quarter-end to unit managers. The unit managers, in turn, report to top management (the certifying officers) or to the disclosure committee. Any exceptions are reported to the officer designated with the responsibility to resolve such exceptions.

In summary, here is what happens:

- The initial Section 404 assessment documents the key controls by process owner.
- Management must identify those elements of internal control over financial reporting that are subsumed by disclosure controls and procedures. See Questions 37 and 38.
- Management must evaluate changes in the internal control over financial reporting on a quarterly basis in the years following the initial annual assessment, including those controls that are an integral part of disclosure controls and procedures.
- Technology provides the foundation for ongoing process-owner self-assessments of control operational effectiveness at any point in time. Customized questions are developed for use in the self-assessment process based upon input of the key controls identified during the initial annual assessment. See Question 189.
- With process owner feedback every quarter, management (i.e., the certifying officers) will be positioned to focus on the need for disclosure as a result of change, e.g., changes in processes, systems, operations and other factors, and their impact upon the effectiveness of internal control.

Because the initial annual assessment is process-based, the upward reporting by process owners will truly be a "chain of accountability" that will contrast with the "chain of certifications" created by many companies requiring their direct reports to individually certify results. In practice, those direct reports have, in turn, often required the same of their direct reports, and so on. The chain of certifications approach, often referred to as "backup certifications," may engage process owners, but it does not necessarily provide assurance that better information will be furnished to management for timely action and disclosure. The chain of accountability arising from the linkage of the key controls on which management relies for purposes of Section 404 compliance to the ongoing quarterly evaluations is a superior process-based approach. In this way, Section 404 compliance enables a more effective evaluation of disclosure controls and procedures.

195. After the initial annual review of control effectiveness is completed, should management assess changes to the company's risk profile on a quarterly basis?

Yes. An enterprisewide risk assessment process will help keep the disclosure process fresh. It will identify changes in factors affecting internal controls as well as new and emerging risks for timely action and disclosure. The company also must disclose any change in its internal control over financial reporting that occurred during its most recent fiscal quarter that has materially affected, or is reasonably likely to materially affect, the effectiveness of the company's internal control over financial reporting.

Because of the impact on financial reporting risk, every company needs a process for identifying environment, operating and other changes that impact the financial statements, other disclosures in public reports and the effectiveness of internal control over financial reporting. Examples of changes requiring evaluation include mergers and acquisitions, divestitures, new innovative business practices, new systems, changes in personnel (including significant early retirement or personnel reduction programs), significant market declines and changes in laws and regulations. The disclosure committee, or an equivalent group of executives, should be charged with the responsibility of monitoring change for purposes of identifying material information requiring consideration and possible disclosure. Operational risks, new related-party transactions, new litigation and other contingencies, emerging strategic risks, new regulatory developments, changing credit and market risks, and risks to reputation and brand image may require disclosure. In addition to considering the implications of change on disclosures required by Section 302, companies also need to look at the implications to the Section 404 assessment and consider the need to update the company's documentation of processes and controls followed by a reexamination of control design and operating effectiveness.

196. After the first year of compliance, what happens to Section 404 compliance costs?

After nonaccelerated filers and newly public companies complete their first year of compliance, they transition from the intense project mode typically experienced in the initial year to an ongoing process in subsequent years. In making this transition, most companies seek to implement a compliance process at costs that are reasonable and sustainable on an ongoing basis. Following is a summary of the cost drivers over the first three years of Section 404 compliance:

Notes:

(1) A process created in Year Two

(2) Improving quality, reducing costs and compressing time of upstream business processes while simultaneously reducing financial reporting risk, through simplifying, focusing and automating manual processes, and improving the mix of preventive and detective controls can result in improvements in efficiency and effectiveness that would *reduce* testing scopes over time

197. Will subsequent annual assessments be similar to the initial annual assessment?

Subsequent annual assessments will be easier and less stressful than the initial annual assessment. Most of the required documentation will already exist and the emphasis will be on the effects of change. Most importantly, the independent public accountant's requirements will be understood for purposes of maximizing his or her use of the work of others.

Role of Management

198. What is the role of the disclosure committee?

The SEC has recommended that reporting companies create a disclosure committee to consider the materiality of information, determine disclosure requirements, identify relevant disclosure issues and coordinate the development of the appropriate infrastructure to ensure that reliable material information is disclosed in a timely manner to management for potential action and disclosure. The SEC contemplates that the disclosure committee would report to, and sometimes include, senior management, specifically the certifying officers.

The SEC indicated that the disclosure committee's members could consist of the principal accounting officer (or the controller), the general counsel (and/or another senior in-house lawyer responsible for SEC disclosure matters), the principal risk management officer and the chief investor relations officer (or an officer with equivalent corporate communications responsibilities). The committee also should include the chief information officer, appropriate representatives from the company's operating units, and other executives the company deems appropriate. To be effective, the disclosure committee should include an expert in SEC reporting and filing requirements.

Following are further observations about the disclosure committee's role:

- The committee defines what constitutes a "significant" transaction or event, and ensures the certifying officers have knowledge of the material information that could affect the company's disclosures. The committee also considers what is material and what isn't material in terms of meeting the SEC's requirements to make appropriate disclosure so that a prudent investor can make an informed decision.
- An effective disclosure committee is able to ascertain whether or not the information in a filing is complete (e.g., consideration of the effects of a decision by management to discontinue a segment of a business). The individuals serving on the committee must be knowledgeable of the business and its risks, and familiar with the disclosure practices of peer companies. They should be knowledgeable of the public reporting preparation process and the critical "feeds" to that process. They also should have sufficient stature within the company to initiate the appropriate action when necessary.
- The committee should assume the responsibility of determining whether there are any aspects of the company's culture that could frustrate the goal of accurate and complete reporting. For example, if a significant component of the CFO's and accounting management's compensation is linked to profits, that approach should be examined to ensure there is adequate balance in the reward system given to quality financial reporting.
- In addition to reporting directly to (as well as being accountable to) the certifying officers, the disclosure committee chair should meet periodically with the audit committee. The audit committee should receive reports on the various activities of the disclosure committee, including the quality of the company's filings and other disclosures, and any disagreements with the certifying officers or with external experts such as legal counsel or independent auditors. At a minimum, the audit committee should work with the certifying officers and the disclosure committee to evaluate the process for (i) identifying important financial reporting issues, (ii) presenting such issues to responsible parties on a timely basis, and (iii) ensuring such issues are fairly presented in conformity with generally accepted accounting principles in the company's external disclosures. The audit committee may have to take a role in resolving significant disagreements.

- The committee should review all publicly disclosed information, including 1934 Act filings, registration statements, and management's quarterly and annual evaluations of disclosure controls and internal control over financial reporting. Information reviewed also should include:
  - All press releases providing financial information or guidance to investors
  - Correspondence disseminated broadly to shareholders
  - Presentations to investor conferences, analysts, rating agencies and lenders
  - Disclosures on the company's investor relations website
- The committee should review internal information for matters having disclosure implications, including internal audit reports, reports to the board and to board committees, and reports to senior management.

These are a few examples of the disclosure committee's activities. A word of caution, however: If a company has a disclosure committee, management should ensure that the committee conforms to its charter. Organizing a disclosure committee with a specific charter and then failing to operate that committee in accordance with its charter exposes management and the company to criticism.

199. What is the role of the Section 404 compliance project sponsor?

The project sponsor should be a senior officer who can emphasize the importance of the project to the organization with credibility. The overall sponsor should be a certifying officer (i.e., CEO or CFO). Additional sponsors may be needed at major operating units and in key geographies. If there is a project steering committee, the sponsor may chair that committee.

200. What is the role of the Section 404 compliance project steering committee?

A Section 404 compliance steering committee serves three primary functions:

- First, the committee evaluates and approves the project plan, approves major scoping decisions, reviews major project findings and approves the internal control report.
- Second, it provides overall project oversight and serves as a sounding board for the project team to discuss and, if necessary, resolve major issues when they arise.
- Third, it assists the project team in gaining access to the internal resources needed to successfully complete the project.

The steering committee consists of the certifying officers, operating unit heads or representatives, and leaders of appropriate functions, including the general counsel, human resources, information technology and internal audit. The project sponsor, who may be one of the certifying officers, chairs the committee. The project leader reports to this committee.

The steering committee's sole purpose is to position the project team to succeed. It may meet periodically as scheduled to provide a checkpoint for key decisions and, when necessary, may meet to address significant issues.

201. How are the disclosure committee and the project steering committee related? How does their scope differ? How should they interact? How should the membership differ?

The disclosure committee has a broader scope than the Section 404 compliance steering committee. Whereas the steering committee is concerned with the success of the company's compliance with Section 404, the disclosure committee is focused on the fairness, accuracy, completeness and timeliness of the company's public reports. The disclosure committee is an integral component of a company's disclosure controls and procedures. It should determine that the company's disclosure controls and procedures are designed and implemented effectively.

With respect to interaction, the disclosure committee, unlike the steering committee, is not as concerned with the overall direction of the Section 404 compliance. However, the disclosure committee is interested in the results of the Section 404 compliance initiative, including the disclosure implications. Thus, both the disclosure committee and steering committee may interact to address common issues, such as identifying what constitutes a "significant deficiency" or "material weakness" in the design or operation of internal controls. They also may interact to review control deficiencies to recommend for disclosure in public reports.

With respect to membership, there may be some overlap in the composition of the disclosure committee and the steering committee. Based on the respective composition of the two committees, we make the following generalizations:

- Both committees may include operating unit heads or representatives and leaders of appropriate functions, e.g., the general counsel, information technology and internal audit.
- The principal accounting officer (or the controller) may serve on the disclosure committee, but also may serve as the Section 404 project leader reporting to the steering committee.
- The SEC recommends inclusion of the principal risk management officer and the chief investor relations officer (or an officer with equivalent corporate communications responsibilities) on the disclosure committee; these individuals are probably not needed on the steering committee.

The certifying officers may be represented on the steering committee, whereas the disclosure committee reports to them. In fact, the Section 404 project sponsor may be one of the certifying officers, who may even chair the steering committee.

202. What is the role of other executives?

To be successful, the project requires a broad base of support. The project sponsor should explain the project and its importance to other members of the senior management team and to operating and functional unit managers. These managers should be sufficiently aware and knowledgeable of the project so that they will be able to support the assessment activities that must be undertaken as well as make quality resources available when they are needed.

203. Who signs off on internal control over financial reporting?

Section 302 of Sarbanes-Oxley requires the principal executive and financial officers to make certifications regarding their company's public reporting and internal control over financial reporting. For most entities, this means the CEO and CFO. Ordinarily, these same officers also will be the ones who approve the internal control report. Thus, it is reasonable to conclude that these officers have the ultimate responsibility to sign off on internal control over financial reporting. The disclosure committee and Section 404 compliance steering committee may assist these officers in carrying out this responsibility. These committees should have appropriate representatives who are familiar with the company's operations, its disclosure controls and procedures, and the applicable public reporting requirements.

204. What communications, if any, are required of management beyond the quarterly executive certifications and annual internal control report?

Section 302 requires the CEO and CFO to report to the independent accountant (and to the audit committee) the following:

- All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting that are reasonably likely to adversely affect the company's ability to record, process, summarize and report financial information
- Any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal control over financial reporting

205. What is the role of operating and functional unit managers?

The project team should include operating, accounting and auditing representatives from the company's major business units and foreign operations. Operating and functional unit managers should support the participation on the project of the resources needed from their respective units to complete the project.

206. Can management rely solely on self-assessments of process owners for purposes of their evaluation of design and operating effectiveness?

No. While self-assessments by process owners can provide a valuable source of evidence, they should not be the sole basis for the certifying officers' evaluation. Other sources of evidence include effective entity-level analytics and monitoring, the results of internal audit testing, and other separate evaluations performed from time to time. See our responses to Questions 117 and 144 for further discussion.

207. Can management rely on the work of the internal auditors?

Yes, but not exclusively. We believe results of internal audit testing provide one source of evidence of the effectiveness of internal control over financial reporting. There are, however, other sources that management should also draw from, e.g., process owner self-assessment and entity-level monitoring.

208. To what extent can management rely on the work of the independent public accountant in making the assessment of internal controls effectiveness?

Management must make its own assessment. The independent accounting firm attests to and reports on management's assessment. Therefore, management should not rely on the work of the independent public accountant when making its assessment. The SEC's principles of independence with respect to services provided by the independent accounting firm are largely predicated on three basic standards: (1) an auditor cannot function in the role of management; (2) an auditor cannot audit his or her own work; and (3) an auditor cannot serve in an advocacy role for the client. Thus, the external auditors cannot perform management decision-making roles, such as determining for the company the controls that should be in place, evaluating the adequacy of the controls design and testing the operating effectiveness of controls, for purposes of supporting management's assertions on the company's internal controls. (See also Questions 218, 219, 220 and 221.) Although the SEC is very clear on this point in its auditor independence rules, the SEC does permit the auditors to provide recommendations for improvement in internal controls. Ultimately, the responsibility rests with management to make decisions regarding any recommendations, including decisions to implement.

Role of Internal Audit

209. What is the current status of the NYSE requirement that listed companies have an internal audit function?

The NYSE listing standards provide that "each listed company must have an internal audit function." In its commentary to that requirement, the NYSE states that the internal audit function must provide management and the audit committee with ongoing assessments of the company's risk management processes and system of internal control. A company may choose to outsource this function to a third-party service provider other than its independent auditor.

210. What should companies do if they are listed on other exchanges? Are they required to have an internal audit function?

NASDAQ and AMEX have not addressed the internal audit function in their listing requirements. The revised NASDAQ rules approved by the SEC were silent with respect to an internal audit function. A nonexistent or an ineffective internal audit function at a company needing an effective function to have effective monitoring and risk assessment could be at least a significant deficiency as well as an indicator of a material weakness. In today's world, companies without an internal audit function will be the exception, regardless of the legal requirements.

In January 2003, The Conference Board Blue Ribbon Commission on Public Trust and Private Enterprise issued its findings and recommendations with respect to auditing and accounting. Under Principle III: Improving Internal Controls and Internal Auditing, one of the "Suggested Best Practices" states:

> All companies should have an internal audit function, regardless of whether it is an "in-house" function or one performed by an outside accounting firm that is not the firm that acts as the company's regular outside auditors.

We believe that all firms should evaluate the need for an internal audit function if they do not have one. We have confirmed with a member of the Blue Ribbon Commission that the term "accounting firm" was not intended to preclude outsourcing to a qualified internal audit services provider.

211. How should internal audit avoid any conflict-of-interest issues as it plays a value-added role with respect to the Section 404 certification process?

There are a number of ways. First, internal audit should not have primary ownership over the Section 404 certification process. Second, a trend is emerging where internal audit is reporting directly to the audit committee. For example, in its findings issued in January 2003, The Conference Board Blue Ribbon Commission on Public Trust and Private Enterprise recommended, as a "best practice," that the chief audit executive or internal audit director has a direct line of communication and reporting responsibility to the audit committee. Finally, internal audit should align its audit plan with management's quarterly evaluation requirements, after management and the independent public accountant have signed off on the controls identified and evaluated during the prior year annual assessment. The IIA has issued a white paper on the role of the internal auditor in regard to compliance with Sections 302 and 404. The white paper helps to clarify the specific ways internal auditors might assist their organizations in complying with Sarbanes-Oxley. This white paper is available at **www.theiia.org** or on Protiviti's KnowledgeLeader℠ subscription-based website at **www.knowledgeleader.com**.

212. What is the role of internal audit in the evaluation process?

Internal audit can play an important role in documenting internal controls, testing internal controls and providing input to management with respect to concluding on design and operating effectiveness. Internal audit provides management a potential source of resources for purposes of complying with Section 404 of Sarbanes-Oxley. The COSO framework points out that separate evaluations conducted by internal audit are a form of monitoring. Again, as noted in our response to Question 211, the IIA has issued limited guidance on this matter.

213. What changes in internal audit can be expected as a result of Section 404?

One change will be a desire or emphasis (on the part of management, process owners and even the audit committee) for internal audit to get involved with various aspects of Sarbanes-Oxley compliance, from planning the Section 404 evaluation process to evaluating control design and all the way through to testing and the tracking and remediation of control deficiencies. While there is no one-size-fits-all response, internal auditors should, of course, strive to add value in the Sarbanes-Oxley-related work they do and assist their companies in complying the best way they can. In assisting their companies in this manner, internal audit also should be careful not to usurp the role of management in these compliance efforts.

Internal audit should continue to take an enterprisewide view of risk and not overlook other areas, issues, changes and risks that need their attention and involvement. In some cases, this may call for the addition of more internal or external resources to assist internal audit in fully meeting their mandates, charters and the most significant risks their organizations face.

Note that as part of obtaining evidence supporting the evaluation of the monitoring and risk assessment components of internal control over financial reporting, the independent auditor may review and assess the impact of the internal auditor's work and reports. This assessment puts more pressure on the internal auditors to fully execute their audit plans. Internal audit functions not using COSO as a framework for conducting and reporting on audits will have to align with the COSO framework to facilitate integration with Section 404 compliance. The emphasis on placing highly competent internal audit departments with direct reporting lines to the audit committee at the highest level of external auditor reliance, for purposes of the external auditor's use of the work of others, will likely create more interest in the results of quality assurance reviews assessing the existing internal audit function and identifying what needs to be improved and how to get it done.

The independent auditor also may evaluate whether the company's internal process of reporting control deficiencies is timely enough. This level of attention on timeliness of reporting can have a significant impact on the appropriate elevation policy for internal auditors and others in organizations that have not thought about the issue. Timely elevation of significant deficiencies or near significant deficiencies is consistent with and supportive of management's reporting responsibilities under Section 302.

Role of the Independent Public Accountant

214. When and how should the independent public accountant be involved during management's annual assessment process?

The project sponsor and team leader should communicate with the independent public accountant at regular intervals throughout the project. They should validate the approach and requirements with the independent accountant, with the intention of understanding expectations, professional standards and other requirements. They also should ascertain whether the "body of evidence" provided by the planned approach provides for an efficient audit. The goal is to plan and execute management's assessment so that the methodologies and frameworks used, the documentation developed, and the substantive issues addressed are consistent with the independent accounting firm's policies and requirements. Otherwise, there is a risk of rework and redundant effort during the audit.

Even though the external auditor is no longer expressing an opinion on management's assessment process, he or she still needs to understand management's process to plan and conduct a cost-effective audit. Following are illustrative examples, not intended as all-inclusive, of relevant checkpoints for the independent public accountant:

- Selection of significant financial statement accounts and disclosures
- Identification of relevant financial reporting assertions
- The relative risk of financial reporting assertions for the significant financial statement accounts and disclosures
- Entity-level assessment results, including the breakdown of the enterprise into control units for purposes of performing an entity-level assessment, the key attributes reviewed and the designation of entity-level controls that have a direct impact on significant financial reporting elements

- General IT controls assessment results
- The results of evaluating the period-end financial closing process
- Multilocation scoping
- The identification of the key controls, including the evaluation of the design effectiveness of those controls
- Documentation standards (i.e., the type and depth of documentation), format of documentation and extent of process-level documentation
- Extent and depth of validation, including management's test plan
- Disposition of documented control gaps from the entity-level controls assessment, pervasive IT controls assessment, and the assessments at the process level of controls design and controls effectiveness
- The process for evaluating the severity of control deficiencies at the end of the evaluation process

The project sponsor and project team leader need to work out a suitable protocol for obtaining the independent public accountant's input during the assessment process.

215. How should management prepare for the attestation process?

Management's preparation for the attestation process begins long before that process begins. All of the steps taken in getting started (see our responses to the questions in the "Getting Started" section of this publication) should be taken with the intention of preparing for the attestation process. The project team must thoroughly document the assessment process in a format that the independent public accountant will be able to understand and use as evidence during the audit. A best practice is to hold periodic checkpoints with the independent public accountant during the documentation preparation and assessment process to ensure the evaluation project is responsive to the auditor's requirements. See Question 214 for illustrative examples of these checkpoints. See also Question 184 for a discussion of the documentation management needs to support the assertions in the internal control report.

216. Did the SEC provide any guidance with respect to the attestation report?

Under the new rules, a company is required to file the independent auditor's attestation report as part of the annual report. The attestation must be made in accordance with standards for attestation engagements issued or adopted by the PCAOB. Section 404 further stipulates that the attestation cannot be the subject of a separate engagement of an accounting firm.

217. What does the PCAOB require with respect to the attestation report?

The PCAOB requires the external auditor to express an opinion on the company's internal control over financial reporting. An auditor cannot issue a Section 404 attestation report unless he or she also is auditing the company's financial statements.

218. What internal control "design" assistance can the independent public accountant provide without impairing independence?

None. SEC Release 33-8183 issued January 28, 2003, "Strengthening the Commission's Requirements Regarding Auditor Independence," states the following:

> … we believe that designing and implementing internal accounting and risk management controls impairs the accountant's independence because it places the accountant in the role of management.

219. Can the independent public accountant perform any testing on behalf of the audit client?

While the work of the independent public accountant does in fact provide yet another checkpoint for management, it should not be the basis for management's evaluation. The independent public accountant's responsibility is limited to reviewing the basis for management's assertions regarding the company's internal control over financial reporting. Under Section 404 of Sarbanes-Oxley, the independent auditor will be required to issue an opinion that attests to and reports on management's assertion in the annual internal control report that the internal control over financial reporting is designed and operating effectively. This assertion is one that management must support with appropriate documentation. Because the independent public accountant will rely on management's supporting documentation, it would be circuitous logic for the independent public accountant's work to be the basis for management's assertions. Further, in Auditing Standard No. 5, the PCAOB includes a written representation for management to provide to the auditor 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.

220. Can the company use its independent public accountant's software and/or methodology to support management's assessment?

Management may use whatever approach it chooses to plan, organize, conduct, document and support its evaluation. Software tools and methodology serve as a means of organizing the process so that management is addressing, documenting and concluding on relevant issues in a manner that is supported by authoritative frameworks (such as the COSO Integrated Framework).

During its open meeting in May 2003, the SEC indicated it would be "problematic" if management were to use auditor software that was designed to help management evaluate the effectiveness of controls or document the controls that exist. This comment was clearly a "red light" in those circumstances. The SEC did not address software in its final rules. However, as noted in Question 221, the SEC issued "reminders" to companies and their auditors, and made other points on independence that raise questions with respect to the use by management of the auditor's software. If the software includes libraries of controls that should be in place and management relies on those control libraries, is that a problem under the independence rules? If the software provides guidance on assessing controls design and management uses that guidance to formulate its judgments about design effectiveness, is that a problem under the independence rules? These are questions that management and the audit committee must resolve. What if the software were a mere shell with no control libraries and no guidance, and is simply an electronic notebook or a template to be completed by the company to assist in the attestation process? That is a very different set of circumstances.

We believe it would be a mistake to conclude that, because nothing was stated in the final rules on the subject, the SEC has issued an unequivocal "green light" on auditor software. The final rules provide, at a minimum, a "yellow light" of caution. Given the ambiguity in the final rules, it appears the overriding message is for management and audit committees to proceed with care when using auditor software. The SEC expects management and the audit committee to evaluate the facts and circumstances in light of the Commission's independence rules.

In choosing the software and/or methodology ("tools") to use, there are many factors for management to consider. For example:

- Are the tools web-based? Are they flexible? Are they easy and intuitive to use, or are they intricate and complicated, requiring extensive training of company personnel?
- Do the tools allow for continuous review and monitoring of internal controls, including quarterly self-assessments? Do they facilitate the distribution of questionnaires and aggregation of results?

- Does the audit firm own and update the information or does the company?
- Does the software enable the ability to view the documentation in the reporting formats desired by users?
- Do the tools facilitate overall project management? Do the formats included in the software provide an effective framework for accumulating the "body of evidence" for testing? Will the tools assist the evaluators in assessing design and operational effectiveness and the relative maturity of internal controls?

Other factors relating to tools and technologies for implementing controls repositories, documenting process maps, facilitating the assessment process and managing overall Section 404 compliance are discussed in Question 60.

These tools do not replace management's critical thinking and responsibility to conclude on relevant matters. The key is to ensure the company and the independent public accountant are on the same page with the approach taken during the evaluation process.

221. Can the company engage the independent public accountant to create original documentation of its internal control over financial reporting without impairing independence?

The safe answer in today's environment is probably not. According to Rule 2-01 of Regulation S-X of the SEC, the external auditor must be independent both in fact and in appearance. While the standards have not been promulgated by which the external auditor will be required to attest, significant involvement in the documentation of a company's internal control structure, followed by an attestation process in which the same documentation is reviewed, would be tantamount to keeping the books and auditing the books. The SEC's position is that the auditor cannot perform in the role of management, or audit his or her own work.

During its open meeting in May 2003, the SEC staff made statements to the effect that the documentation of controls and the evaluation of their effectiveness are indeed a management function. Therefore, if the auditor has been asked to perform that role instead of, or on behalf of, management, that kind of involvement could result in the auditor taking on a management role. Thus, the SEC staff pointed out that companies and their auditors need to be mindful of the independence requirements and determine how involved the auditor needs to be to understand adequately the controls and what management has done without having to actually "step into a management role."

The final rules released on June 6, 2003, do not reconcile clearly to the discussion during the open meeting in May. Specifically, in the open meeting, an absolute restriction was articulated as a "red light" to prohibit the independent accountant from documenting internal control over financial reporting for audit clients. The final rules, however, do not prohibit this practice but instead place limits around this activity and remind issuers and their auditors to adhere to the independence restrictions.

This development is not a surprise. The SEC has a long-standing practice of allowing issuers to formulate their own policies with respect to compliance matters. Subsequent to the open meeting, the SEC staff pointed out to us that nothing said in the open meeting or included in the final release on Section 404 is intended to change the independence release or rules, or the appropriate interpretation of those rules. When formulating company policies in this regard, management and audit committees must take into account the SEC's oral comments in the open meeting as well as its written rules. Thus, the burden is on management and the audit committee to evaluate the desirability of engaging the independent accountant in documenting internal control over financial reporting on behalf of management. In effect, the final rules constitute a "yellow light" of caution signaling to companies that it would be wise to monitor further SEC and PCAOB developments for additional clarification.

In the final rules, the SEC states it understands the need for management and the company's independent auditors to coordinate their respective activities relating to documenting and testing internal control over financial reporting. In stating that understanding, the SEC also issued two reminders to companies and their auditors:

- First, the Commission's rules on auditor independence prohibit an auditor from providing certain nonaudit services to an audit client.
- Second, management cannot delegate its responsibility to assess its internal control over financial reporting to the auditor.

The SEC also made two other points on independence:

- If the auditor is engaged to assist management in documenting internal controls, management must be actively involved in the process.
- Management's acceptance of responsibility for the documentation and testing performed by the auditor does not satisfy the auditor independence rules.

The above views expressed by the SEC raise several points.

- First, documentation of internal control over financial reporting by the independent accountant is implied to constitute a nonaudit service.
- Second, if the auditor performs documentation and/or testing of internal controls, management cannot simply accept responsibility for that work. This would be tantamount to management accepting responsibility for the results of bookkeeping or other services provided by the auditor related to the company's significant accounting records or financial reporting areas. Management must be actively involved in the documentation process.
- Third, the auditor must exercise care to ensure that he or she does not end up auditing his or her own work, or provide a service acting in a management capacity.
- Finally, while there is some ambiguity in the final rules that didn't exist during the SEC's open meeting in May 2003, it appears the overriding message is for management and the audit committee to proceed with care when engaging independent accountants to document internal control over financial reporting.

One practical approach to addressing the ambiguity of this issue is to focus on the magnitude of the documentation required to bring a company into compliance. This approach would prescribe that any situation in which "significant" documentation was necessary should avoid engagement of the external auditor other than in an advisory role. On the other hand, those environments in which minimal additional documentation was necessary might utilize the external auditor to help management identify and finalize the Section 404 documentation.

Sarbanes-Oxley requires management to establish and maintain controls and procedures to ensure all material information is presented to the public in accordance with the SEC's rules and forms, i.e., management is required to design the internal control structure. The documentation issue represents a minefield for boards and management teams because it will forever remain difficult to delineate the difference between documenting the internal control structure and designing the internal control structure. Documenting an internal control structure is similar to "blazing a trail." It requires a decision-tree type approach in which someone must decide each path to achieve an appropriate control structure. The selection of the primary path is a function of the risks that management perceives the company faces. Subsequent decision points will revolve around questions such as:

- What entity-level controls have a direct impact on significant financial reporting elements?
- What is the proper combination of preventive controls or detective controls?
- Do transaction volume and velocity permit manual controls or must computerized system controls be utilized?
- Within a process, how much segregation of duties is required?

- Are there pervasive controls affecting multiple processes and, if so, what is their impact?
- What is the impact of a centralized versus decentralized organization?

Each of these and other decisions require significant professional judgment. They represent trail markers about which management must make the ultimate determination. If the independent public accountant is asked to blaze and mark the trail and subsequently also determine if the markings are correct, then management, the board and the auditor could be exposed to allegations that independence was impaired. While independence in fact may have been preserved, the appearance of independence would be difficult if not impossible to explain in the public arena. If explanations are subsequently required, the accounting firm could be placed in the position of an advocate for management, a position the SEC rules do not permit.

Ultimately, the questions around appearance must meet the test of scrutiny by an objective third party who understands the nature of the work and the judgments required. This test makes these questions all the more important for management and the audit committee to consider. Given today's hypersensitive environment, this issue does not appear to be one in which it is in anyone's interest to test.

222. What kind of work can management expect of the company's independent public accountant during the attestation process?

The independent public accountant will want to understand management's assertions regarding internal control over financial reporting and how management supports those assertions. Management can expect the independent public accountant to, among other things:

- Interview management and the key players who were involved in the assessment.
- Review the documentation supporting the assessment.
- Perform tests of the documentation at both the entity level and process level to ensure it fairly reflects the controls that are actually in place.
- Evaluate management's conclusions as to design effectiveness.
- Perform independent reviews and selected audit tests of operational effectiveness.
- Evaluate whether the body of evidence in totality supports management's assertions on internal controls.
- Evaluate and advise on the disclosure implications of the findings.

Management also can expect the independent public accountant to consider the results of the audit work on the financial statements, consistent with an integrated audit model. If errors or omissions are noted by the auditor's tests, the auditor will evaluate the root causes of the errors to determine whether they arise from deficiencies in internal controls. The response to Question 184 provides a high-level checklist of things management must document when supporting the assertions in the internal control report and preparing for the attestation process.

223. Can management share interim drafts of the financial statements with the auditor?

Interim drafts of the financial statements may be shared with the auditor; however, to minimize the risk of the auditor determining that his or her involvement in the process might represent a significant deficiency or material weakness, the PCAOB staff notes that management should clearly communicate three things to the auditor:

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

Due to the changed dynamics in the auditor-client relationship, management should be careful when submitting financial statement drafts to the auditor. If the drafts are incomplete, the auditor may conclude there is a significant deficiency or worse. If specific footnotes are not included in the draft, management should point out the omission as well as the expected timing for completing those footnotes.

Management also should discuss the ground rules with the auditor in advance of submitting financial statement drafts. If there is any uncertainty with respect to the protocol for sharing drafts and management wants advice on financial statement presentation during the report preparation process, they should consider seeking the input of a qualified third party.

224. Can management discuss accounting issues with the auditor?

Yes. The PCAOB staff points out that "a discussion with management about an emerging accounting issue" or "the application of a complex and highly technical accounting pronouncement in the company's circumstances," are examples of "timely auditor involvement" that should not necessarily be an indication of a deficiency in the company's internal control over financial reporting. In these instances, management should proceed with caution until they clearly understand the auditor's ground rules for evaluating the company's internal control over financial reporting in view of these types of discussions. When in doubt, management should consult with third-party advisors.

225. Can management rely on the statutory audit work performed by the external auditor for significant subsidiaries or joint ventures?

Some argue that the regulatory or contractual environment for statutory audits at specific subsidiaries or joint ventures helps to decrease the inherent risk in their respective financial statements. Therefore, the argument continues, management need not test the controls as much as they would otherwise. These companies appear to have difficulty divorcing themselves from the standalone "full and separate" audits performed by the external auditor because they have relied upon them in the past. The rationale is that the company isn't really "relying" on the external auditor but is only considering the audit in evaluating inherent risk.

We recommend that management exercise caution with respect to taking this position for the following reasons:

- As explained in our response to Question 221, the auditor cannot audit his or her own work. Neither can the auditor provide services acting in a management capacity. Evaluating company inherent risk and internal controls, whether at a subsidiary or elsewhere, is a management responsibility.
- As explained in our response to Question 219, the PCAOB requires the auditor to obtain a written representation from management that management did not rely on the external auditor's audit work for purposes of formulating the assertions in the internal control report.

226. Can the external auditor use the work of the internal audit function and others for purposes of performing an audit of internal control over financial reporting?

Yes. Section AU 322 was issued over 15 years ago by the Auditing Standards Board to address how an auditor considers the work and direct assistance of an internal audit function when performing an audit of financial statements in accordance with generally accepted auditing standards. AU 322 requires that the external auditor inquire about internal audit's (a) organizational status within the company, (b) application of professional standards, (c) audit plan and (d) access to records. In addition, the external auditor is to inquire as to any scope limitations in the internal auditor's work. AU 322 also provides guidance on how the external auditor assesses the competence and objectivity of internal auditors.

The guidance included in Auditing Standard No. 5 applies the principles in AU 322 to focus the auditor's use of the work of others more specifically on altering the nature, timing and extent of the external auditor's work that otherwise would have been performed to test controls as part of an integrated audit of the financial statements

and internal control over financial reporting. The basic premise of Auditing Standard No. 5 is that the external auditor may use work performed by, or receive assistance from, internal auditors, company personnel (in addition to internal auditors) and third parties working under the direction of management or the audit committee that provides evidence about the effectiveness of internal control over financial reporting.

The auditor may evaluate the use of the work of others based on two fundamental principles relating to (1) the risk associated with the control being tested and (2) the competency and objectivity of the individuals performing the work the auditor plans to use. With respect to the first principle, the PCAOB states the following: "As the risk associated with a control increases, the need for the auditor to perform his or her own work on the control increases." This principle replaces the "principal evidence" ceiling and explicit restrictions (such as testing the control environment) on using the work of others, which was previously included in the now superceded Auditing Standard No. 2.

With respect to evaluating the qualifications of the persons performing the work, the Board defines "competence" as "the attainment and maintenance of a level of understanding and knowledge that enables personnel to perform ably the assigned tasks." The Board defines "objectivity" as the "ability to perform assigned tasks impartially and with intellectual honesty." In addition, the Board refers to the application of certain paragraphs of AU Section 322 that provide more specific guidance with respect to this assessment. For example, when assessing competence, the external auditor considers such factors as:

- Educational level and professional experience
- Professional certification and continuing education
- Audit policies, programs and procedures
- Practices regarding assignment of internal auditors and other individuals
- Supervision and review of internal audit and testing activities
- Quality of working-paper documentation, reports and recommendations
- Evaluation of internal auditors' and evaluators' performance

The context of the auditor's assessment of competence in conjunction with an audit of internal control over financial reporting is whether the persons performing the work have the qualifications and the ability to perform the work the auditor plans to use.

When assessing objectivity, the external auditor considers such factors as:

- The organizational status of the chief audit executive or controls evaluation function, including:
  - Whether the executive or function reports to an officer of sufficient stature to ensure broad audit and testing coverage and adequate consideration of, and action on, evaluation findings and recommendations
  - Whether the executive or function has direct access and reports regularly to the board of directors and/or the audit committee
  - Whether the board of directors or audit committee oversees employment decisions related to the internal audit or controls evaluation function
- Policies to maintain internal auditors' or the controls evaluation function's objectivity about the areas evaluated:
  - Policies prohibiting internal auditors and others from evaluating or testing areas where relatives are employed in important or audit-sensitive positions
  - Policies prohibiting internal auditors and others from evaluating or testing areas where they were recently assigned or are scheduled to be assigned on completion of responsibilities in the internal audit or controls evaluation function

The context of the auditor's assessment of objectivity in conjunction with an audit of internal control over financial reporting is whether factors are present that either inhibit or promote a person's ability to perform with the necessary degree of impartiality, and freedom of bias, the work the auditor plans to use.

In Auditing Standard No. 5, the Board also refers to "personnel whose core function is to serve as a testing or compliance authority at the company, such as internal auditors, [who] normally are expected to have greater competence and objectivity in performing the type of work that will be useful to the auditor." This point of view suggests that the auditor will be able to rely to a greater extent on the work of a "highly competent and objective internal audit or equivalent testing or compliance function" than on work performed by others within the company. That said, the auditor also will be able to rely on the work of company personnel other than internal auditors as well as third parties functioning under the direction of management.

In summary, the PCAOB's approach under Auditing Standard No. 5 clearly allows the external auditor to appropriately use the work of others, and not just internal auditors, as a basis for altering the scope of an audit of internal control over financial reporting. The Board encourages greater use of the work of others by requiring auditors to (1) understand the relevant activities of others and determine how the results of that work may affect his or her audit and (2) evaluate whether and how to use their work to reduce audit testing. Section 404 compliance teams will want to make sure they are managing their work appropriately, consistent with the PCAOB's criteria.

227. Can the independent auditor issue a report to management or the audit committee indicating that no significant deficiencies were noted during an audit of internal control over financial reporting?

No. The PCAOB precludes the auditor from issuing such representations or reports. Under the standards set forth in Auditing Standard No. 5, an audit of internal control over financial reporting is not designed to detect significant deficiencies. These reports may not be issued because of the potential for misinterpretation.

228. Will the SEC accept an adverse opinion on internal control over financial reporting?

Yes. While the SEC will not accept an adverse opinion on the financial statements, the Commission will accept an adverse opinion on internal control over financial reporting. Both the SEC and the PCAOB require the auditor to issue an adverse opinion on the effectiveness of internal control over financial reporting if one or more material weaknesses exist. If management issues an internal control report in the Form 10-K asserting that internal control over financial reporting is ineffective due to the existence of a material weakness, the auditor's issuance of an adverse opinion is, in effect, symmetrical with the conclusion in management's report. However, if the auditor concludes a material weakness exists, but management does not and therefore concludes in its internal control report that internal control over financial reporting is effective, the Board states the following in Auditing Standard No. 5:

> If [a] material weakness has not been included in management's assessment, [the auditor's report] should be modified to state that a material weakness has been identified but not included in management's assessment. Additionally, the auditor's report should include a description of the material weakness, which should provide the users of the audit report with specific information about the nature of the material weakness, and its actual and potential effect on the presentation of the company's financial statements issued during the existence of the weakness. In this case, the auditor also is required to communicate in writing to the audit committee that the material weakness was not disclosed or identified as a material weakness in management's assessment.

If a material weakness is included in management's assessment and the auditor concludes that the disclosure of the material weakness is not fairly presented in all material respects, the auditor's report is required to articulate this conclusion as well as describe the information necessary to fairly present the material weakness. If the

auditor issues an adverse opinion on internal control over financial reporting due to a material weakness, the auditor must make mention that the material weakness was considered in determining the nature, timing and extent of auditing procedures in connection with the audit of the financial statements and that the report on internal control over financial reporting does not affect the report on the financial statements.

229. What is required of the independent auditors each quarter?

In SAS 722, the PCAOB requires the auditor to perform certain procedures on a quarterly basis. These procedures include making inquiries about significant changes in the design and operation of internal control over financial reporting that have occurred subsequent to the preceding annual audit or prior review of interim financial information. The auditor must evaluate the implications of any changes noted and determine whether such changes materially affect, or are reasonably likely to materially affect, internal control over financial reporting. The auditor is not required to render a report on a quarterly basis.

This is the same type of involvement the auditor has with respect to the quarterly 10-Qs. Note also that the definition of a control deficiency incorporates the potential for misstatements in interim financial statements.

230. Can the same audit firm issue an opinion on internal control over financial reporting of a user organization and also issue the SAS 70 letter pertaining to a service organization to which the user organization has outsourced a significant process?

In situations where management has outsourced certain functions to third-party service provider(s), management retains responsibility for assessing the controls over the outsourced operations (see Question 86). However, the SEC staff has noted that management would be able to rely on a Type 2 SAS 70 report even if the auditors for both companies were the same. In this situation, the management of the service provider engaged the audit firm and that management is independent of the user organization's management. On the other hand, the staff also noted that if the management of the user organization were to engage its 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. In any event, management is still responsible for maintaining and evaluating, as appropriate, controls over the flow of information to and from the service organization.

Role of the Audit Committee

231. With respect to the financial reporting process and internal control over financial reporting, what is expected of the audit committee?

The audit committee oversees the issuer's external financial reporting and internal control over financial reporting. This is an important role. Board and audit committee oversight is an element of the control environment, according to COSO. In addition, the SEC has indicated that the activities of the audit committee represent an entity-level control and classifies these activities as one of several examples of "controls to monitor other controls." While the SEC has not specifically addressed in detail the relevant activities of the audit committee in this context, the Commission has stated that it would ordinarily expect a board of directors or audit committee, as part of its oversight responsibilities for the company's financial reporting, to be knowledgeable and informed about the evaluation process and management's assessment of internal control. It would be expected that the scope of such oversight would include controls to prevent or detect management override. The SEC also has stated that ineffective audit committee oversight is a situation requiring an evaluation as to whether a material weakness exists.

Auditing Standard No. 5 states that the independent auditor is required to focus on factors related to the effectiveness of the audit committee's oversight of the company's external financial reporting and internal control over financial reporting. These factors include:

- Independence of audit committee members from management
- Clarity of committee responsibilities, as articulated in the committee charter, and the extent to which the audit committee and management understand those responsibilities
- Extent of audit committee involvement and interaction with the external auditor
- Extent of audit committee involvement and interaction with the internal auditor
- Extent of interaction with key members of financial management, including the chief financial officer and chief accounting officer
- Degree to which appropriate questions are raised and pursued with management and the external auditor, including questions that indicate an understanding of the critical accounting policies and judgmental accounting estimates
- Time devoted to issues around internal control over financial reporting
- Level of committee responsiveness to issues raised by the auditor, including those required to be communicated by the auditor to the audit committee (for example, significant deficiencies)

The requirements of the auditor, as articulated by the PCAOB, do not supplant the overall responsibility of the board of directors to evaluate audit committee effectiveness. Other examples of factors the board, audit committee and management – but not the outside auditor – should consider when evaluating committee effectiveness include:

- Committee compliance with Sarbanes-Oxley Section 301
- Presence of one or more financial experts on the committee
- The nomination process (i.e., are committee members selected using an outside search firm or equivalent process based upon desired skill sets?)
- Committee compliance with other provisions set forth in the applicable listing requirements

Although the external auditor may not consider the above factors in his or her evaluation, the board should.

232. How and when should the audit committee be involved in management's evaluation process and in the independent public accountant's attestation process?

During one of the SEC's open meetings on Section 404, the SEC staff commented that the audit committee is expected to play an important governance role in requiring changes to correct internal control deficiencies. Audit committees should understand the extent of diligence they must perform with respect to management's internal control report and the independent accounting firm's attestation report. This is a question for legal counsel. We understand that counsel are generally advising audit committees to use the same type of line of inquiry on these matters as on the annual certified audit opinion, i.e., they should ask what problems and issues were found and how they are being resolved.

Because internal control over financial reporting is a subset of disclosure controls and procedures, the audit committee also should inquire as to (1) whether there are any material changes that could either affect or potentially affect internal control over financial reporting and (2) whether any significant deficiencies or potential significant deficiencies have come to management's attention. These inquiries should be integrated with the committee's role in the quarterly evaluation of disclosure controls and procedures. The audit committee also should work with the CEO, the CFO and the chairman of the disclosure committee, if any, to evaluate the process for (i) identifying important financial reporting issues, (ii) presenting such issues to the responsible

parties on a timely basis, and (iii) ensuring such issues are fairly presented in conformity with generally accepted accounting principles in the company's external disclosures. In this respect, the audit committee should pay close attention to the adequacy of management's risk assessment process to ensure that it is a quality process each year.

233. What questions are audit committees asking with respect to the Section 404 evaluation during the first year of compliance?

With respect to the first year of compliance with Section 404, some of the questions audit committee members have asked at the inception of the project include:

(a) How do you define "internal control" in the context of financial reporting? In plain and simple language, please.

(b) What are the company and the audit firm doing to prepare for the Section 404 requirement for management to issue an internal control report and for the auditor to issue an opinion on internal control over financial reporting? Is the planning taking place in an orderly manner to make the process more effective, less disruptive and less costly? How is the project being scoped to ensure the review focuses on what matters?

(c) How does the audit of internal control over financial reporting impact the cost of the audit? Is there an opportunity to reduce audit costs by spreading the attestation process over a longer period of time out of the audit firm's peak? Is the Section 404 internal control audit "integrated" with the financial statement audit to minimize cost? Is the external auditor maximizing his or her use of the work of others supporting management's Section 404 assessment?

(d) What is it going to cost? Assuming an audit firm quotes 30 percent of the annual audit fee, does that mean it will take 30 percent of the time the annual audit takes? If not, how much of this fee is a premium for assumption of risk? Are the audits of internal control over financial reporting and of the financial statements being integrated effectively?

(e) What is the proper role of the audit committee in this area? How much diligence should the audit committee do with respect to management's internal control report and the audit firm's attestation report? To what level of granularity should the audit committee review the underlying project details? How does the audit committee best keep an eye on project progress, the nature of interim results, the impact of these results and the achievement of project milestones? How do we minimize or manage "surprises" (as in "no surprises")?

(f) Is the audit committee satisfied that the role planned for the independent accountant during the controls assessment is appropriate, given the SEC's views on independence?

(g) If you, the independent auditors, had to make this certification for last year's financials, knowing what you know now, do you know of anything that would stand in your way in terms of reporting that the company's internal controls are effective? What don't you already know that will require additional and/or extensive work for you to gain the fact base you need?

As the Section 404 compliance project progresses during the first year of compliance, the additional questions audit committee members have been asking include:

(a) How will the auditor evaluate the effectiveness of the audit committee's oversight with respect to the financial reporting process and internal control over financial reporting, and what is the current status of these new requirements? Is there anything the committee should be doing that historically it has not? (See also Question (e) above.)

(b) Are there any disagreements between management and the auditor with respect to management's approach to assessing internal control over financial reporting?

(c) Is management satisfied that the company's internal reporting policies are sufficient to surface in a timely manner control deficiencies that could potentially be significant deficiencies or material weaknesses? (Note that this question has quarterly implications under Section 302.)

(d) Has management decided on the company's test plan? If so, how does the plan compare with the testing planned by the external auditor?

(e) What is management doing to prepare for ongoing compliance with Sections 302 and 404 after the initial internal control report is filed?

(f) As a practical matter, when does the controls testing work for most companies have to be completed in order to have adequate time to do remediation work to cure potential defects?

(g) If the auditor issues an adverse opinion on internal control over financial reporting, how will that report affect the auditor's opinion on the financial statements? What are the ramifications under the SEC's rules?

234. What questions are audit committees asking of companies that have complied with Section 404 for several years?

For companies that have already complied with Section 404, following are examples of some of the questions audit committee members are asking of management regarding the company's assessment approach:

(a) What changes will management make to the company's approach to make it more top-down and risk-based? How will these changes affect the cost of compliance?

(b) Has management significantly increased or decreased the level of controls testing in any areas this year? If so, in which areas have there been significant changes, and why?

(c) Have there been any significant systems changes this year? If so, were these changes disclosed as material changes in internal control over financial reporting as part of the Section 302 certification reporting? How have these systems changes affected the Section 404 evaluation process?

(d) How did management assess the strength of the company's entity-level controls? Were there any deficiencies or areas of concern?

(e) How has management's assessment of entity-level controls and the IT general controls changed from the prior year? If there were significant changes, how have the changes affected the Section 404 evaluation plan?

(f) Has management used self-assessment techniques? If so, what processes and controls were covered by self-assessment(s), and what were the results?

Following are questions of management regarding the company's internal control structure:

(a) Has management thought about the company's entity-level and process-level monitoring controls and whether the company's test plan is sufficiently balanced with respect to reliance on these controls as well as reliance on independent transaction-level controls testing?

(b) Has management determined that the company's automated controls are being used in the most effective way possible? If so, are such controls being relied upon in the Section 404 evaluation?

(c) If there are any significant deficiencies or material weaknesses identified as part of last year's Section 404 assessment, how has management addressed the underlying processes and controls this year?

(d) How is management using the Section 404 assessment to identify opportunities for improving the quality of the internal control structure and the upstream business processes?

(e) Is management satisfied that the company's entity-level analytics, metrics and other controls are providing transparency as to the effectiveness of internal control over financial reporting in significant areas?

In addition, following are some questions of management and the external and internal auditors:

(a) Is sufficient testing directed to higher risk areas, e.g., areas involving significant accounting estimates, related party transactions or critical accounting policies?

(b) Is management satisfied that the key controls have been narrowed down to the vital few that really matter? If so, is the external auditor in agreement with the company's designated key controls, including the design effectiveness of these controls?

(c) What changes will the auditor put in place to make the audit of internal control over financial reporting more top-down and risk-based as well as more integrated with the audit of the financial statements? How will these changes affect the cost of the audit?

(d) Is significant independent direct testing being focused on areas management regards as "low risk"? If so, why?

(e) Are there any areas in which management believes the external auditors could increase their reliance on the work of others?

(f) How does the internal audit plan align with the Section 404 test plan?

Impact on Sections 302 and 906

235. What is the impact of the Section 404 rules on Sections 302 and 906?

The list of required exhibits to be included in quarterly and annual reports filed with the SEC includes the certifications required by Sections 302 and 906 of Sarbanes-Oxley. For example, the exhibit requirements of Forms 20-F and 40-F and Item 601 of Regulations S-B and S-K add the Section 302 certifications to the list of required exhibits. The intent of including the certifications in the list of required exhibits is to make the certifications easier to locate. Following the first year of Section 404 compliance, the Section 404 rules also amend the form of certifications to be provided pursuant to Section 302 of Sarbanes-Oxley by adding a statement that the certifying officers are responsible for designing, and have designed, internal control over financial reporting or have had such controls and procedures designed under their supervision.

With respect to the Section 906 certifications, Exchange Act Rules 13a-14 and 15d-14, Investment Company Act Rule 30a-2, and the exhibit requirements in Forms 20-F, 40-F and Item 601 of Regulations S-B and S-K, all require inclusion of these certifications as exhibits in reports filed with the Commission. Although Section 906 does not explicitly require the certifications to be made public, the SEC believes Congress intended for public disclosure. The exhibit requirement enhances compliance by allowing the Commission, the Department of Justice and the public to monitor the certifications effectively. By subjecting the Section 906 certifications to the signature requirements of Regulation S-T, companies are required to retain a manually signed signature page or other authenticating document for a five-year period, which preserves evidential matter in the event of prosecution.

These rules and form amendments concerning Section 302 and Section 906 certifications apply to any reports due on or after August 14, 2003. Companies also are permitted to "furnish" rather than "file" the Section 906 certifications with the SEC. Thus, the certifications will not be subject to liability under Section 18 of the Exchange Act. The certifications also are not subject to automatic incorporation by reference into a company's Securities Act registration statements, which are subject to liability under Section 11 of the Securities Act, unless the issuer takes specific steps to include the certifications in a registration statement.

236. May certifying officers cite "reasonable assurance" when referring to the company's disclosure controls and procedures?

In their executive certifications, some companies have indicated that disclosure controls and procedures are designed only to provide "reasonable assurance" that the controls and procedures will meet their objectives. The SEC staff generally has not objected to this disclosure and has requested additional disclosure to set forth,

if true, the conclusions of the certifying officers that the disclosure controls and procedures are, in fact, effective in providing "reasonable assurance."

Other companies have included disclosure that there is "no assurance" that the disclosure controls and procedures will operate effectively under all circumstances. In these instances, the staff has requested companies to clarify that the disclosure controls and procedures are designed to provide "reasonable assurance" of achieving their objectives and to set forth, if true, the conclusions of the certifying officers that the controls and procedures are, in fact, effective in providing "reasonable assurance."

237. Why do companies report control deficiencies that are not material weaknesses?

In the early days of the first adopters of Section 404, a number of companies made advanced disclosure regarding control deficiencies. For example, during the eight months ended June 30, 2004, approximately 1 percent of U.S. public companies filing reports with the SEC reported disclosures regarding internal control matters. Approximately 75 percent of these filings involved reporting and/or remediation of material weaknesses in internal control over financial reporting. The remaining filings reported control deficiencies and other matters not involving material weaknesses. This was, and still is, due to companies being required to disclose change that has materially affected, or is reasonably likely to materially affect, internal control over financial reporting.

To illustrate, some companies have reported changes in their business, such as: rapid growth through acquisitions and market conditions; increased complexity of transactions; large and complex acquisitions; integration of legacy accounting and information systems; new installations of ERP systems; and other major developments. Human resources matters also have been a point of focus for disclosure of change. For example, some companies have disclosed significant reductions in the workforce. Others have disclosed the turnover of key finance personnel, such as turnover at the chief financial officer position and layoffs of accounting personnel, which significantly reduced the number and experience level of accounting staff. One company disclosed the transition of a large number of general and administrative personnel from one facility to another facility. Still other companies have reported on their remediation of significant deficiencies or provided an update on the resolution of previously disclosed deficiencies, while others have disclosed uncertainties with respect to the internal control environment as a "risk factor."

238. What are the common types of control deficiencies being reported by public companies?

According to an AuditAnalytics™ study published in March 2007, during the first year of compliance with Section 404 (periods ended prior to November 15, 2005), almost 17 percent of the Section 404 filings included adverse audit opinions. For the second year, the same study also compiled data for all filings for periods ended through January 31, 2006, and found that just over 10 percent of the filings included adverse opinions. An AuditAnalytics™ study published in May 2006 also reported the most common types of internal control failures reported during the first year of Section 404 compliance as well as during the second year for filings with periods ended through January 31, 2006. These control failures are summarized below:

	Percent of Total Failures	
Internal Control Failures	**Year 1**	**Year 2**
Personnel Issues	48.1	46.9
Segregation of Duties	21.2	12.4
Restatements of Financials	49.6	30.4
Material Year-End Adjustments	53.1	70.1
IT Processing Access Issues	20.8	17.5

Note that the preceding percentages are based on the total number of filings. A single filing may reflect more than one type of failure. For example, a restatement of financial statements could have been attributed to personnel issues.

239. What are the sector and size characteristics of companies reporting control deficiencies?

According to a study by AuditAnalytics™ in May 2006, during the first year of Section 404 compliance as well as during the second year for filings with periods ended through January 31, 2006, the following characteristics were noted:

- The six industries reporting the most filings with material weaknesses during the study period were (in descending order from most frequent to least frequent) financial services/banking/credit, equipment manufacturing and software as the top three, with home/office/personal manufacturing and telecommunications tied for fourth, and semiconductors and electronics in the sixth spot. These six sectors comprise 72 percent of the filings related to internal control failures included in the study period.
- During the first year of Section 404 compliance, the five industries reporting the highest percentage of filings with material weaknesses were (in descending order from most frequent to least frequent) entertainment, restaurants, mining, telecommunications and software. The five industries reporting the highest percentage of filings with material weaknesses in the second year of Section 404 compliance were (in descending order from most frequent to least frequent) telecommunications, hotels and motels, mining and software (tied for third), and equipment manufacturing.
- Companies with revenues of less than $100 million submitted 26 percent of the filings reporting internal control failures.
- Companies falling into the category of revenues of over $100 million but less than $1 billion submitted one-half of the reports indicating internal control failures.

240. If a significant change occurred in the second fiscal quarter but before the filing of the first fiscal quarter Form 10-Q, is there a requirement to disclose the subsequent event in the first fiscal quarter Form 10-Q?

Yes, if the change materially affects, or it is reasonably possible that it might materially affect, internal control over financial reporting. The disclosure requirements under Section 302 extend through the filing date.

241. Must management aggregate and evaluate control deficiencies on a quarterly basis at the same level of rigor as at year-end?

Under Section 302, management must report any significant deficiencies and material weaknesses to the audit committee and to the auditors. When the executive certification is issued each quarter, the certifying officers represent that they made these disclosures. Because "materiality" and "material weaknesses" are defined by the SEC and PCAOB in terms of both annual and interim reporting, if there are control deficiencies – whether "new" or carried over from the prior year – management must be cognizant of its responsibilities around reporting to the audit committee and to the auditors. Reporting to the audit committee and to the auditors can ultimately lead to disclosure to investors.

These quarterly requirements suggest three things:

- First, management needs an elevation process so that new issues are raised in a timely manner with the appropriate decision-makers for possible action and disclosure. From a practical standpoint, some companies may choose to disclose all known control deficiencies to the audit committee, except the obviously trivial ones. That practice eliminates having to make a "significance" cut for borderline deficiencies (i.e., between "significant" versus "not significant").

- Second, open deficiencies need to be monitored to make sure they don't become problem areas. Remediating them to eliminate them as issues might be even better from a risk reduction standpoint.
- Third, evaluation of open and new control deficiencies must take place using an appropriate methodology to ascertain whether the disclosure obligations under Section 302 are triggered and some level of external reporting is required. This methodology need only focus on whether a material weakness exists. An intricate analysis is not required to determine whether a significant deficiency exists. Now that the SEC has modified the definition of a significant deficiency (see Question 108), management must only determine whether a deficiency, or combination of deficiencies, "merits attention by those responsible for oversight of the [company's] financial reporting." Thus, management is able to exercise more judgment in determining whether significant deficiencies exist and must be disclosed.

The Disclosure Committee plays an important role in the above process.

We do not believe that the above discussion requires a detailed *quarterly* aggregation analysis. The above discussion outlines a practical approach and recognizes that the Section 404 assessment is a point-in-time assessment as of year-end. This means that a rigorous aggregation analysis is only required at the end of the year. In a published interpretation, the PCAOB staff has stated that "some issuers may correct identified control deficiencies prior to year end without reaching a conclusion as to their severity." The staff goes on to say that "the significance of the deficiency [is] irrelevant in terms of management's year-end conclusion … because the deficiency would not exist as of year-end. This commentary by the PCAOB staff at least implies that the staff does not expect a detailed quarterly aggregation analysis. That said, we are aware of some companies choosing to conduct a quarterly analysis to sharpen the focus of communications to the audit committee. At the time this publication went to print, the SEC had not addressed itself to this issue.

Accelerated Filing Requirements

242. What are the latest filing requirements with respect to Form 10-K and Form 10-Q?

The SEC accelerated the filing of quarterly and annual reports under the Exchange Act for domestic reporting companies that have a common equity public float of at least $75 million, that have been subject to the Exchange Act's reporting requirements for at least 12 calendar months and that previously have filed at least one annual report. These accelerated filer rules have since been amended several times. They are used as the basis for determining when companies must comply with Section 404.

The initial purpose of the accelerated filer phase-in period was to allow a transition for companies to adjust their reporting schedules and to develop efficiencies to ensure that the quality and accuracy of reported information would not be compromised. The Section 404 compliance process made this transition more complicated for most companies. Therefore, the accelerated filer rules also are used as the basis for determining when companies must comply with Section 404.

Under the current rules, as amended:

- A new category of companies has been created called "large accelerated filers." This category includes companies with a public float (see Question 243) of $700 million or more and that meet the other three conditions that currently apply to accelerated filers, as explained in Question 245.
- The category of "accelerated filers" has been redefined to ease the restrictions under the old rules on the process for exiting accelerated filer status as well as establish requirements for exiting out of large accelerated filer status. These companies must have at least $75 million, but less than $700 million, in public float. The exit requirements out of accelerated filer status have been modified to permit an accelerated filer whose public float has dropped below $50 million to file an annual report on a nonaccelerated basis for the same fiscal year

that the determination of public float is made. The Commission also permits a large accelerated filer to exit promptly out of large accelerated filer status once its public float has dropped below $500 million.

- An accelerated filer's annual report on Form 10-K is due within 75 days after fiscal year-end and its quarterly reports on Form 10-Q are due within 40 days after fiscal quarter-end.
- Beginning with the annual reports for fiscal years ending on or after December 15, 2006, a large accelerated filer's annual report on Form 10-K would be due within 60 days after the fiscal year-end and, subsequent to the filing of the aforementioned annual report, its quarterly reports on Form 10-Q would be due within 40 days after fiscal quarter-end.

The current Form 10-K and 10-Q compliance requirements are summarized below:

	Form 10-K Deadline (After Fiscal Year-End)	Form 10-Q Deadline (After Fiscal Quarter-End)
Large Accelerated Filers	60 days	40 days
Accelerated Filers	75 days	40 days
Nonaccelerated Filers	90 days	45 days

As this publication went to press, the SEC proposed rule amendments relating to its disclosure and reporting requirements for smaller companies under the securities laws. The Commission proposed to extend the benefits of its current optional disclosure and reporting requirements for smaller companies to a much larger group of companies. In effect, its proposals would allow companies with a public float of less than $75 million to qualify for the smaller company requirements, raising the threshold from $25 million. The substance of the proposals is to combine the "small business issuer" and "nonaccelerated filer" categories of smaller companies into a single category of "smaller reporting companies." The proposals would maintain the current disclosure requirements for smaller companies contained in Regulation S-B, but would integrate them into Regulation S-K. The bottom line is that Section 404 is still expected to apply to these smaller companies.

243. For purposes of applying the SEC's market capitalization test, what is meant by "public float"?

The SEC defines "public float" as "the aggregate market value of a company's outstanding voting and non-voting common equity (i.e., market capitalization) minus the value of common equity held by affiliates of the company." For example, outstanding shares held in a voting trust, the shares of which are held by management or members of a controlling family, would be excluded. The SEC explained in its release of the original accelerated filing rules that a public float test serves as a reasonable measure of company size and investor interest.

In Regulation S-X, an "affiliate" is defined as follows:

> An "affiliate" of, or a person "affiliated" with, a specific person is a person that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with, the person specified.

The definition of an affiliate is a fairly intricate one and requires hands-on knowledge of experiences with different facts and circumstances and relevant literature published in various SEC staff releases. For example, shares held by management would be included in the definition of shares held by an affiliate, recognizing management as beneficial owners. Shares held by family members related to management also would be considered to be held by affiliates, as are shares owned by a subsidiary of the company. In certain instances, shares held by board members also are included in the determination. Accordingly, legal counsel must assist in this determination.

244. When determining the applicability of the accelerated filing requirements under the SEC's Section 404 rules, when is the measurement date for purposes of quantifying a company's "market capitalization"?

The SEC's rules on accelerated filings state that the determination of market capitalization is "as of the last business day of its most recently completed second fiscal quarter." For example, a U.S. nonaccelerated filer will have to ask itself: "Was our public common float $75 million or greater at the end of our most recent second quarter?"

The purpose of the public float test, according to the SEC, is to provide a reasonable measure of company size and market interest. This definition of accelerated filers *excludes* nearly half of all publicly traded companies.

245. If a company is below the market capitalization threshold now but subsequently exceeds the threshold, when must it begin to comply with the accelerated filing deadlines?

The SEC's rules state the following:

> Accelerated deadlines will apply to a company after it first meets the following conditions as of the end of its fiscal year:
>
> (a) Its common equity public float was $75 million or more as of the last business day of its most recently completed second fiscal quarter;
>
> (b) The company has been subject to the reporting requirements of Section 13(a) or 15(d) of the Exchange Act for a period of at least 12 calendar months;
>
> (c) The company has previously filed at least one annual report pursuant to Section 13(a) or 15(d) of the Exchange Act; and
>
> (d) The company is not eligible to use Forms 10-KSB and 10-QSB.

Note that the accelerated deadlines vary according to whether the company's common equity public float exceeds $700 million, which is the threshold for distinguishing between a large accelerated filer and an accelerated filer (as discussed in Question 244).

Thus, if a calendar-year reporting company meets the size test (Item A) as of the end of the second quarter in any particular year (2006, for example), and then meets the other three tests (Items B, C and D) as of December 31, 2006, it must begin complying with the accelerated filing requirements beginning the first quarter in calendar 2007.

Once a company becomes an accelerated filer, it remains an accelerated filer until the public float drops below $50 million. The annual report for the fiscal year in which that determination is made may be filed on a nonaccelerated basis. The prior exit requirements made it very difficult to exit the accelerated filing requirements once a company qualified as an accelerated filer. Likewise, a company may exit out of large accelerated filer status once its public float has dropped below $500 million.

246. If a calendar-year reporting company meets the requirements as an accelerated filer for SEC reporting purposes as of December 31, 2006, what is its Section 404 compliance status if its market cap subsequently falls below the required threshold as of June 30, 2007?

If an accelerated filer company's common equity public float were to fall below $50 million as of June 30, 2007, it wouldn't matter from a Section 404 compliance standpoint because, under the current rules, it must comply with Section 404 anyway in calendar 2007. In effect, even if a calendar-year reporting company loses its accelerated filer status in 2007, the Section 404 transition process will have run its course and all calendar-year reporting companies, regardless of size, will be required to comply.

However, there is always the chance that the SEC could extend the Section 404 transition period yet again for nonaccelerated filers. For example, if it deferred the deadline for another year, then the premise of the above question frames a different response. If the market capitalization of a calendar-year company that complied with Section 404 as an accelerated filer in 2006 were to fall below $50 million as of June 30, 2007, then the company would have the option to no longer comply with Section 404.

While the SEC rules would permit an exit from Section 404 compliance, management would want to be sure that it made sense to do so. For example, what if a material weakness were reported in the internal control report filed for 2006? The market will want to know if management successfully remediated the material weakness. Furthermore, the exit from Section 404 compliance will only last as long as the SEC's extended deadline. Therefore, there could be added costs associated with exiting compliance and subsequently picking it back up again a year or so later. Finally, management should consider the impact of an exit from Section 404 compliance on the company's stock price and credit rating, for it is not clear at this time what that impact might be.

Private Companies and Initial Public Offerings

247. Any advice for a privately held company that intends to either undertake an IPO or sell to a public company during the next two to three years?

All companies, public and private, benefit from a sound and cost-effective system of internal controls. If a privately held company aspires to "go public," its management should consider an initial evaluation of its internal control over financial reporting to identify the company's readiness and areas that may require improvement. These areas can be addressed systematically over time rather than all at once when the company files its registration statement and is burdened with substantially more disclosure requirements and responsibilities.

248. If a private company has plans to go public sometime in the future, with plans to file an S-1 three years from now (which would require three years of audited financial statements), would three years of internal control attestation reports by its public accountants be required as well?

No. The SEC has granted relief from the Section 404 requirements for companies that are new to Exchange Act reporting. The Commission's rules provide all newly public companies, regardless of size, with a transition period that prevents them from having to comply with the Section 404 requirements in the first annual report that they file after becoming an Exchange Act reporting company. The transition period applies to a company that has become public through an initial public offering (whether equity or debt) or a registered exchange offer or that otherwise has become subject to the Exchange Act reporting requirements. It also includes a foreign private issuer that is listing on a U.S. exchange for the first time. The transition period is intended to permit newly public companies to concentrate on their initial securities offerings and to prepare for their first annual report without the additional burden of having to comply with the Section 404 requirements at the same time.

249. Should a privately held company implement provisions of Sarbanes-Oxley?

This, of course, is a choice that management of the privately held company must make. Regardless of the letter of the law, no organization can afford the reputation loss caused by misleading regulatory authorities and auditors. Fairness and integrity are fundamental to every organization's sustainability and command of the public trust. We are finding that private companies are implementing some and, in some cases, many of the provisions of Sarbanes-Oxley. Every company of significant size and complexity would benefit from effective governance. Privately held companies must meet the expectations of ownership groups, banks and other stakeholders. The current business environment should drive management of all companies and institutions, and their boards, to

take a renewed look at their governance, risk assessment and financial reporting processes to determine that they are effective, both in design and in operation. The governance process is enhanced through efforts to strengthen the control environment and create accountability. Voluntary compliers with plans to go public also reap the benefits of IPO-readiness because the transition process will be easier.

250. Assuming a June 30 year-end company goes public on September 30, 2007, is the first Section 302 certification required to be included in the first 10-Q for the quarter ended December 31, 2007, or will the company be required to certify as of September 30, 2007?

Section 302 applies to periodic reports under the Exchange Act of 1934 and is not applicable to registration statements filed under the 1933 Act. Therefore, the first 10-Q (or the 10-K, if it is the first report filed after going public) is when the executive certification requirement takes effect. In this case, the certification would first be filed in the 10-Q filed for the quarter ended December 31, 2007. With respect to these and other similar reporting matters, we advise companies to consult with legal counsel.

U.S. and Foreign Nonaccelerated Filers and Foreign Locations

251. Is Section 404 applied differently to smaller companies?

Many smaller companies generally have less complex processes, fewer layers of management and fewer operating units and locations, and therefore, less complex and formalized controls. Small- and medium-size companies often do not have the formal control structure found in larger companies. The SEC points out in its interpretive guidance that it is important to recognize what makes many smaller companies different when identifying risks. The manner in which financial reporting risks are identified will vary based on the size, complexity and organizational structure of the company, and its processes and financial reporting environment. To illustrate, in a small company with less complex business processes that operate on a centralized basis and with little change in its risks or processes, management's daily involvement with the business may provide them with adequate knowledge to appropriately identify financial reporting risks.

Furthermore, the SEC also states that management's daily interaction with its controls may provide it with sufficient knowledge about their operation to evaluate the operation of internal control over financial reporting, particularly in smaller companies. For example, ongoing direct participation in and direct supervision of control operation may contribute to this level of knowledge. Management should therefore consider the particular facts and circumstances when determining whether or not its daily interaction with controls provides sufficient evidence for the evaluation.

According to the SEC, reliance on management's daily interaction also impacts the level of documentation available. The SEC's interpretive guidance indicates that in those situations in which management is able to rely on its daily interaction with its control processes as the basis for its assessment, "management may have limited documentation created specifically for the evaluation of [internal control over financial reporting]" in addition to "documentation regarding how its interaction provided it with sufficient evidence."

How a smaller company environment will affect the audit process is unclear. A focus on principles requires auditors to consider each company's unique facts and circumstances. The PCAOB provides guidance on scalability in Auditing Standard No. 5, which includes a description of some of the attributes of smaller, less complex companies and a discussion of six areas of the audit process that are often affected by these pervasive attributes:

(1) Obtaining sufficient competent audit evidence with limited company documentation

(2) Assessing entity-level controls to sufficiently address risks of misstatement

(3) Evaluating the risk of management override and mitigating actions

(4) Evaluating controls implemented in lieu of segregation of duties

(5) Evaluating financial reporting competencies

(6) Evaluating information technology controls

In essence, the Board directs the auditor to tailor the audit of internal control over financial reporting to reflect the attributes of smaller and less complex companies. More guidance on scalability is expected later as the Board continues to work with a task force of accounting firms in identifying issues that affect the audits of smaller, less complex companies.[5]

In summary, while the concept of control activities in a small company is the same as in a larger one, the formality of the controls may be different and management (including the CFO) may be more personally involved in the company's processes. COSO has provided guidance for smaller, less complex companies to use when applying the Internal Control – Integrated Framework.

252. Can public companies rely on their external auditor to compute the tax provision and reserves included in their financial statements?

No. Public companies need to have someone in-house who at least understands the basic financial reporting principles relating to the tax area in order to ensure proper reporting, including the related risks and controls over the completeness and accuracy of the data used in the calculation and the reasonableness of the computed tax provisions and reserves. If companies have historically used their auditors to determine their quarterly and/or annual tax provisions, they should reevaluate this practice given the SEC's independence rules. As discussed in Question 221, the Commission has made it clear the auditor cannot audit his or her own work.

253. Based on experiences to date by U.S. and foreign filers, what are the lessons for companies who have just begun their compliance efforts?

Some of the key lessons relating to planning, organizing and managing the project are as follows:

- For most first adopters, the Section 404 compliance effort is a major project effort requiring a PMO. See Question 47.
- Top management support is vital. It is difficult to succeed without it.
- Engage unit managers and process owners (both in-house and outsourced) by getting them involved and holding them accountable. Communicate everyone's role up, down, across and outside the organization and monitor progress.
- Take charge of the project. Avoid such pitfalls as managing the project at too low a level within the organization, letting the project team get lost in irrelevant details and allowing key scoping decisions to remain unaddressed too long.
- Don't ignore the clock. This can be a significant effort during the first year. Start early if you can.

---

[5] At the time this publication went to print, the PCAOB released to the public for review and comment its *Preliminary Staff Views – An Audit of Internal Control That is Integrated with An Audit of Financial Statements: Guidance for Auditors of Smaller Public Companies*. Within the guidance, various scenarios are discussed and detailed examples provided for areas that have been typically challenging in a smaller, less complex company, including fewer employees, which limits the opportunity to segregate incompatible duties and functions; less complex information systems that make greater use of off-the-shelf packaged software that has not been modified; use of outside professionals to address the need for specific financial reporting competencies; and increased likelihood of less formal documentation to run the business and to support internal control. Of particular interest to the management of smaller, less complex public companies is the discussion around how the nature and extent of a company's documentation of internal control can have a significant effect on the auditor's procedures to assess internal control over financial reporting.

- Involve the external auditor at appropriate points during the process. Work with them, understand their needs and timing requirements, conduct periodic checkpoints and plan to give them sufficient time to complete their work. Recognize management must represent to the auditor that they did not use the auditor's procedures performed during the audit process as evidence for management's assertions in the internal control report.

Some of the key lessons relating to executing the project are as follows:

- Answer key scoping questions early – which financial reporting elements, which locations and units, which processes, which systems and which controls? In particular, focus on the priority financial-reporting elements, assertions and risks. Link the priority elements, processes, key assertions, risks and controls. Integrate IT risks and controls with the Section 404 assessment.
- As early as possible in the process, assess your entity-level controls, evaluate your general IT controls and plan on making fraud explicit in the assessment process.
- Inventory the company's existing controls documentation, and use process maps or other documentation to provide the most effective "walkthrough" of the critical processes. Make sure your process owners are prepared for the auditor walkthroughs.
- Pay attention to details. Read the SEC interpretive guidance and document your road map for applying the guidance. Apply the COSO framework (or some other suitable framework) as it is designed. Expect the initial annual assessment to be a learning experience. Expect to encounter "bumps" along the road; the first year is often a challenge – for everyone.
- Be sure to identify and document the key controls. These are the controls on which management relies for purposes of the Section 404 assessment. The number of key controls is the most significant cost driver of the entire assessment process.
- Define the test plan and "rules of engagement" up front. Focus on the key controls to test, define the "failure conditions," articulate testing documentation protocols and decide what to do when failure conditions are encountered. Vary testing scopes according to frequency of the control, use appropriate sample sizes to obtain a reasonable level of assurance, use competent and objective evaluators, and don't forget to conduct refresh testing updates close to year-end. Remember that you have significant flexibility in lower risk areas. The key is to balance your test plan as discussed in Question 121.
- Consider timely the nature and extent of remediation requirements. Begin the evaluation process and tackle significant design deficiencies as soon as practicable. Thoughtfully remediate operating deficiencies. Be sure to retest remediated controls.
- When documenting the assessment, address the points outlined in the response to Question 184.

254. Are foreign filers subject to the Section 302 executive certification requirements?

Foreign private issuers filing Forms 20-F and 40-F are not subject to quarterly reporting requirements.

255. Must the Section 404 documentation prepared in countries outside the United States be presented in English?

There is no SEC or other requirement to prepare all internal control documentation in English. For most companies, such a requirement would be an unnecessary burden. Typically, audit firms are able to refer work to their offices with the language skills necessary to do the required work. The capability of local management to effectively assess and conclude on the effectiveness of the processes and controls is a factor when determining whether translation is necessary. The rigor and consistency of the company's assessment approach and the tools and training supporting it also are a consideration.

If translation is deemed necessary, then perhaps only certain aspects of the documentation would need to be translated based upon importance. For example, depending on significance, an overall memorandum and selected summary schedules could be prepared in English to address matters of importance to the management of a U.S. registrant. In addition, matters requiring consolidation often require translation to the language of the reporting entity.

Foreign locations must be put in perspective as to size and risk when deciding how much of the documentation, if any, must be in English. The key is to make sure an emphasis on translation does not undermine the quality of the assessment or the implementation of controls. Indiscriminate emphasis on translation could present increased risk. For example, in countries like Japan, where the language does not translate well into English, translation would complicate the process and make it more difficult to ensure that the right risks are identified and the right controls are in place. It also would potentially limit the number of people who could be involved, as in some countries, few of the nationals may speak English or, at a minimum, be able to speak and write the language fluently, especially in a business context. This issue applies to other countries as well due to the complexities of evaluating internal control, which is difficult enough in English. Therefore, it may make more sense for multinational companies to use the language of the local country for documentation purposes, unless English is usually spoken in the business environment, e.g., Singapore.

As with so many of these types of issues, early consultation with a company's external auditor is strongly advised. This issue also underscores the value of a company's internal audit function having the appropriate language skills or being able to access a co-sourcing provider who can deliver qualified internal audit or risk and control specialists fluent in selected local languages.

256. If a foreign private issuer files financial statements prepared in accordance with home country generally accepted accounting principles (GAAP) or International Financial Reporting Standards (IFRS), with an accompanying reconciliation to U.S. GAAP, should it conduct its evaluation based on the primary financial statements or the amounts disclosed in the reconciliation to U.S. GAAP?

In these circumstances, the SEC staff has stated that the foreign private issuer should plan and scope the evaluation based upon the primary financial statements, i.e., home country GAAP or IFRS. In addition, the evaluation should include in scope the controls related to the preparation of the U.S. GAAP reconciliation because this reconciliation is a required element of the foreign private issuer's financial statements.

257. When evaluating the severity of control deficiencies, how do foreign private issuers apply the reference to "interim financial statements" included in the definition of a material weakness?

As explained in Question 109, the definition of a material weakness refers to a company's annual or interim financial statements. The SEC staff points out that the home country requirements regarding the preparation of interim financial statements vary significantly. In addition, there are no uniform requirements under the Exchange Act for foreign private issuers to file periodic interim financial statements with the Commission. Accordingly, the SEC staff has stated that the reference to "interim financial statements" in the definition of a material weakness is not applicable to foreign private issuers. However, foreign private issuers filing on U.S. domestic forms are subject to the same requirements as U.S. domestic issuers with respect to interim financial information.

258. How does a foreign private issuer treat an investee company reported in the registrant's primary statements differently than in the reconciliation to U.S. GAAP?

Situations arise when an investee company is reported in the registrant's primary statements differently than in the reconciliation to U.S. GAAP. For example, the investee company may be consolidated in the foreign private issuer's primary statements and accounted for under the equity method in the U.S. GAAP reconciliation. As stated in Question 256, management should determine the scope of its evaluation based on the primary financial statements. Accordingly, the determination as to how investee companies are included in management's evaluation of the effectiveness of internal control over financial reporting should be based on how those entities are accounted for in the foreign private issuer's primary financial statements. That said, as discussed in Question 256, management's evaluation also should consider controls related to the preparation of the U.S. GAAP reconciliation.

Glossary of Commonly Used Acronyms and Terms

Accelerated Filer – A public company that meets the SEC's accelerated filing requirements, as defined in Rule 12b-2 under the Exchange Act. It is often differentiated by having a common equity public float of at least $75 million, but less than $700 million, as of the last business day of its most recently completed second fiscal quarter, as well as meeting certain other conditions as explained in Question 245.[6]

The Act – Refers to the Sarbanes-Oxley Act of 2002. Also referred to as "Sarbanes-Oxley."

AICPA – American Institute of Certified Public Accountants.

AMEX – American Stock Exchange.

The Bulletin – Protiviti's periodic newsletter that reviews corporate governance and risk management issues. (For more information, please visit **www.protiviti.com**.)

COSO – The Committee of Sponsoring Organizations of the Treadway Commission. See Question 39 for more information.

ERP – Enterprise Resource Planning.

The Exchange Act – Refers to the Securities and Exchange Act of 1934.

FDIC – Federal Deposit Insurance Corporation.

FDICIA – Federal Deposit Insurance Corporation Improvement Act of 1991.

GAAP – Generally accepted accounting principles.

Large Accelerated Filer – A public company that meets the SEC's accelerated filing requirements, as defined in Rule 12b-2 under the Exchange Act. It is often differentiated by having a common equity public float of more than $700 million, as of the last business day of its most recently completed second fiscal quarter, as well as meeting certain other conditions as explained in Question 245.[7]

[6] This definition excludes companies that have only publicly traded debt securities, foreign governments and registered investment companies. It does not exclude foreign private issuers.

[7] Ibid.

NASDAQ – The computerized stock exchange established by the National Association of Securities Dealers.

Nonaccelerated Filer – A public company that does not meet the SEC's accelerated filing requirements, as defined in Rule 12b-2 under the Exchange Act. It is often differentiated by having less than $75 million in public float, as of the last business day of its most recently completed second fiscal quarter, as explained in Question 245.[8]

NYSE – The New York Stock Exchange.

PCAOB – The Public Company Accounting Oversight Board. Established by the Sarbanes-Oxley Act, PCAOB oversees the audits of the financial statements of public companies through rigorous registration, standard setting, inspection and disciplinary programs. For more information about the Board, see www.pcaobus.org.

PMO – Project Management Organization.

Sarbanes-Oxley Act of 2002 – Corporate governance and oversight legislation signed into law on July 30, 2002. Also referred to as "Sarbanes-Oxley" and "the Act."

SEC – The U.S. Securities and Exchange Commission.

Section 302 – Refers to Section 302 of the Sarbanes-Oxley Act, which addresses certifications by the principal executive officer (the CEO) and principal financial officer (usually the CFO). See Question 18 for more information.

Section 404 – Refers to Section 404 of the Sarbanes-Oxley Act, which addresses internal control over financial reporting.

Section 906 – Refers to Section 906 of the Sarbanes-Oxley Act, which requires an executive certification stating that a company's periodic report containing its financial statements fully complies with the requirements of Section 13(a) or 15(d) of the Exchange Act, and that the information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer. See Question 19 for more information.

Title IV – Refers to Title IV of the Sarbanes-Oxley Act of 2002.

---

[8] This definition includes companies that have only publicly traded debt securities.

About Protiviti

Business operations improvement. Transforming finance to meet increasing stakeholder and regulatory demands. Regulatory compliance. Information technology (IT) process improvement and organization effectiveness. Effective risk management strategy and implementation. Managing ever-increasing exposure to litigation. These are just a few of the many priorities that top organizations face today while continuing their efforts to grow revenues, increase profitability and gain a competitive advantage. Over the past decade, the global business landscape has become far more complex as a result of new regulatory requirements, exponential IT expansion and the resulting security issues, increased potential for corporate fraud, highly competitive markets, and heightened expectations among stakeholders for stronger corporate governance and accountability, among many other factors. As a result, management and boards must analyze carefully and understand the key organizational and market challenges – along with the related business, operational and technology risks – their companies face, and determine if they are being addressed, managed and monitored properly. To accomplish these objectives and enable them to achieve greater success, more organizations call on the risk management, internal audit and process improvement expertise of Protiviti.

Protiviti has more than 60 locations in the Americas, Asia-Pacific and Europe, and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

ABOUT OUR SOLUTIONS

We help our clients seize new opportunities for growth and profitability while protecting them from their risks by providing proven and cost-effective answers to their business challenges. Our focus is not solely on resolving risks. We look at an organization's business objectives and the multitude of issues that could hamper its success in achieving those objectives. Our solutions-based approach helps our clients understand the interdependent risks within their operating environment, including the critical technologies and processes underlying their business model. This perspective enables organizations to obtain better information for decision-making and the confidence to advance those decisions to create a competitive advantage. Our solutions help companies improve:

Regulatory, Financial and Operational Risk Management

Risks are present virtually anywhere inside an organization. Many are industry-specific, such as the regulatory concerns within financial services and healthcare. Others are common to all industries, such as supply chain capacity, financial reporting reliability, human resources availability and customer relationship integrity. We help organizations identify, prioritize and manage their risks so they can enhance performance of their processes and, ultimately, enhance and protect enterprise value. Our solutions in this space draw from our deep competencies in anti-money laundering, Basel II, capital projects and construction, credit risk management, e-discovery, energy commodity risk, enterprise risk management, financial investigations, financial process effectiveness, fraud risk management, litigation consulting, regulatory compliance, revenue optimization, Sarbanes-Oxley Act compliance, spend risk solutions, supply chain management and treasury risk management.

Technology-Related Risk Management

Effective management of technology-related risks allows an organization to innovate and advance the maturity of its business processes with confidence. We offer many solutions to help the CIO and his or her organization design and implement practical risk management practices, improve the core IT processes, manage business continuity issues, and identify the right technology road map and standards for the business, allowing organizations to push their technology to the edge and maximize enterprise value. Our solutions draw from our products and capabilities in security and privacy, continuity, change management, IT infrastructure management, program management and application controls effectiveness.

Internal Audit

Protiviti provides a full spectrum of services, technologies and skills to management, directors and the internal audit community. We provide world-class people and state-of-the-art methodologies and tools. Our network allows us to offer the right resources, at the right time, in the right place. And we offer a creative and flexible approach to quality assurance reviews, from a standard compliance report to a full transformation of organizational capabilities. We also provide ongoing assistance for internal staff and systems. Our internal audit services include audit committee advisory, co-sourcing and specialized resource enhancement, full outsourcing, technology and tool implementation, quality assessments and readiness reviews, internal audit transformation, IT audit services, and startup and development advice.

INDUSTRY EXPERTISE

Protiviti's professionals possess vertical talent and skills together with extensive experience in a broad range of industries, including the airline sector, communications, consumer products, distribution, educational institutions, energy, financial services, government services, healthcare insurers, healthcare providers, hospitality, life sciences, manufacturing, media, nonprofit organizations, real estate, retail, services, technology and utilities.

PROVEN TECHNOLOGIES

For many client engagements, Protiviti offers proprietary technology solutions, including the Protiviti Governance Portal. Protiviti also offers a variety of information solutions to help companies manage the entire information life cycle so decision-makers have the right information at the right time, including business intelligence, data analytics, contents and records management, and data management. We integrate state-of-the-art technologies to increase productivity and effectiveness, and enhance the overall value our clients receive.

The Governance Portal™

Protiviti's Governance Portal is a technology solution that addresses multiple governance, risk, and compliance (GRC) objectives, including financial reporting compliance, regulatory compliance, IT governance, operational risk, internal audit and enterprise risk management. These compliance objectives are addressed through several integrated modules, including the Governance Portal for: Controls Management, Risk Management, Incident Management, Assessment Management and Internal Audit. These modules share a common user interface, key features and common frameworks that remove redundant administrative activities, consolidate remediation efforts across various governance exercises, and provide management with holistic reporting capabilities. The result? A more sustainable, repeatable, cost-effective GRC program designed to reduce organizational risk and exposure.

THOUGHT LEADERSHIP

Protiviti continues to deliver insightful research and publications that highlight our deep competencies in internal audit and business and technology risk management. Our Guide to the Sarbanes-Oxley Act series is recognized as among the best in the industry at dissecting and analyzing the complex issues around complying with this law. Our Global Risk Barometer program is setting new standards for assessing the risk management efforts of companies around the world. Our *Guide to Enterprise Risk Management: Frequently Asked Questions* is the most comprehensive publication of its kind. Other recent Protiviti thought leadership includes *Guide to Business Continuity Management: Frequently Asked Questions, Enterprise Risk Management in Practice: Profiles of Companies Building Effective ERM Programs,* and the report on our Internal Audit Capabilities and Needs Survey.

OUR MARKET POSITION

The name Protiviti represents professionalism, integrity and independence. Unlike most other risk consulting practices, Protiviti has no affiliation with an external audit firm, nor do we provide any external audit services. This commitment to independence gives us a key strategic advantage, as we can offer the resources, quality, capabilities and expertise of any large accounting firm without regulatory or market concerns regarding conflicts of interest.

WHAT MAKES US DIFFERENT

In addition to our independence, we offer a unique resource model. We draw on the experience and knowledge of our process and industry experts throughout our practice. The deep skills and competencies of our consultants match those of the world's top consulting firms. We also are able to capitalize on Robert Half International's network of more than 500,000 variable-cost professionals worldwide.

Notes

Notes

Notes

Protiviti is a leading provider of independent risk consulting and internal audit services. We provide consulting and advisory services to help clients identify, assess, measure and manage financial, operational and technology-related risks encountered in their industries, and assist in the implementation of the processes and controls to enable their continued monitoring. We also offer a full spectrum of internal audit services to assist management and directors with their internal audit functions, including full outsourcing, co-sourcing, technology and tool implementation, and quality assessment and readiness reviews.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti.com 1.888.556.7420