



Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements

Frequently Asked Questions
Regarding Section 404
Updated to reflect the SEC's final rules

protivitiSM
Independent Risk Consulting

Business Risk

Technology Risk

Internal Audit

Table of Contents

	Page No.
Introduction	9
Applicability of Section 404 Requirements	
1. Which companies are subject to the requirements of Section 404?	10
2.* Are foreign companies subject to the requirements of Section 404?	10
3.* Does Section 404 apply to small-business issuers?	10
4. Are unlisted companies with public debt required to comply with Section 404?	10
5.* Are municipal utilities or universities that sell bonds required to comply with Section 404?	11
6.* Do banks that are already complying with the requirements of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) have to comply with Section 404?	11
7.* Does Section 404 apply to registered investment companies?	12
8. Does Section 404 apply to U.S. divisions of foreign-based companies?	13
9. Does Section 404 apply to not-for-profit entities?	13
10.* Does Section 404 apply to asset-backed issuers?	13
What is Section 404 and How Does It Relate to Sections 302 and 906?	
11.* What does Section 404 require companies to do annually?	13
12.* What does Section 404 require companies to do quarterly?	14
13.* How often must management assess internal control over financial reporting?	14
14. Is Section 404 limited to public reports for which executive certification requirements are required?	14
15.* What does Section 302 of the Sarbanes-Oxley Act require companies to do?	15
16. What does Section 906 of the Sarbanes-Oxley Act require companies to do?	16
17.* How are the requirements under Section 404 and the requirements under Sections 302 and 906 of the Sarbanes-Oxley Act related?	16
18. Is there a value proposition from a controls assessment process beyond compliance with Section 404?	18
When is Section 404 Effective?	
19.* When do companies have to comply with the Section 404 requirements?	18
20.* Why did the SEC defer the effective date of Section 404 compliance?	19
21.* 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?	19
22.* Assume Company A, which reports on a calendar year, plans to go public next year and is expecting a capitalization below the accelerated filing floor. When must it comply with Section 404?	19
23.* When is the internal control report due?	19
24. How often must the independent accounting firm attest to management's assertions regarding internal control over financial reporting?	20

* indicates new or substantially revised material (in comparison to the first edition of this guide)

Table of Contents (continued)

	Page No.
25.* As of what date is management's annual assessment conducted?	20
26.* May an issuer comply earlier than required under the final rules?	20
27.* Is a quarterly assessment required and, if so, when?	20
28.* What is the effective date of the new exhibit requirements for Sections 302 and 906?	20
29.* If management is not required to assess internal control over financial reporting now, what about the references to such internal controls in the quarterly executive certifications required by Section 302?	20
30.* Now that the SEC has deferred the timing of Section 404, should companies defer their efforts to comply?	21

What is Meant by “Internal Control Over Financial Reporting” and “Disclosure Controls and Procedures”?

31.* What is “internal control over financial reporting”?	22
32. What are “disclosure controls and procedures,” a key component of the certification requirements under Section 302?	23
33. What are examples of disclosure controls and procedures that generate required disclosures?	24
34. How should management design the disclosure controls and procedures so that the disclosure process will not become simply a ritual?	25
35.* What should the certifying officers do when evaluating disclosure controls and procedures on a quarterly basis?	26
36. How is internal control over financial reporting distinguished from disclosure controls and procedures?	28
37.* Are there examples of internal control over financial reporting that fall outside the realm of disclosure controls and procedures?	29

The COSO Internal Controls — Integrated Framework

38.* What is COSO?	29
39.* What is the Internal Controls – Integrated Framework?	30
40. How is the COSO framework applied at the entity level in a Section 404 assessment?	31
41.* How is the COSO framework applied at the activity or process level in a Section 404 assessment?	33
42. Since the COSO framework includes internal controls over operations, to what extent do these controls need to be evaluated to support the internal control report?	37
43. If a company already uses the COSO framework, is there anything more it needs to do to comply with Section 404?	38
44. Will the COSO framework on Enterprise Risk Management affect the Section 404 assessment?	38

Getting Started With Section 404 Compliance

45. How does management get started?	38
46. How is the project team formed?	39
47. How should management articulate roles and responsibilities?	39

* indicates new or substantially revised material (in comparison to the first edition of this guide)

Table of Contents (continued)

	Page No.
48. What should management consider when developing a project plan?	40
49. When planning the project, what key scoping decisions should be evaluated, and what criteria should management consider when making these decisions?	41
50. How does a company decide the “significant areas” to review for purposes of documenting and evaluating its internal control over financial reporting?	41
51. What are “control units” and why are they important?	42
52.* How does management select the control units and locations to review?	42
53.* How does management evaluate the company’s internal control with respect to unconsolidated investments accounted for under the equity method?	43
54. How should management communicate the project effort to the organization?	43
55. What steps should be included in the project plan?	44
56. To what extent can companies rely on prior controls documentation?	44
57. How should companies document and validate their assessments of internal controls?	45
58. Is there a way to estimate the effort and cost of complying with Section 404?	45
59. Will companies need to add internal resources to comply with Sections 404 and 302?	45
60. Is a cultural assessment necessary?	46

Identifying Reporting Requirements and Relevant Processes

61. Can management use a risk-based approach for determining the extent to which internal controls should be documented and validated?	47
62. What standards and criteria should be set before beginning the project?	48
63. Are all transactions evaluated in a similar manner when understanding transaction flows and the related controls?	49
64. How are the critical processes identified?	50
65. What role do process owners play?	50

Summarizing Risks and Developing Control Objectives

66. Why identify risks?	51
67. How are risks identified?	51
68.* What are control objectives and how do they relate to risks?	51
69. How are control objectives defined?	53

Identifying and Assessing Controls — Initial Annual Assessment

70.* Does the SEC provide any guidance to management for purposes of evaluating internal control over financial reporting?	53
71.* Does the SEC provide any guidance to management for purposes of documenting its evaluation of internal control over financial reporting?	53
72. How is the entity-level assessment conducted?	54
73.* How are entity-level controls validated?	55
74.* Are entity-level controls the same thing as entity-wide controls?	57

* indicates new or substantially revised material (in comparison to the first edition of this guide)

Table of Contents (continued)

	Page No.
75.* How are pervasive IT controls considered?	57
76.* What if transaction processing is outsourced?	58
77.* Where does an entity-controls review end and a process-controls review begin?	60
78. How is the activity-level assessment conducted?	60
79.* How are processes and transaction flows documented?	61
80.* What are some examples of control activities?	64
81. When should the financial reporting process (close the books) be evaluated?	66
82. What factors are considered when evaluating the design effectiveness of controls?	67
83. What factors are considered when evaluating the operating effectiveness of controls?	68
84.* What level of assurance must management attain when reaching a conclusion on the design and operating effectiveness of internal controls?	68
85. How does management define “reasonable assurance” for purposes of evaluating the effectiveness of controls?	68
86. How should control gaps be identified and summarized?	69
87.* What should be done to address control gaps if any are found during the assessment?	71
88. How does a company define a “significant deficiency” in internal control?	73
89. How does a company define a “material weakness” in internal control?	73
90.* Assume a June 30 reporting 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?	76
91. How does a company define a “significant deficiency” or “material weakness” in the so-called “soft control” areas?	76
92. What if there is a “significant deficiency” or a “material weakness” in internal control?	76
93.* 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?	76
94.* 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?	77
95. Can management rely on the self-assessments of process owners as the sole basis for rendering the annual internal control report?	77
96. 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?	77
97.* What does it mean that the Section 404 assessment is based on a point in time and why is it important?	77
98. 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?	77

* indicates new or substantially revised material (in comparison to the first edition of this guide)

Table of Contents (continued)

Page No.

Identifying and Assessing Controls — After Initial Annual Assessment

99.*	After the initial annual assessment, how does management conduct the quarterly evaluation of those elements of internal control over financial reporting that are a subset of disclosure controls and procedures?	78
100.*	After the initial annual review of control effectiveness is completed, should management assess changes to the company's risk profile on a quarterly basis?	78
101.	Will subsequent annual assessments be similar to the initial annual assessment?	79

Validation of Operating Effectiveness (“Testing of Controls”)

102.*	What approaches are recommended for “testing” the effectiveness of internal control over financial reporting?	79
103.*	Who is responsible for validating operating effectiveness?	80
104.*	What is “testing of controls”?	80
105.*	How does management test controls that do not leave a trail of documentary evidence?	80
106.*	How can inquiries or interviewing be considered “tests” of controls?	80
107.*	What is reperformance?	81
108.*	When are tests of controls performed?	81
109.*	What is a testing plan?	81
110.*	How does management decide which controls to test?	83
111.*	Why are control descriptions important and how does management know they are adequate?	84
112.*	How are inquiries, inspections and observations documented?	85
113.*	Is testing by process owners acceptable for purposes of supporting management's assertion?	85
114.*	With respect to the period between the date management completes its evaluation of operating effectiveness and year-end, what must management do to update its evaluation?	85
115.*	What should management do when exceptions are identified?	86
116.*	How is monitoring evaluated?	87
117.*	How are pervasive process controls tested?	88
118.*	How are information process controls tested?	88
119.*	How are sampling methodologies applied?	89
120.*	What if the external auditor's testing results differ from management's results?	90

Reporting

121.	How should management formulate conclusions with respect to internal control over financial reporting?	90
122.	What should be communicated to executive management, project sponsors and the board?	91
123.*	What is the internal control report?	91
124.*	When management identifies an internal 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 report?	91

* indicates new or substantially revised material (in comparison to the first edition of this guide)

Table of Contents (continued)

	Page No.
125. What are the form and content of the internal control report?	91
126.* Where is the internal control report included in Form 10-K?	91
127.* Can the results of the assessment of internal control over financial reporting affect the company's executive certification under Sections 302 and 906?	91
128. What impact would a conclusion that the internal controls are ineffective have on the company?	92

Role of Management

129.* What is the role of the disclosure committee?	92
130. What is the role of the Section 404 compliance project sponsor?	93
131.* What is the role of the Section 404 compliance project steering committee?	93
132.* 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?	94
133. What is the role of other executives?	94
134.* Who signs off on internal control over financial reporting?	94
135.* What communications, if any, are required of management beyond the executive certifications and internal control report?	95
136. What is the role of operating and functional unit managers?	95
137. Can management rely solely on self-assessments of process owners for purposes of their evaluation of design and operating effectiveness?	95
138. Can management rely on the work of the internal auditors?	95
139. To what extent can management rely on the work of the independent public accountant in making the assessment of internal controls effectiveness?	95

Role of Internal Audit

140.* What is the current status of the NYSE requirement that listed companies have an internal audit function?	96
141. What should companies do if they are listed on other exchanges? Are they required to have an internal audit function?	96
142. 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?	96
143.* What is the role of internal audit in the evaluation process?	96

Role of the Independent Public Accountant

144. When and how should the independent public accountant be involved during management's annual assessment process?	97
145.* Did the SEC provide any guidance with respect to the attestation report?	97
146. How should management prepare for the attestation process?	97
147. What internal control "design" assistance can the independent public accountant provide without impairing independence?	98
148. Can the independent public accountant perform any testing on behalf of the audit client?	98

* indicates new or substantially revised material (in comparison to the first edition of this guide)

Table of Contents (continued)

	Page No.
149.* Can the company use its independent public accountant's software and/or methodology to support management's assessment?	98
150.* Can the company engage the independent public accountant to create original documentation of its internal control over financial reporting without impairing independence?	99
151. What kind of work can management expect of the company's independent public accountant during the attestation process?	101
152.* What is the Public Company Accounting Oversight Board (PCAOB)?	101
153.* When will the PCAOB issue guidance regarding the independent public accountant's attestation requirements and standards?	102

Role of the Audit Committee

154. How and when should the audit committee be involved in management's evaluation process and in the independent public accountant's attestation process?	102
155.* What questions are audit committees asking in this initial phase of Section 404 compliance?	102

Impact on Sections 302 and 906

156.* What is the impact of the new rules on Sections 302 and 906?	103
157.* May certifying officers cite "reasonable assurance" when referring to the company's disclosure controls and procedures?	104

Other

158. What are the new filing requirements with respect to Form 10-K and Form 10-Q?	104
159.* When determining the applicability of the accelerated filing requirements under the SEC's final Section 404 rules, when is the measurement date for purposes of quantifying a company's "market capitalization"?	105
160.* 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?	105
161. 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?	105
162.* 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?	106
163.* Should a privately held company implement provisions of Sarbanes-Oxley?	106
164.* What is the impact of the various state statutes on companies complying with SOA, and do these statutes apply to nonpublic companies?	107

Glossary of Commonly Used Acronyms and Terms	108
---	------------

* indicates new or substantially revised material (in comparison to the first edition of this guide)

Introduction

In fall 2002, Protiviti published *Frequently Asked Questions Regarding the Sarbanes-Oxley Act Executive Certification Requirements*. That publication focused on the executive certification requirements mandated by Sections 302 and 906 of the Sarbanes-Oxley Act of 2002 (hereinafter referred to as the “SOA,” the “Act” or “Sarbanes-Oxley”) and required by the U.S. Securities and Exchange Commission (hereinafter referred to as the “SEC” or the “Commission”) in its rule release issued on August 29, 2002. These certification requirements have been the focal point of recent 10-K and 10-Q filings by companies in which certifying officers have made public various representations regarding, among other things, the fair presentation of financial statements and the effectiveness of disclosure controls and procedures.

Sections 302 and 906 lay a foundation for restoring investor confidence in the integrity of public reporting. Building on that foundation, Section 404 requires management to file an internal control report with its annual report. The internal control report must articulate management’s responsibilities to establish and maintain adequate internal control over financial reporting and management’s conclusion on the effectiveness of these internal controls at year-end. The report must also state that the company’s independent public accountant has attested to and reported on management’s evaluation of internal control over financial reporting. Moreover, this report must be disclosed in the company’s annual report. The SEC’s rules adopted under Section 404 also require management to disclose certain material changes to internal control over financial reporting that occurred during the most recent quarter.

For many companies, the Section 404 requirements present a challenge. As a result, many directors, certifying executives, other senior managers and even the auditors themselves have many questions as they work together to facilitate compliance with these requirements. Boards and management may need independent advisors to assist them in addressing these questions.

This updated publication is designed to help answer your questions about the sections of SOA pertaining to public reporting without you having to wade through material you already know. This information will assist Section 404 project sponsors, leaders and team members within your organization. Issue 8 of *The Bulletin*, “Internal Control Over Financial Reporting: An Update on Section 404 of Sarbanes-Oxley,” provides an executive summary of the SEC’s final rules to C-level executives and directors and the options for complying with them. (*The Bulletin* is available for download at www.protiviti.com).

The questions listed in this publication are ones that have arisen in our discussions with clients, attorneys 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 improve their executive certification process. We have also held discussions with the SEC to understand its views on key points and confirm our interpretations in certain areas. This booklet does not replace the one we issued last fall, which is still current. The rules pertaining to Sections 302 and 906 have not changed since *Frequently Asked Questions Regarding the Sarbanes-Oxley Act Executive Certification Requirements* was published. It should be noted, however, that the SEC’s proposed Section 404 rules would modify the existing requirements of Section 302, including the executive certification. These modifications would become effective when the Section 404 rules are adopted.

This publication is a second edition reflecting the effects of changes arising from the SEC’s final rules released in June 2003. It is not intended to be a legal analysis. Companies should seek legal counsel and appropriate risk advisors for advice on specific questions as they relate to their unique circumstances. Implementation of these rules will depend on the standards for attestation engagements that will be issued by the Public Company Accounting Oversight Board (PCAOB). Accordingly, a number of the issues addressed in this publication will continue to evolve. Protiviti will provide updates for material changes to these interpretations on its website (www.protiviti.com) as they become available. Companies can obtain a copy of the SEC’s final rules at www.sec.gov.

Protiviti Inc.
July 2003

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.

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 from attorneys 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 material 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 is delayed for “foreign private issuers” (i.e., non-U.S. companies that file annual reports on Form 20-F or, for Canadian companies, Form 40-F) until their fiscal years ended on or after April 15, 2005 (instead of the June 15, 2004, date applicable to most other filers). The final rules on Section 404 also reaffirmed that foreign private issuers are required to evaluate and disclose 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 small companies, including small-business issuers, 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 the larger companies have. Thus, many small companies may wait to comply with the new Section 404 rules until their fiscal years ended on or after April 15, 2005 (instead of the June 15, 2004, date applicable to most other filers). The SEC provided this extended compliance period for companies that are not subject to the “accelerated filer” rules (i.e., companies that have a public common stock market capitalization that is less than \$75 million or that otherwise qualify as “small-business issuers” eligible to file annual reports on Form 10-KSB).

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 statements for such debt are 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 executive certification and internal control requirements because the SEC has made those requirements an integral part of Forms 10-Q and 10-K (and the accompanying exhibits). Therefore, if 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 certifications and internal control report.

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, 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 be taking a fresh look at how they can improve their internal controls and governance processes and meet the needs of their constituencies.

6. Do banks 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, certain 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
- (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. 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 SEC final 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 that 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 threshold 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
- The requirement that the company state that the independent accountant that audited the financial statements included in the annual report has also issued an attestation report on management's assessment of the company's internal control over financial reporting
- The requirement that the company must provide the attestation report on management's assessment of internal control over financial reporting in the company's annual report filed under the Exchange Act

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 of SOA. 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. The institution or holding company will also have to provide the attestation report on management's assessment in its annual report filed under the Exchange Act. For purposes of the report of management and the attestation report, financial reporting must encompass both financial statements prepared in accordance with GAAP and those prepared for regulatory reporting purposes.

7. 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 SOA. 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 which 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 did 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 continue to evaluate their disclosure controls within 90 days prior to the filing date of the report, as the Section 302 certification rules originally required. 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.

8. Does Section 404 apply to U.S. divisions 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. Thus if the foreign-based company does not file such annual reports, Section 404 does not apply.

9. 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 SOA, including internal control evaluations. (See also Question 4 for applicability to unlisted companies with public debt.)

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

No. Issuers of asset-backed securities are not required to implement Section 404 of SOA. 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.

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

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

Section 404 of SOA 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 auditor to attest to, and report on, management's assessment of the company's internal control over financial reporting in accordance with standards established by the PCAOB.

Pursuant to the SEC's final 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 as criteria for evaluating 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

The final 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 an assertion by management that there are no material weaknesses in such internal control.

The new rules, as noted above, require management to disclose to the public any material weakness identified by management. The report must also 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 states in the final rules that it expects the

PCAOB to assess the appropriateness of existing audit and attestation standards and modify them as necessary. Pending further standard-setting by the PCAOB (and approval by the SEC), the Statement on Standards for Attestation Engagements No. 10 will remain the applicable standard for the required attestation. For most companies, this new attestation requirement under Section 404 expands the scope of the accounting firm's audit procedures beyond the work required solely to render an opinion on the financial statements.

12. 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 evaluations 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 evaluate 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.

The quarterly certification requirement under the Section 302 rules with respect to management's disclosure of material weaknesses to the audit committee and to the independent accountant remain in force. The SEC made clear in the final 404 rules its expectation 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 final 404 rules changed the evaluation date to "as of the end of the period" covered by the quarterly or annual report, eliminating the previously required "90 day period" (however, see comments in Question 7 regarding registered investment companies). For purposes of evaluating the effectiveness of disclosure controls and procedures on a quarterly basis, the traditional relationship between disclosure in annual reports on Form 10-K and the intervening quarterly reports on Form 10-Q will continue for domestic companies. For example, disclosure in an annual report that continues to be accurate need not be repeated. Thus 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.

13. 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).

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

Yes. The requirements of both Section 302 (executive certifications) and Section 404 (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.

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

While the final Section 404 rules were released in June, 2003, the Section 302 executive certification requirements became effective on August 29, 2002. The final Section 404 rules make important modifications to the Section 302 requirements. 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, as modified by Section 404, are discussed below. They 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 which 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, with 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. The SEC has not accepted certifications of companies that did not follow verbatim the prescribed wording (however, see Question 157).

Because portions of the required certifications that relate to the Section 404 internal control rules are not yet effective, the SEC has advised that officers should delete the text related to the new rules (as noted in Question 29). Specifically, the first reference to “internal control over financial reporting” in the fourth paragraph of the certification and the entire portion regarding the design of such controls in the fourth paragraph should be deleted until such time as Section 404 applies to a particular company.

MAKE CERTAIN DISCLOSURES – Revised 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.

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

The Section 906 certification requirement became effective immediately upon enactment of the Act on July 30, 2002. 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, and both are required even though they overlap significantly. 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.

17. 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 SOA, are inextricably linked and comprise the public reporting aspects of the Act. They are summarized on the following page:

Comparison of Sections 302, 404 and 906			
	302	404	906
When is it effective?	August 29, 2002	Fiscal years ended on or after: • June 15, 2004, for accelerated filers • April 15, 2005, 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 issued 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

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” apply 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’s material and what’s 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 issued by the SEC is that the days of ad hoc reporting and disclosure activities are over. Financial reporting processes and the related internal controls that are in place to produce reliable financial statements must be consistently performing, 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 36.

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.

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

Yes. 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 SOA and the SEC's regulations) is accomplished through well-documented and monitored processes and controls that provide 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 critical processes 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. Reduction of such risks decreases the company's exposure to the market cap declines that inevitably result from these events. Recognizing its continuing reporting obligations, management should also 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 increased 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.

When is Section 404 Effective?

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

The specific timing requirements in the final rules were 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.” These companies will be required to file a management report on internal control over financial reporting beginning in fiscal years ending on or after June 15, 2004, amounting to a delay of nine months from the September 15, 2003 effective date originally proposed by the Commission. To illustrate, calendar year reporting companies are required to file their first internal control report in Form 10-K for calendar-year 2004 filed on March 1, 2005 (60 days after year-end).

The second group of companies consists of all other issuers, including small-business issuers and foreign private issuers. For these companies, compliance is required for fiscal years ending on or after April 15, 2005. To illustrate, calendar-year reporting companies are required to file their first internal control report with Form 10-K for calendar-year 2005 filed on March 1, 2006. This additional 10-month extension (beyond the June 15, 2004, effective date for accelerated filers) enables these issuers to reduce their costs by giving them sufficient time to do the work themselves, if that is what they choose to do.

These transition rules apply to companies other than registered investment companies. Registered investment companies must comply with the rule and form amendments applicable to them beginning August 14, 2003, except as follows: Registered investment companies must 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 June 15, 2004. In addition, similar to other companies (as noted in Question 29), a registered investment company's

certifying officers may temporarily modify the content of their Section 302 certifications to eliminate certain references to internal control over financial reporting.

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

In its open meeting on May 27, 2003, the SEC staff indicated the rationale for the delay was threefold:

- First, the Commission wanted to provide companies an opportunity to complete the preparatory work that is needed to comply.
- Second, the auditors need to gear up for these new requirements.
- Finally, the PCAOB, created by Congress last summer, needs additional time to develop its rules on the independent auditor's attestation report on management's assertions on the adequacy of internal control over financial reporting, and to consider whether additional standards or guidance are appropriate.

Thus the Commission staff wanted to provide companies more time to do a thorough job. The additional time allows companies greater flexibility. For example, the activities of documenting processes and controls, evaluating control design effectiveness, validating control operating effectiveness and fixing internal control deficiencies to close gaps can now be accomplished over a longer period of time, provided that companies take advantage of the additional time.

21. 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 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 159 and 160. Market capitalization is relevant to determining whether a company is an accelerated filer. The breakpoint is \$75 million and the determination is 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 19 and 160, then the company must file an internal control report for that year and, for each subsequent quarter, conduct a quarterly evaluation for significant changes.

Smaller companies "on the bubble" during the transition period are going to have to pay close attention to this determination and be anticipatory. 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.

22. Assume Company A, which reports on a calendar year, plans to go public next year and is expecting a capitalization below the accelerated filing floor. When must it comply with Section 404?

As noted in Question 19, a company that is an "accelerated filer," as defined in Exchange Act Rule 12b-2, as of the end of its first fiscal year ending on or after June 15, 2004, must begin to comply with Section 404. At the end of its first fiscal year, a new IPO company cannot be an "accelerated filer" because (1) it will not have been subject to the reporting requirement for at least 12 months, and (2) it will not previously have filed an annual report. The result might be different for a voluntary filer that goes public.

23. When is the internal control report due?

The report is due when Form 10-K is filed for the year Section 404 is effective. This means that for calendar-year companies that are accelerated filers, the year ending 2004 is the first period management must include an internal control report in its annual Form 10-K, which must be filed by March 1, 2005.

24. How often must the independent accounting firm attest to management's assertions regarding internal control over financial reporting?

Under Section 404, the independent auditor is required to attest to and report on management's assessment annually. The attestation report would be included in the annual report.

25. 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, 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 period and were they adequate at that time?) However, to support this assessment, it is necessary to demonstrate operating effectiveness over a sufficient period of time.

26. May an issuer comply earlier than required under the final rules?

Yes. The SEC pointed out that companies may voluntarily comply with the new disclosure requirements before the mandatory compliance date. Early compliance, however, may be complicated by the potential for changing PCAOB standards and the independent accountant's willingness (or unwillingness) to issue an attestation report that is not required. Thus we expect that "early adopters" will likely not include an attestation.

27. Is a quarterly assessment required and, if so, when?

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 2004 are required to begin their quarterly evaluation of changes made during the first quarter of calendar-year 2005.

28. What is the effective date of the new exhibit requirements for Sections 302 and 906?

For filings due on or after August 14, 2003, the effective date of the final rules, a company must comply with the new exhibit requirements for the certifications required by Sections 302 and 906 of SOA and changes to the Section 302 certification requirements in its periodic or annual reports, as further explained in the response to Question 156. Thus, filings for periods ending June 30, 2003, and thereafter will need to comply with the new exhibit requirements. Although not required, the SEC encourages companies filing reports due prior to the effective date of the new rules to file Section 906 certifications as exhibits.

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

As noted in Question 15, the executive certification makes references to internal control over financial reporting. The SEC's final 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, 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.

This transition is intended to account for the difference between the compliance date of the rules relating to internal control over financial reporting and the effective date of changes to the revised language of the Section 302 certification. However, while this extended transition period allows companies to exclude this language 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 weakness in internal control, as well as any fraud involving employees who have a significant role in internal control.

30. Now that the SEC has deferred the timing of Section 404, should companies defer their efforts to comply?

By deferring the effective date, the SEC intended to provide companies more time to do a thorough job. Companies should think through what they need to do and why. For example, what does management want to accomplish this year and why do they want to accomplish it? What is the external auditor's deadline going to be next year for completing the evaluation? What external message is management planning this year? How can management accomplish the project and the attestation process more cost-effectively now that there is more time?

Many companies are planning to complete the evaluation of "control design effectiveness" this year, so that next year they can focus on evaluating the effects of change on design. These companies are also planning to spread the effort to validate "control operating effectiveness" over this year and next year. For example, they may test critical financial processes, ERP systems and the financial close process starting this year and branch out to other processes next year. This approach will lead to correction of significant control design deficiencies this year and provide added time to thoughtfully remediate control operating deficiencies.

We see other companies "staying the course" with their plans as if they will "early adopt." These companies will have the option to issue an internal control report in this year's 10-K (in most instances, without an attestation). The SEC allows early adoption.

Following are points for management to consider:

- What message does management want to deliver to shareholders, analysts and others about the company's compliance status and commitment to fair financial reporting? Companies have an opportunity to send a positive message about their commitment to these issues.
- What is the timeline the company will follow? What milestones will management use to monitor progress? How will management define and evaluate "success"?
- What is the external auditor's deadline going to be next year? For 2003, most Big 4 firms told their clients to have everything documented for their attestation process by no later than the end of the third quarter. While companies will want to confirm timing with their auditors, it is unrealistic for companies to expect their auditors to perform the required work in the fourth quarter next year. The resulting activity spike would increase audit costs substantially. A more rational approach would be for companies to "stay the course" and spread the work over the rest of 2003 and into 2004 so that the auditor can start the attestation process earlier next year.
- Management should take advantage of the additional time to improve the company's entity-level analytics and metrics. The stronger management's monitoring processes, the less detailed testing of controls is needed.
- One way to take advantage is to "early adopt," which positions a company to deliver a proactive message to the Street that it is in compliance with Section 404. Companies that early adopt are those that "stay the course" and complete the evaluation and implement remedies to fix internal control deficiencies this year in sufficient time to demonstrate that the improved controls are operating effectively. These companies will be in a position to file an internal control report without an attestation. This approach

would be no different than the current practice of filing a statement of management's responsibility for financial reporting and internal control; however, the report would address the specific points required by the SEC, with the exception of referring to the auditor's attestation. For companies planning to "early adopt" by issuing an unattested internal control report, we recommend that they consider the feasibility of engaging their independent accountants to review, at a minimum, their documentation of controls design and their plans for testing controls.

- Companies need to remember that Sections 302 and 906 are still in force. If there are significant deficiencies in internal control not known to management, staying the course will help get them surfaced so they can be corrected in a timely manner.

Following is advice to public companies provided by a senior representative of the SEC in May 2003:

If you have not yet started to prepare for the internal control evaluation, begin working on it immediately. The need to document the existing internal controls, consider whether other controls should be added, and design and perform tests of controls, indicates that a lot of time is necessary in order for management to be in a position to conclude as to the effectiveness of the company's internal control over financial reporting. Please do not use the extension of the compliance date as a reason to relax, take your eye off the ball, or otherwise not make use of the extra time you've been given. We listened to your concerns about timing, and we believe we've done our part to ensure an effective and smooth implementation of the rules, which is in the best interests of investors. If you don't take advantage of this extra time to work on the implementation, you will not have done your part for investors.

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

31. 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 picks up language from SOA 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).

32. What are “disclosure controls and procedures,” a key component of the certification requirements under Section 302?

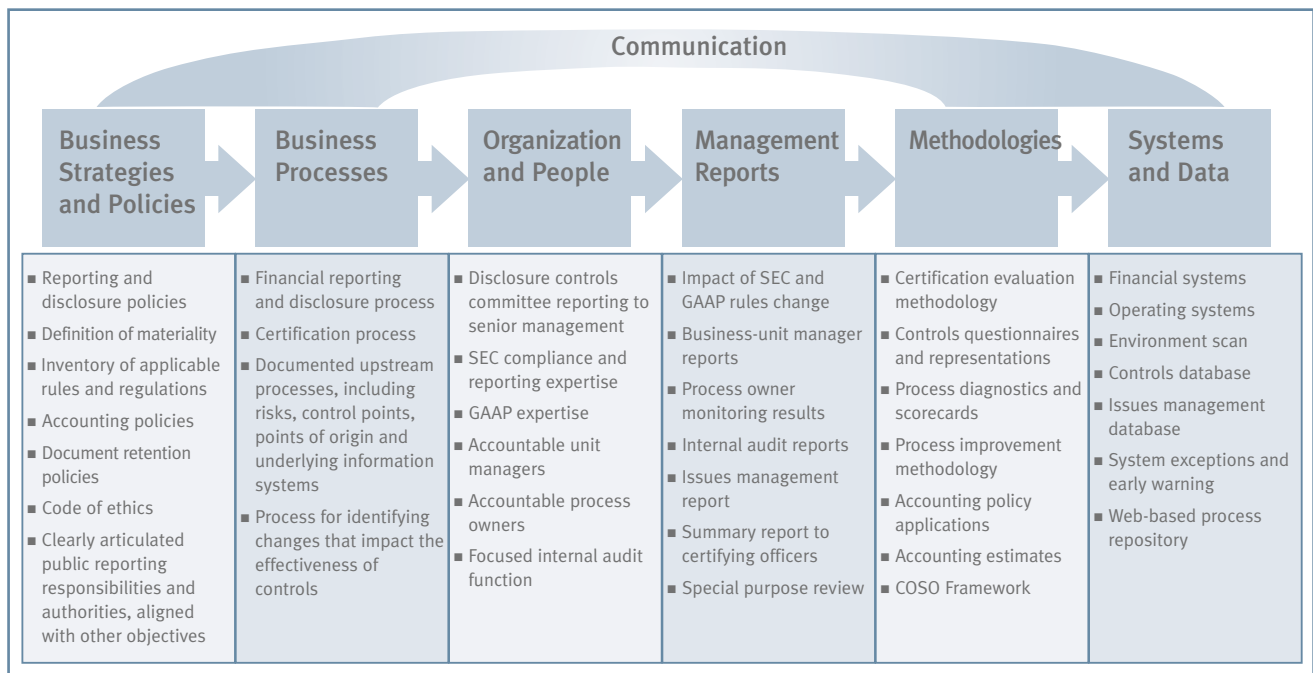
The SEC introduced “disclosure controls and procedures” as a new term in its August 29, 2002, release. Disclosure controls and procedures are controls and other procedures that are designed to ensure that information required to be disclosed by the company in its Exchange Act reports is recorded, processed, summarized and reported within the time periods specified in the Commission's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by the company in its Exchange Act reports is accumulated and communicated to the company's management (including its principal executive and financial officers) for timely assessment and disclosure pursuant to the SEC's rules and regulations. 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 nonfinancial 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 33, 34 and 35.

33. 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. 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 quality material information is disclosed in a timely manner to management for potential action and disclosure. See Question 129 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. A standard reporting package is a common practice followed by many companies. We see companies enhancing these reporting packages to facilitate upward communications of material information from unit managers and process owners by 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 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 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.
- Establish 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 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.
- 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.

34. 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.

- 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.
- 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. 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.

35. 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 are not changed by the new rules on Section 404. 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 weaknesses, the impact of changes from prior periods and other areas of concern representing changes from the annual report. 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 quality 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 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.

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

- Identify critical processes that require immediate evaluation to ensure the underlying controls are adequately designed and operating effectively. A diagnostic should be performed on critical processes that require immediate assessment 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 non-routine activities that take place in that process.
- Document the critical 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 significant processes should be documented over time, depending on management's assessment of criticality. As each 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 the internal control rules, the SEC points out that companies should maintain evidential matter, including documentation, to provide a reasonable basis for management's conclusions. It seems reasonable 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 the report, 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 possibility for significant errors or omissions, i.e., 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.
- 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?

36. 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 (e.g., reasonable assurance that receipts and expenditures are made only in accordance with management and board authorization) that do not directly relate to disclosure.

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

MANAGEMENT MUST:	REQUIRED BY:	
	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 non-financial 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 404 and 302 through common and interfacing processes	Substantially overlaps disclosure controls and procedures	Includes many elements of internal control over financial reporting
REPORT to the public	Internal control report	Officers' certification

37. 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 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 Controls — Integrated Framework

38. 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 final rule, 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 the final rule 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 two documents, one in 1992 on the Internal Controls – Integrated Framework, and the other in the mid-1990s on derivatives.

39. What is the Internal Controls – Integrated Framework?

The COSO Internal Controls – 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 cube below, 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).

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.

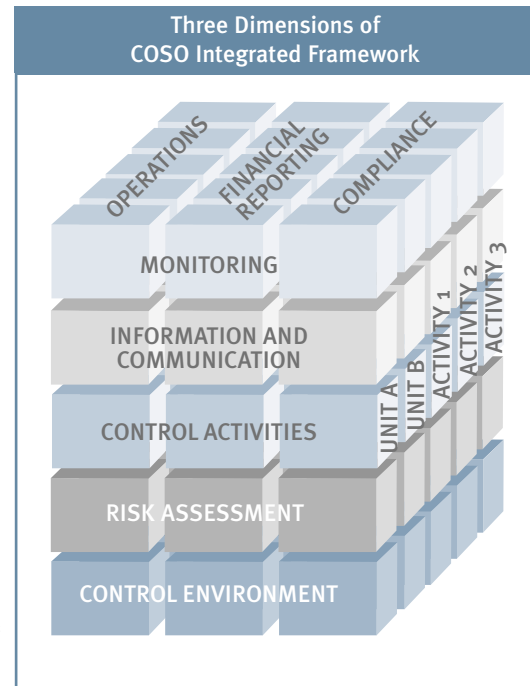
The third dimension includes the five components of internal controls (bottom to top, on the face of the cube):

- 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 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 embraces COSO. Banks complying with FDICIA (see Question 6) have used COSO.



Source: COSO Internal Controls – Integrated Framework

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, management should "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.

40. How is the COSO framework applied at the entity level in a Section 404 assessment?

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.

At the entity level, management must address the various attributes COSO provides for each component. The illustration below 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 Component	Attributes	Points of Focus
Risk Assessment	<ul style="list-style-type: none"> Entity-wide objectives Activity-level objectives Risk identification and assessment Managing change 	<ul style="list-style-type: none"> Are there policies, procedures and effective processes for hiring, compensating, promoting, training and terminating employees?
Control Environment	<ul style="list-style-type: none"> Integrity and ethical values Commitment to competence Board of directors or audit committee Management's philosophy and operating style Organizational structure Assignment of authority and responsibility <u>Human resource policies and practices</u> 	<ul style="list-style-type: none"> 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?
Information and Communication	<ul style="list-style-type: none"> External and internal information is identified, captured, processed and reported Effective communication down, across, up the organization 	<ul style="list-style-type: none"> Are employee retention and promotion criteria clearly defined, and is the performance evaluation process effective?
Control Activities	<ul style="list-style-type: none"> Policies, procedures and actions to address risks to achievement of stated objectives 	<ul style="list-style-type: none"> Does management take appropriate remedial action in response to departures from approved policies and procedures?
Monitoring	<ul style="list-style-type: none"> Ongoing monitoring Separate evaluations Reporting deficiencies 	<ul style="list-style-type: none"> 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?

Source: COSO Internal Controls – Integrated Framework, Framework and Evaluation Tools

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 resources 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 might include (not intended as all-inclusive):

- 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 above illustration:

- 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 above, 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.
- 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, 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 51 and 52), 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.

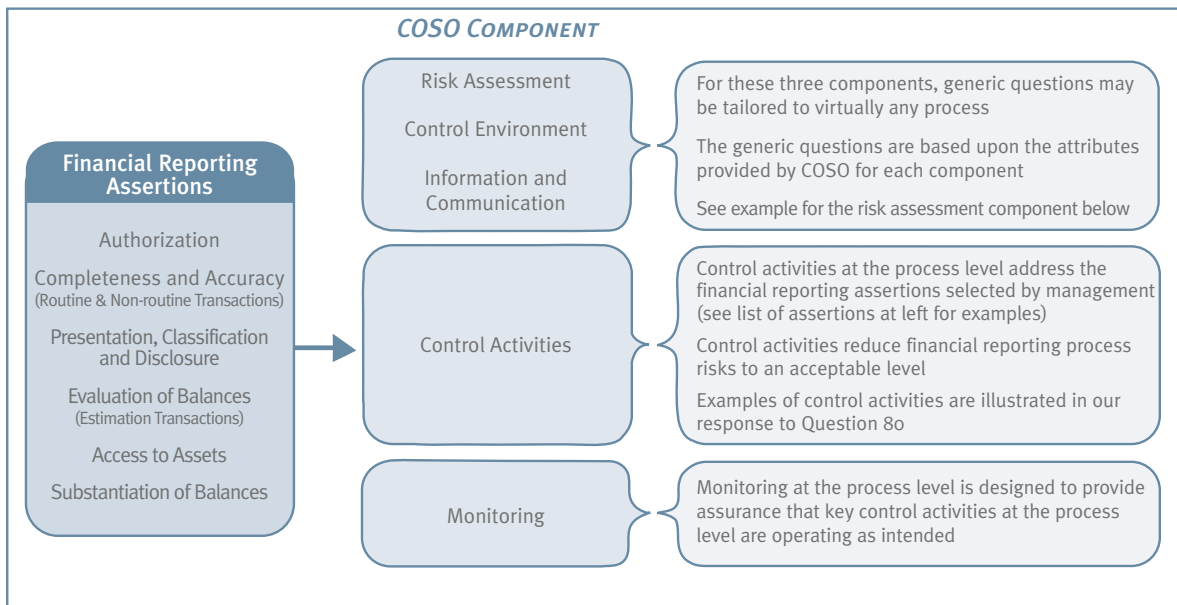
For example, consider a reporting entity with several highly autonomous operating units included in its consolidated statements. Assume that each of the operating units represents a control unit along with the reporting entity. For purposes of assessing the control environment:

- 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 different risks inherent in those operations and business units, and other factors impact the project team’s approach to assessing the entity-level controls.

41. How is the COSO framework applied at the activity or process level in a Section 404 assessment?

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 illustrated on the following page:



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 67 and 68 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 errors and irregularities 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 67 and 68 for examples). Control activities should be in place within the process to reduce “financial reporting process 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** focuses 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.

The control activities in place should provide reasonable assurance that management’s financial reporting objectives or assertions are met. Management must evaluate the design and operational effectiveness of the control activities:

- 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 80.

At the process level, monitoring addresses 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 consists 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 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 resolved in a timely manner.

The above 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 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:

- 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:

- 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.

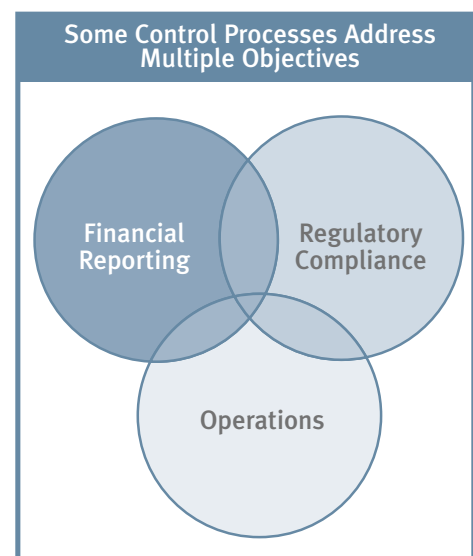
Following are appropriate questions:

- 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?

42. Since the COSO framework includes internal controls over operations, to what extent do these controls need to be evaluated 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 at right). For example, defining processes, documenting procedures and supervising activities are examples of operational controls that may also be relevant to financial reporting activities. Further, 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.

Management may choose 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. (See Question 18.)



43. 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.

44. Will the COSO framework on Enterprise Risk Management affect the Section 404 assessment?

No. COSO's forthcoming Enterprise Risk Management Conceptual Framework will not replace the Internal Controls – 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

45. 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 of those resources, both internal and external. A team leader, such as the chief accounting officer or corporate controller, should also be appointed.

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 carefully considered 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 public accountant to perform the attestation work. For a company with a December 31 year-end for reporting purposes, this probably means completing the project during the third quarter or earlier. Before the SEC delayed the effective date of Section 404 compliance, we were aware of instances where a company's independent public accountant has requested management to complete the documentation, assessment and validation by at least five months prior to year-end. It is possible that with the deferral the auditor may request an even earlier deadline. Regardless of the specific deadline, management must back up from that date for planning purposes and allow for sufficient time and resources to complete the project. 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 among 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. 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 67 and 68 for examples of common language of risks or assertions. See Questions 63 and 64 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 49.)
- 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. (See Questions 55 and 56.)
- Define the control units by which to break down the organization for purposes of evaluating entity-level and process-level controls. (See Questions 51 and 52.)
- 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.
- Agree on control framework by which management will evaluate effectiveness. (See Question 39.)
- Validate approach and requirements with the independent public accountant to ensure everyone is in agreement. (See Question 144.)
- Define internal communication plan for management to execute during the project. (See Question 54.)

46. 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, 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 project management office supported by 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 130, may chair this committee. The project leader reports to this committee.

47. 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 48, 49, 50 and 52 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.

48. What should management consider when developing a 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. These points 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, timely 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.

49. 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. For example, following are factors to consider when determining key financial reporting elements:

- Nature and types of errors and omissions that could occur, i.e., “what can go wrong”
- Nature, size and composition of an account or group of accounts (e.g., revenue and receivables)
- Volume, size, complexity and homogeneity of the individual transactions processed through a given account or group of accounts
- Materiality and significance of possible errors and omissions to investors
- Susceptibility to error or omission as well as to manipulation or loss
- Robustness versus subjectiveness of the processes and methods for determining significant estimates
- Problem areas from prior years that may require attention during the assessment
- The 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
- Extent of 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, etc.
- Independent public accountant expectations and requirements

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 IT systems and components of the IT infrastructure to consider.

With respect to documenting the 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 flows, inter-functional process analysis, and procedural and process narratives.

50. 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 49), 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. Prioritization is based on the risks there are significant errors that, individually or combined, could have a material effect on the financial statements. The areas of greatest risk for material financial misstatements or untimely disclosure should also be identified, e.g., revenue recognition, loss contingencies, capital expenditures, etc. Input should be obtained from management and the audit committee, with management approving the results. The results of this exercise should be validated with the independent public accountant.

51. 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, and operating styles. 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 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.

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. 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 materiality must be considered when planning the controls assessment.

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

Once the organization is broken down into separate control units, the relative materiality of the various units should be evaluated to determine those units that should be included in the scope of the controls assessment. It may not be necessary to assess the controls at every control unit or at each location of the company. However, those units or locations excluded from the assessment scope should be clearly immaterial, both individually and in the aggregate.

Management must first determine the appropriate criteria for this evaluation. Examples of two primary criteria are:

- Relative significance of assets and contributed sales and profits at each unit and location. For many companies, the individually important business units or locations often represent a relatively small number of units or locations that encompass a large portion of the consolidated entity’s operations and financial position.
- Existence of significant risks. 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 material misstatement of the consolidated entity’s financial statements. For example, a global trading unit managing currency, commodity and other financial risks for the enterprise as a whole may present unique risks not found in the operating units.

The above two criteria carry substantial weight in the selection process. Other criteria may be used to select additional units and locations that are not individually important or do not present significant risks. These criteria may be used to select additional units and locations so that there is sufficient coverage of the consolidated entity’s operations and financial position:

- Consistency of operations, transaction processing and the control structure across units and locations, including the existence of shared services operations
- The extent to which transactions affecting a significant account or group of related accounts (e.g., receivables and sales) are dispersed across many units and locations
- The extent to which the accounting records and systems are centralized

- The decision-making authority of a given unit or location, e.g., can it create obligations on behalf of the reporting entity or encumber significant assets of the reporting entity?
- The potential for surprise, e.g., a unit may be immaterial based on traditional financial measures, but through its actions or inaction can have a huge impact on the organization, such as involvement in a catastrophic environmental disaster
- The existence of effective entity-level monitoring and analytics that are entity-wide in scope, and that provide reporting entity management with sufficient transparency as to whether key controls are operating effectively and whether what is reported is consistent with economic reality
- Potential for surprises at a given unit or location, including exposure to significant future changes in operations or other factors, which could impact controls
- Previously identified internal control issues

Once the criteria are determined, management should select the most significant control units and locations for purposes of assessing controls. Needless to say, the process involves judgment. Once the units and locations are selected, management should document the supporting rationale and obtain concurrence of the independent public accountant.

The overall process is similar to how independent public accountants decide which units and locations to visit when evaluating scopes for financial statement audits. The independent auditor will often differentiate scopes at various units and locations that are considered significant. For example, some units and locations may be so material to the reporting entity, the company must document and assess the processes, risks and controls for all significant accounts. Other units and locations may warrant a conclusion to document and assess the processes, risks and controls for selected accounts. With respect to the units or locations excluded from the assessment scope, management should be satisfied that they should be unable, individually or in the aggregate, to create a material misstatement in the financial statements.

53. How does management evaluate the company's internal control with respect to unconsolidated investments accounted for under the equity method?

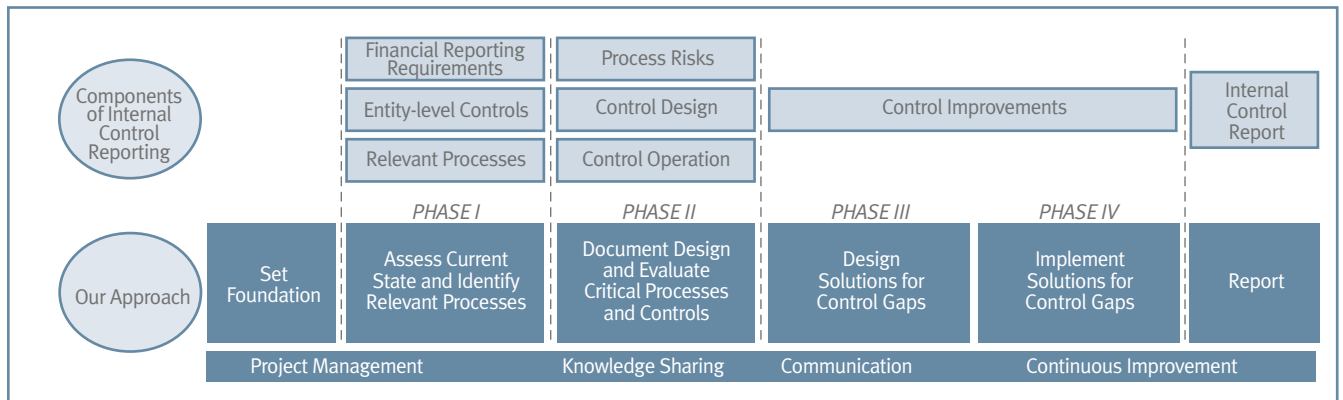
Assume Company A, an issuer with listed stock, owns 25 percent of Company B, a private company, and accounts for its investment using the equity method. If Company B's statements are audited, the management of Company A should focus on ensuring the company's investments in this unconsolidated entity 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. 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.

54. 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 through the duration of the project. When designing and implementing an internal communications plan, keep in mind that the objective is to build stakeholder commitment. 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.

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

The project plan should be a phased approach, as illustrated below:



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 from public report requirements, inventories available internal controls documentation, documents the financial close process, and develops a critical process scorecard (see Question 56 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, assesses the effectiveness of control design, validates and tests effectiveness of control operation, summarizes results, and develops action plan for improvements.

Phase III (Design solutions for control gaps) – Designs process improvements to facilitate management reporting and issues management, align objectives with corporate governance guidelines, and identify changes that impact controls. In this phase, the project team designs the revisions needed to improve 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 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. The suggested approach above should address both the initial annual assessment and the ongoing assessment. Management must evaluate internal control over financial reporting on a quarterly basis in the years following the initial annual 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 change each quarter, e.g., changes in processes, systems, operations and other factors.

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

If controls documentation exists, it should be used if it is current and complete. 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, 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, e.g., procedures, policies, maps and risks.

57. 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 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 walk-through of the process using the relevant documents is an effective method of ascertaining the procedures and controls as they really function. (See Questions 102 through 120 for guidance with respect to validating operating effectiveness of internal controls.)

58. Is there a way to estimate the effort and cost of complying with Section 404?

Estimates are hard to come by without some analysis. Ultimately, the effort and cost is a function of the number of entities 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) deciding on scoping decisions with respect to the appropriate control units, priority financial reporting elements and processes, key locations, and IT systems and infrastructure; (b) inventorying the existence of current policies and procedures and quality process and control documentation; and (c) determining the nature of the control gaps that exist and must be corrected. Once resource requirements are estimated, management must decide the extent to which internal resources are available. The complexity of the organization and its underlying processes must also be considered.

Referring to the approach in Question 55, the project team should first complete both Set Foundation and Phase I before committing to an estimate.

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

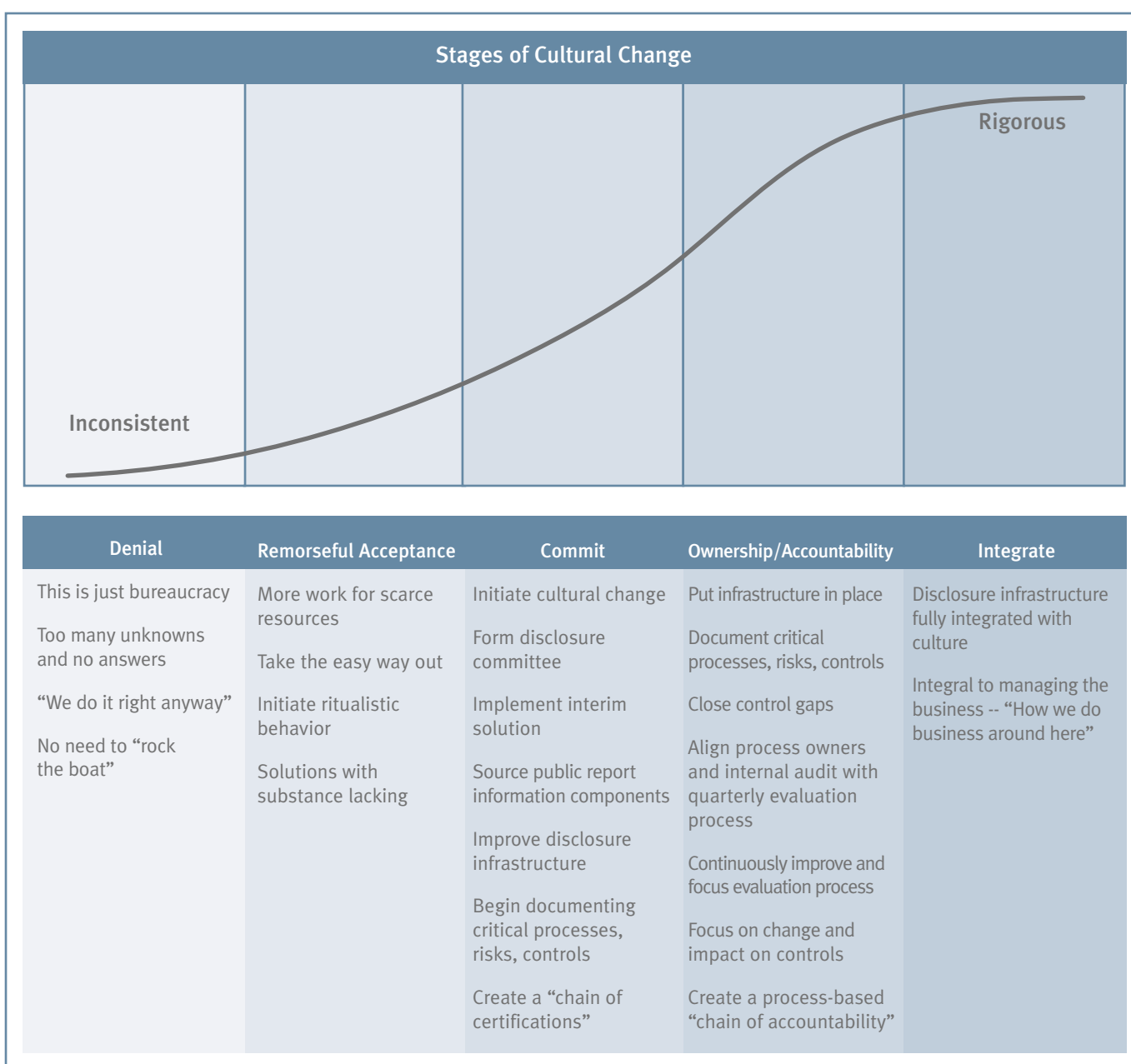
Not necessarily. With respect to the initial annual assessment, external resources may be used to supplement gaps that internal resources are unable to address. The key is to deploy qualified resources with the requisite knowledge of processes, risks and controls as well as appropriate knowledge of the Sarbanes-Oxley Act and its specific requirements related to internal controls and procedures. 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 and internal audit, to execute it.

60. 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:



When Sarbanes-Oxley was passed, many companies 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 have formed a disclosure committee. Some companies created a chain of certifications (see Question 99 for explanation). Others began documenting their processes, such as the financial close process.

The Section 404 compliance process should result in further movement 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. If Section 404 is implemented effectively, process-owner monitoring and internal audit plans will be aligned with the certifying officers’ quarterly process to evaluate disclosure controls and procedures, resulting in a process-based chain of accountability. If 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.

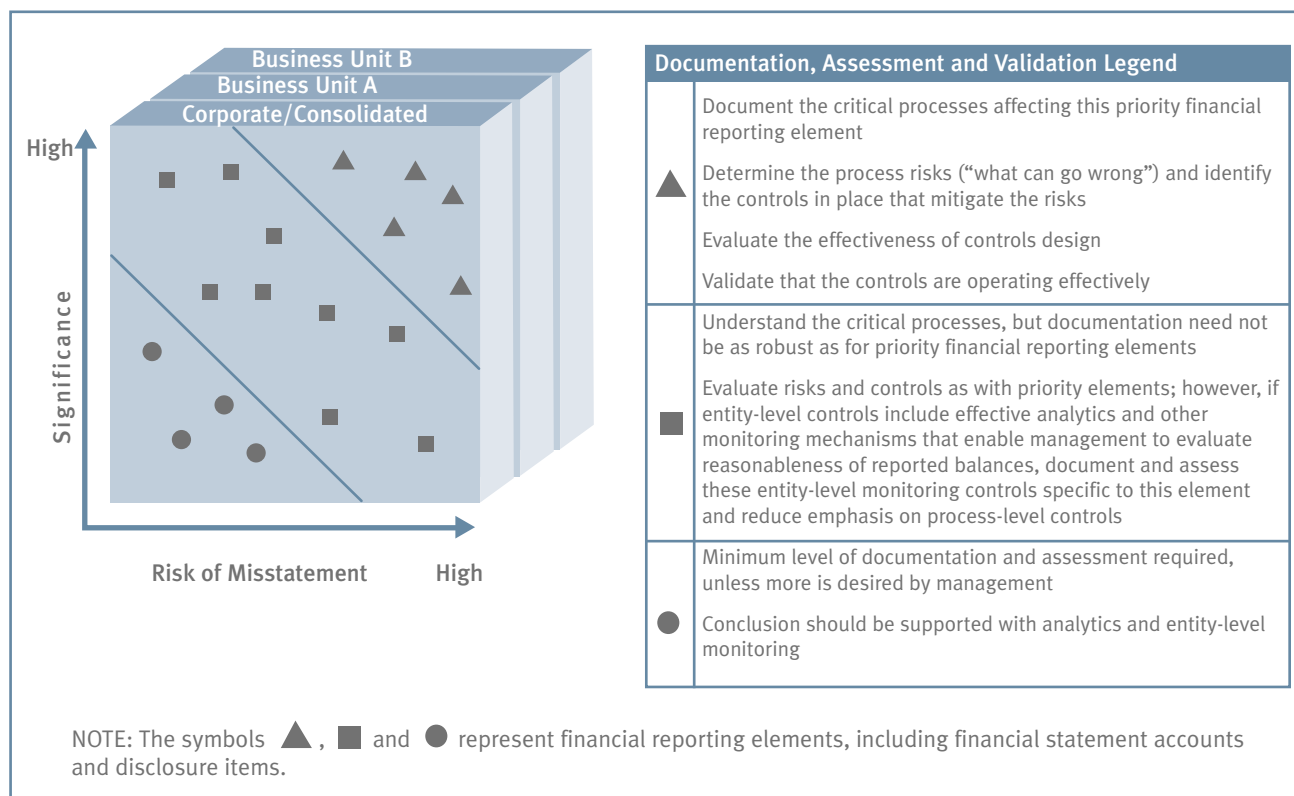
A cultural assessment survey could be useful in evaluating what stage a company is at, as well as checking its preparedness for compliance with Section 404.

Identifying Reporting Requirements and Relevant Processes

61. Can management use a risk-based approach for determining the extent to which internal controls should be documented and validated?

Yes. A risk-based approach is the most practical way to evaluate internal controls. It is a top-down approach that begins with selecting the most significant captions and disclosures from the financial statements. That accomplished, the project team then determines (a) the transaction flows that impact the priority captions and (b) the information processes that generate the required disclosures.

The following framework may be useful for illustration purposes.



Prioritization of financial reporting elements is accomplished by evaluating two things:

- First, the significance of the account or disclosure to the reporting of financial position, results of operations and cash flows. When evaluating significance, consider materiality and the importance to fairness of presentation and to a full understanding by investors of the financial statements.
- Second, the risk of misstatement or omission. 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 ability to predict results reliably and detect error through monitoring or analytical activities, the volume and size of the individual transactions processed through a given account, the complexity of calculation, and the susceptibility to material error or omissions or manipulation or loss.

Other factors to consider when prioritizing financial reporting elements include:

- Robustness versus subjectiveness of the methodologies determining significant accounting estimates
- Extent of change in the business and its expected effect on internal controls
- 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, etc.
- Problem areas experienced by the company or commonly experienced within the industry, e.g., revenue recognition
- Desire by management to document those processes affecting key accounts that may not be susceptible to significant misstatement and are reasonably predictable. For example, payroll is reasonably predictable for most companies, but it is a significant amount in cost of sales and in selling, 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.

Once the financial reporting accounts and disclosures are prioritized, plan the appropriate documentation, assessment and validation activities. The preceding illustration includes a sample documentation, assessment and validation legend. The high-priority financial reporting elements are given the most attention. Less significant elements require less work if effective analytics and entity-level monitoring provide reasonable assurance that the accounts and disclosures are fairly stated and presented. Insignificant elements require a minimum level of documentation.

Keep in mind three points:

- The illustration is just an example. Management and the project team must work out the method by which to prioritize financial reporting elements.
- Use “groups of 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 affected by routine revenue transactions.
- Last, but certainly not least, understand the independent public accountant’s expectations and requirements. A scoping exercise is only as good as the independent accountant’s concurrence with the result.

62. 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? 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 Question 49.)

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

An understanding of the major transaction flows enables the project team to identify the processes relevant to financial reporting. It is within these processes where significant errors or omissions might occur. Thus an understanding of the flow of major transactions provides the foundation for an 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 *non-routine* transactions and transactions from *accounting estimates*. 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, 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, 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. 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 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 *non-routine* transactions and transactions arising from *accounting estimates*. Unusual transactions include mergers, acquisitions, divestitures, plant closings, extraordinary items, disposals of a segment of a business and other transactions that occur infrequently. Non-routine transactions are transactions that occur periodically, generally in conjunction with calculations by accounting personnel at month-end. Examples include calculations of income taxes, accrued interest on investments and loans, accrued liabilities for goods and services received but not invoiced, prepaid expenses, and liabilities for advance payments for services not yet delivered.

Transactions arising from accounting estimates often 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 non-routine 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 non-routine 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 non-routine 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.

64. How are the critical processes identified?

Once the key financial reporting elements are determined, management must identify the processes affecting them. The processes that 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 control weakness or a process issue. 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 requirements and documents processes as they are defined in the business.

65. 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 that makes the 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

66. Why identify risks?

An 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 downstream in the process are “detective” controls. Whether preventive or detective, controls are evaluated in terms of their effectiveness in reducing the process risks to an acceptable level.

67. How are risks identified?

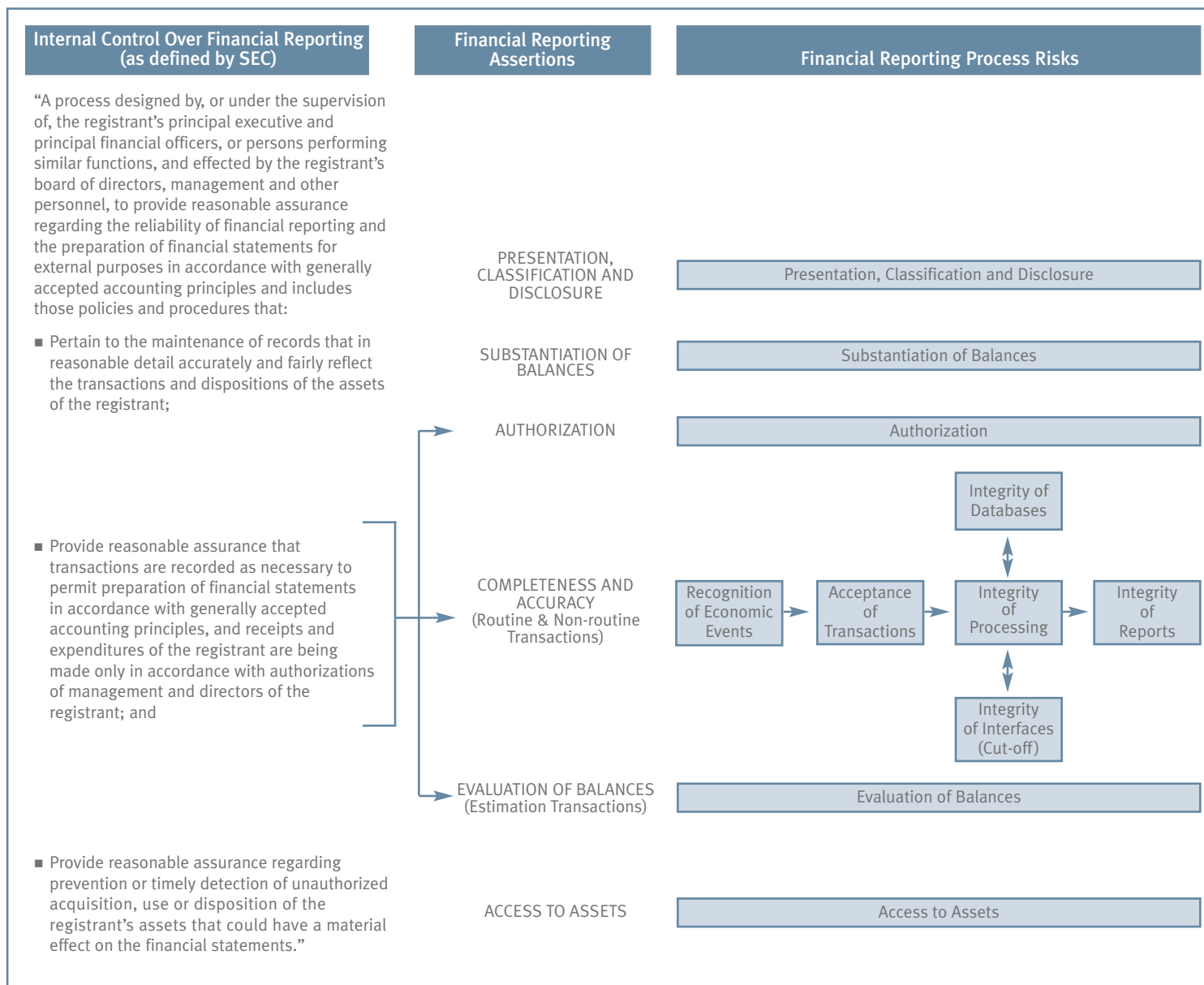
Risks are identified using objectives as a framework. When evaluating internal control over financial reporting, these objectives are sometimes referred to as assertions. For example, COSO provides the following assertions that underlie an entity’s financial statements:

- **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 63 and 64), the project team should identify 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 non-routine transactions and transactions arising from accounting estimates, the team should examine the underlying methodologies, assumptions, supporting data sources and review processes. The above assertions (or alternative assertions – see Question 68, for example) are used to identify points within the transaction process, estimation methodology or disclosure generation process where things can go wrong. These sources of risk provide the focal point for evaluating controls to provide reasonable assurance that the assertions are being met.

68. 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 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 illustrated on the following page, 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, 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.

For examples of financial reporting assertions from the COSO framework, see Question 67.

69. How are control objectives defined?

Our responses to Questions 67 and 68 illustrate the use of financial reporting objectives for purposes of focusing an evaluation of internal control over financial reporting. 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, compliance with applicable laws and regulations, and risk management.

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 identify performance gaps.

Identifying and Assessing Controls – Initial Annual Assessment

70. Does the SEC provide any guidance to management for purposes of evaluating internal control over financial reporting?

Yes. While the final rules do not specify the method or procedures to be performed in an evaluation of internal control over financial reporting, the SEC provides 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, 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 non-routine and non-systematic 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.

Due to the general nature of this guidance, management should develop a comprehensive testing plan, as further discussed in Question 109, and review that plan with the independent auditor.

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

Yes. While the final rules do not specify the method or procedures to be performed in documenting an evaluation of internal control over financial reporting, the SEC provides 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 is being added to new Item 308 of Regulations S-K and S-B and Forms 20-F and 40-F to remind registrants to maintain such 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 independent accountant that is required to attest to, and report on, management's assessment of the effectiveness of the company's internal control over financial reporting also will require that the company develop and maintain such evidential matter to support management's assessment. Thus it would be wise to obtain input from the auditor at an early stage of the project regarding documentation standards.

72. How is the entity-level assessment conducted?

An entity-level assessment should be conducted as early as possible in the evaluation process. 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, 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.

A determination that the entity-level controls are weak can 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 controls will drive an increase in reliance on process controls and an increase in testing requirements.

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

Customize entity-level 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 are a framework for evaluating internal control over financial reporting at the entity level. In our response to Question 40, 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.

Assess 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 51 and 52 for explanation) within the organization, interviews should be conducted with unit management to assess the entity-level controls. For the various points of focus, 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 controls in place at the entity level.

Gather supporting evidence – An overall assessment of entity-level controls is 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 controls at the entity level, 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 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. The project team should develop and execute a plan to obtain, document and assess relevant supporting evidence of controls at the entity level.

Evaluate impact on process-level controls – When all assessments are completed, management evaluates the combined results and concludes as to the effectiveness of each of the COSO components comprising the overall entity-level controls. 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 40 for further explanation). Overall results and documentary evidence should be validated (see next question).

Based on the results of the assessment and validation activities, a conclusion that the entity-level controls are effective may reduce the need to document processes, risks and controls in less significant areas that are not susceptible to material misstatements. 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.

When the entity-level review 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.

73. How are 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 management control structure. Validation is not a one-time event but a continuous and ongoing process and, depending upon the nature of the control, a judgmental process.

How does the project team validate the “soft controls” that often define the control environment as part of the entity-level controls evaluation? Granted, it is difficult to perform an objective test of “tone at the top” type controls. This is why the external auditor probably will not rely on management’s validation of operational effectiveness of these controls. There is too much subjectiveness 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:

- Are they comfortable with their control environment?
- What are the hard spots and how do they know?
- What are the soft spots and can they be corrected? If so, when?

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 these controls.

- There are four types of testing – inquiry, observation, inspection and reperformance. Reperformance is rarely an option at this level, so 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 does at the entity level.
- Management should only choose to validate areas where validation is appropriate. It is not necessary to validate every single control at this or at any other level.

- One approach to validation at this level, and one that the external auditor will possibly use, 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 toward financial reporting and compliance with SOA, etc. The absence of warning signs says a lot about management's philosophy and operating style, commitment to ethical values and other "tone at the top" values.
- 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.
- Still another option is to use survey instruments in selected areas. For example, to validate commitment to ethical values, surveys of employees 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.
- 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 ethics, board minutes, conflict-of-interest policies, HR policies, etc.
 - 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
 - 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 entity level (see Question 40 for an explanation of these terms), but rather only those responses considered most significant to management's overall conclusions. 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, 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.

74. Are entity-level controls the same thing as entity-wide controls?

No. Entity-wide controls include entity-level controls plus controls over processes that are entity-wide in scope. For example, entity-wide controls include:

- The control environment, including the assignment of authority and responsibility, consistent policies and procedures, and entity-wide 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 financial reporting process

75. How are pervasive IT controls considered?

Computer operations, physical and logical security, program change, systems development, business continuity and similar controls are examples of pervasive IT controls. These IT controls are “pervasive” because they impact the achievement of financial control objectives across multiple processes through the related application systems at the process level. Pervasive IT controls in financial reporting are designed to ensure that:

- Changes to application systems (through systems development, upgrades and maintenance) are authorized, tested and approved before they are implemented, which directly relates to the authorization, completeness and accuracy, classification, and access to assets assertions.
- Segregation of incompatible duties and security over 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 relates to the authorization and access to assets assertions.

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.

The assessment of pervasive IT controls is illustrated below:

Tailor pervasive IT controls assertions – Identify the critical information systems supporting financial reporting and other critical processes (as discussed in Questions 63 and 64). Most likely, there are several pervasive IT areas that should be examined, including IT operations, security, business continuity planning, application changes, remote access, Internet/EDI and outsourcing. There are several control issues (i.e., assertions and/or specific process-level risks) that should be considered when evaluating each of these IT areas. First, decide which control issues to consider for each IT area. Second, select appropriate specific risk statements for each area. These specific risk statements should be developed in the context of the potential effect of the area on the achievement of the financial reporting assertions discussed in the two bullets in the first paragraph above. Once the approach and customized diagnostic are developed, the evaluation approach and plan should be reviewed with the independent public accountant.

Assess the relevant pervasive IT controls – Pervasive IT controls should be evaluated in the same way that controls over other critical business processes are evaluated. This would include the use of process maps, process narratives, policy and procedure evaluations, etc. In essence, the pervasive IT control areas are those areas that are critical to ensuring effective control over the important financial and other disclosure-related applications. These evaluations may begin with questionnaires and self-assessments relating to the critical process areas. For example, key IT personnel may be requested to complete a questionnaire on a self-assessment basis in which input on the nature and type of evidence that exists to support the assessment is provided for each question. Other assessment methods include interviews and facilitated workshops. If surveys are used and there is a large population, consider using web-based technology.

Consider business continuity issues – An important aspect of managing a company's overall risk, including its continuation as a going concern, is its ability to effectively address business continuity and disaster recovery. A company must have a responsive business continuity plan, including an IT disaster recovery plan, addressing the findings from a business impact analysis (BIA). The purpose of the BIA is to identify recovery objectives for critical business processes and IT assets, as well as continuity-related business risks to which the organization may be vulnerable. Once an adequate BIA is completed, the company can evaluate whether changes are needed in its business continuity and disaster recovery plans. These plans must be kept up to date and periodically tested to maintain their adequacy in ensuring that the company can fulfill its obligations to shareholders and under SOA.

In light of the events of September 11, 2001, business interruption is clearly an important business risk to be managed. There are compliance and regulatory issues around SOA Sections 302 and 404 requiring companies to design and maintain procedures and controls to identify in a timely manner all material information for action and disclosure, and provide fairly presented financial and other information to the public in periodic and current reports. There is a presumption in financial reporting that a company's continuity capabilities are sufficient to enable it to meet regulatory requirements for accurate and timely disclosures and reporting under the SEC rules and regulations. A company's systems and controls must make available all material information needed for fair presentation and disclosure, including the update of accounting estimates with current and reliable information. On a more strategic scale, an organization's business continuity methodology and approach must be agreed to by management as the foundation for mitigating financial and reputational risk posed by business interruption.

Gather supporting evidence – During their assessment, IT personnel evaluate the effectiveness of pervasive IT controls and also indicate the nature and type of available supporting evidence. The project team must develop and execute a plan to obtain, document, assess and validate the relevant supporting evidence.

Evaluate impact on process-level controls – Management evaluates the combined results and concludes on the pervasive IT 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 pervasive 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 pervasive IT controls. In any event, management should review assessment and validation results with the independent public accountant.

76. What if transaction processing is outsourced?

When transaction processing is outsourced, it does not change the need for management to assess controls over processing that are significant to the company's accounting systems and controls. The IT and other control issues exist regardless of whether the processing takes place internally or externally. Under the provisions of SOA, management must evaluate the controls over the process activities and applications 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.

When an organization considers internal controls relative to outsourced processes and systems, a reading of the outsourcing agreement is a critical first step. The agreement hopefully 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 and ownership rights, etc.) and should also define service-level agreements, which also may get into some of the control aspects that need to be understood.

The evaluation of internal controls resident in business processes should consider the controls needed to achieve the financial statement assertion objectives, which are likely to require appropriate controls residing at the service provider (outsourcer). During an SOA 404 project, these controls would need to be evaluated and tested like any other controls for a process or an application managed and controlled directly by the company. Without clear guidance on this topic, organizations may look to accomplish this evaluation and testing through either an SAS 70-type report provided by the outsourcer (provided the issues noted below 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 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. Thus 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 provider's controls.
- SAS 70 reports typically are 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 provider's auditors. The alternative is for management to test the service provider's controls independently, which is often not a practical option.

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

- First, a reading of an SAS 70 report clearly indicates that it is an auditor-to-auditor communication, so it is possible that the Auditing Standards Board (ASB) did not intend for it to be used for management reliance from a regulatory standpoint. While this may not be an issue, management should ask legal counsel to review the legal aspects of this reliance.
- 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 statement may need to be expanded, perhaps significantly, to satisfy the additional requirements of management. Again, this is an area for which management is clearly responsible under SOA. 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 financial statements.

- 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 could 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 question concerning the issue 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? The answer to this question may require quarterly SAS 70 reports issued by the service provider’s independent accountant.

While there are many issues that should be considered, it is clear that for significant applications some work at the service provider is required. An SAS 70 report is a good starting point, but the SAS 70 reporting process will require modification, perhaps by the PCAOB, to align with the requirements of Section 404. The financial reporting implications of the outsourcing arrangement are key 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.

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

The line between these two reviews is not always clear. The project team ultimately must decide where the line is drawn. Generally, controls at the entity level are not directly involved with initiating, recording, processing and reporting transactions. Controls at the process level are directly involved with the critical transaction flows. It should be noted, however, that there may be certain processes that are entity-wide in scope, such as IT processes or shared services. These entity-wide processes should be treated as process-level control evaluations because they function at an enterprise level, which is different from most of the business processes reviewed in conjunction with a Section 404 project.

78. How is the activity-level assessment conducted?

Question 41 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.

Document the risks and controls – After the process inputs, activities and outputs have been documented, 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 Question 68 for an illustration). When identifying controls, the project team filters them down to the vital activities 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 controls discussed in Question 75.

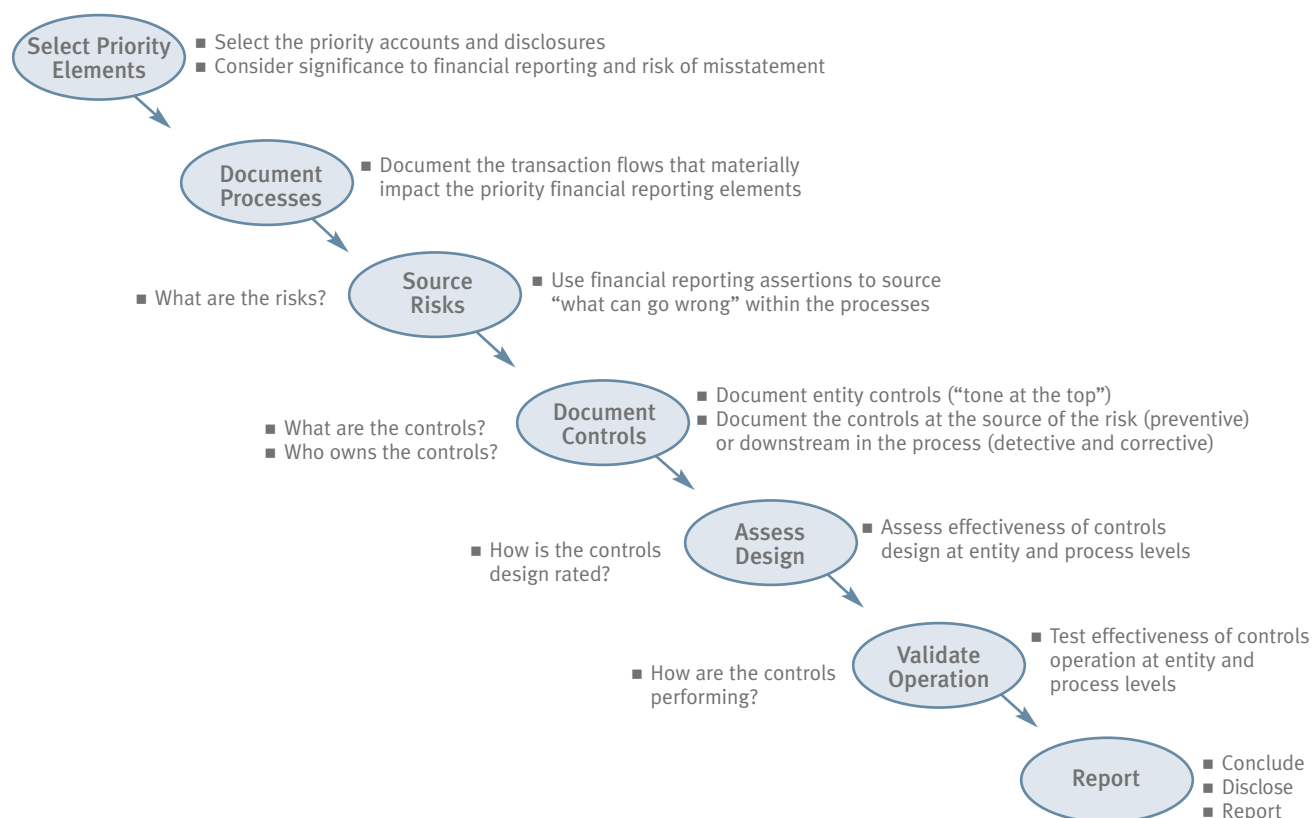
Assess design effectiveness – After the risk and controls are documented, the project team is ready to evaluate whether the controls, as designed, provide reasonable assurance that the risks have been reduced to an acceptable level, i.e., the stated financial control objectives have been met.

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.

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 below.)

A PLAIN ENGLISH SUMMARY



79. 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. For guidance on documentation, it may be useful for the project team to review professional auditing standards and the COSO framework. These standards do not dictate 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.

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, 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 63, transactions were categorized as routine, unusual or non-routine 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.
- RECORD*** • Describe how transactions are authorized or 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, 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, how do they document their processes to support their evaluation?

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?

Process mapping is a valuable tool for documenting processes and transaction flows; however, it is 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 controls during the evaluation process.

- **Facilitates analysis** – Surfaces risks and controls related to 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.
- **Enables focus on change** – Provides a way to identify process changes during subsequent reviews.
- **Provides operating benefits** – For example, process mapping 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.

The evaluator of controls must understand the major transaction flows; however, the auditing literature does not dictate the form of documentation required. Therefore, management must decide whether or not process owners can conclude that all of the key risks have been identified for each financial reporting assertion applicable to the process. If the answer is “yes,” then the next question should be, “How do you know the risk assessment is sufficiently comprehensive if there is little or no documentation of the process?”

Maps do not have to be highly sophisticated or detailed. Project teams should set their sights on documenting, communicating and understanding transaction flows using a framework from which to hang risks and 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 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 may decide documentation is necessary to facilitate the attestation process.

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, except for financial reporting (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 financial close 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.

OTHER TRANSACTIONS

With respect to unusual or non-routine transactions as well as transactions arising from accounting estimates, 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 (mergers, divestitures, etc.), emphasis should be given to understanding the extent of documentation required to support these transactions, and to the timeliness of involving persons with specialized knowledge to determine the correct accounting and reporting. There should also be evidence of board approval of significant unusual transactions.

The documentation of non-routine 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 application systems used to process these transactions
- The persons responsible for approving results of processing

For transactions arising from accounting estimates, special attention should be given to these transactions due to their subjective nature. Factors to consider in documenting these processes include:

- The frequency and timing of the estimate
- 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 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

80. 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.

The SEC provided several examples of controls subject to management’s assessment of internal control over financial reporting:

- Controls over initiating, 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 non-routine and non-systematic 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:

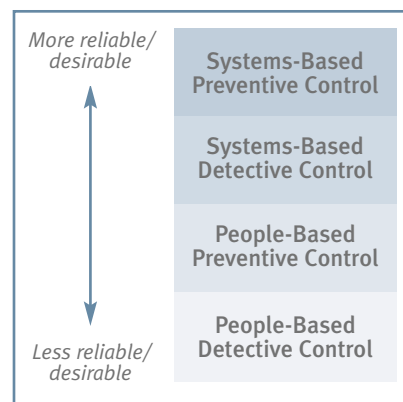
- Controls, including general controls, on which other significant controls are dependent
- Each significant control in a group of controls that functions together to achieve a control objective
- Controls over the period-end financial reporting process, including controls over procedures used to enter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

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

Pervasive Process Controls	Information Process Controls
<ul style="list-style-type: none"> • Establish and communicate objectives • Authorize and approve • Establish boundaries and limits • Assign key tasks to quality people • Establish accountability for results • Measure performance • Facilitate continuous learning • Segregate incompatible duties • Restrict processing system and data access • Create physical safeguards • Implement process/systems change controls • Maintain redundant/backup capabilities 	<ul style="list-style-type: none"> • Obtain prescribed approvals • Establish transaction/document control • Establish processing/transmission control totals • Establish/verify sequencing • Validate against predefined parameters • Test samples/assess process performance • Recalculate computations • Perform reconciliations • Match and compare • Independently analyze results for reasonableness • Independently verify existence • Verify occurrence with counterparties • Report and resolve exceptions • Evaluate reserve requirements

The so-called pervasive process controls apply to all categories of 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 right should be considered during the assessment of design, particularly in dynamic environments involving large volumes of transactions (such as in e-commerce and business-to-business environments). 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 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
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 42, some operational and compliance controls may be relevant to reliable financial reporting.

81. When should the 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 79. This analysis should document:

- The closing process itself, including the consolidation process
- The information processed during the close, including non-routine transactions and accounting estimates

- The various individuals responsible for different phases of the close
- The movement of documents, data and information during the process
- The process for generating financial statement disclosures, including the extent of involvement of the disclosure committee

Once the 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, simplification of targeted areas and elimination of nonessential tasks
- Evaluate the report preparation process, including the processes for accumulating disclosure information

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

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. 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. An 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.”

A suitable form (e.g., a risk and control matrix) should be used to document this evaluation for each process. This document includes appropriate information with respect to each management 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. 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.

The completed document is the key deliverable from this step. It addresses three questions with respect to controls design: (1) what are the controls; (2) who owns the controls; and (3) how are they rated? This document is prepared for all relevant 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 or insignificant 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 pervasive 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
- Whether the process and the controls within the process are collectively, at a minimum, at the “defined state” of capability (see Question 86)
- Whether the identified controls are preventive versus detective, 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 systems-based controls
- Extent of change in the business and its expected effect on internal controls

83. 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 time to ensure they are operating as designed. There are several methods of validating controls – process-owner monitoring, entity-level monitoring by reporting 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. Once those decisions are made, unit managers and process owners can conduct quarterly 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 are executed throughout the year.

84. 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 new 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 157.

85. How does management define “reasonable assurance” for purposes of evaluating the effectiveness of controls?

The professional auditing literature doesn’t provide much guidance on this question. Thus management must exercise its judgment when evaluating whether the level of assurance attained is “reasonable.” 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 meeting assertions. The concept of reasonable assurance 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.

86. 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 82 and 83. The analysis may be documented in many ways, such as the matrix introduced in Question 82.

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.

Internal Controls Capability Maturity Continuum			
Capability Level	Capability Description	Capability Attributes	Section 404 Implications
Optimizing	<p>CONTINUOUS IMPROVEMENT</p> <p>Continuously improving controls enterprisewide</p> <p>"Chain of accountability" sustained</p>	<ul style="list-style-type: none"> ■ 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 	<ul style="list-style-type: none"> ■ Internal controls – Integrated framework fully implemented ■ Entity-level analytics and monitoring fully operational ■ Faster decisions on improving controls ■ Controls preventive and systems-based
Managed	<p>QUANTITATIVE</p> <p>Risks managed quantitatively enterprisewide</p> <p>"Chain of accountability" is in place</p>	<ul style="list-style-type: none"> ■ Control process performance standards established and managed ■ Rigorous estimation methodologies and analysis ■ Risks are managed quantitatively and aggregated at corporate level ■ Process-based solution 	<ul style="list-style-type: none"> ■ Controls effectiveness continuously assessed and validated ■ Process owners report to management ■ Internal audit plans aligned ■ Entity-level analytics and monitoring emerging
Defined	<p>QUALITATIVE/QUANTITATIVE</p> <p>Policies, processes and standards defined and institutionalized</p> <p>Controls documented and accountability emerging</p>	<ul style="list-style-type: none"> ■ Internal control uniform across the entity ■ Transaction flows documented ■ Risks of errors and omissions sourced ■ Control processes for mitigating risks better documented and integrated 	<ul style="list-style-type: none"> ■ 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	<p>INTUITIVE</p> <p>Process established and repeating; reliance on people continues</p> <p>Controls documentation lacking</p>	<ul style="list-style-type: none"> ■ Common control framework ■ Increased controls awareness ■ Basic policies and control processes established ■ Processes are repeating but not necessarily documented 	<ul style="list-style-type: none"> ■ Quality people assigned to support control activities ■ Some control gaps identified and fixed ■ Communication is lacking ■ Limited monitoring activities
Initial	<p>AD HOC/CHAOTIC</p> <p>Control is not a priority</p> <p>Unstable control environment leads to dependency on heroics</p>	<ul style="list-style-type: none"> ■ Reliance on individual initiative ■ "Just do it" ■ Ad hoc disclosure activities ■ Policies not articulated ■ Few processes are defined ■ Institutional capability lacking 	<ul style="list-style-type: none"> ■ Key controls are not in place ■ Controls are not periodically evaluated for deficiencies ■ Success depends on manual efforts and validation by seasoned managers ■ Gaps result when key people leave

The following five capability levels represent states of maturity by which the project team can rate a company's internal controls in a particular process:

- 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 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 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 state 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, often a by-product of improved quality and reduced risk, enables 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 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 process. Management can then decide where on the continuum the company needs to be with respect to each process. For example, assume that the controls over revenue processing are at the Repeatable State. Management must decide at what state they want the controls in 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, i.e., in lieu of “revenue processing,” management may assess order entry, shipping, billing, costing of sales, commission accounting, etc.

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

The assessment of controls design and operational effectiveness is complete and control gaps 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 stated objectives are met or that process 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 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. Internal 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 adjustment 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.

So what happens now that 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. 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. 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 86) and measure performance to ensure control operates in accordance with the design. For operating deficiencies, management often will need to publish policies to clarify roles and responsibilities, implement hiring and training initiatives to ensure the requisite competence and resources are brought to bear, and measure 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.

88. How does a company define a “significant deficiency” in internal control?

For purposes of the final rules, the SEC indicated that the term “significant deficiency” has the same meaning as the term “reportable condition” as used under GAAS and attestation standards for purposes of reporting to the audit committee by the independent public accountant. 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. 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.

A significant deficiency in internal controls arises if:

- The process, as it is designed, could lead to errors or omissions in the recording, processing, summarization and reporting of financial data that are inconsistent with the assertions of management, or
- Effectively designed internal controls fail to operate as intended.

Whether the deficiency is in design or in operation, it is significant if management concludes that the effect of the deficiency is a condition that warrants management's attention and should be corrected as quickly as possible because it either is or could become a material weakness in internal control.

If the independent public accountant concludes that a deficiency in the design or operation of the internal control over financial reporting could “adversely affect a company's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements,” that deficiency is a reportable condition. Thus management and the auditor have the same standard in terms of their responsibility to report to the audit committee. That standard is also management's for purposes of reporting to the independent public accountant.

From a practical standpoint, if management identifies a deficiency in internal controls that it believes could adversely affect the company's ability to record, process, summarize and report financial data (and, therefore, is significant), it should discuss that deficiency with the independent public accountant, the internal auditors and the audit committee before finalizing its conclusion that the deficiency does have an adverse impact. This is particularly important because, as explained earlier, the independent public accountant must report to the audit committee all significant deficiencies identified in connection with the audit. This could result in situations 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 earlier in the year. This situation could potentially increase management's exposure if these matters resulted in errors or omissions in the company's financial reporting and were not reported on a timely basis when they came to management's attention.

89. How does a company define a “material weakness” in internal control?

For purposes of the final rules, the SEC indicated that the term “material weakness” has the same meaning as in the definition under GAAS and attestation standards. 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.’” The SEC also asserts that an aggregation of significant deficiencies could constitute a material weakness in a company's internal control over financial reporting.

A significant deficiency in internal control is not necessarily a material weakness. A material weakness is a significant deficiency in internal control that could have a material effect on the financial statements. After a

control weakness is identified, management should evaluate the severity of the control weakness and determine whether the control weakness is a minor deficiency, a significant deficiency or a material weakness.

The AICPA defines a “material weakness” as “a condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by errors or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.” The SEC referred to this definition in the final release.

A material weakness is a condition in internal controls in which there is a high probability that errors or irregularities in amounts material to the financial statements could occur and not be detected by employees and processes the company has in place. 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 when making an assessment as to whether a controls weakness is a “material weakness.” For example, the overall control environment, the nature of the identified control weakness and compensating controls, the nature of the assets at risk, the presence of other control weaknesses, changes in company practices and procedures, and past experience are examples of such issues. Because of the complexity of these issues, management should consult with the independent public accountant if there is any question as to whether a particular weakness in internal controls is a material weakness.

The evaluation of a control weakness to determine whether it is material is based upon three principal considerations, each of which is discussed below.

- 1) The nature, timing and extent of the audit tests the independent public accountant must perform to reduce residual audit risk to an acceptable level. The severity of an identified control weakness is often reflected in the amount of audit testing deemed necessary by the independent public accountant to reduce residual audit risk to an acceptable level at the audit date. The more extensive the procedures, the larger the sample size, and the closer the timing of the work is to the balance sheet date, the more likely that the control weakness is other than minor.
- 2) The results of the other audit tests, that is, the nature of proposed audit adjustments, if any. The independent public accountant and management must review the nature and root causes of proposed adjustments to determine whether they result from a control weakness. Proposed adjustments that are the result of fraud (intentional misstatements, misappropriation of assets or illegal acts) may be indicative of a material weakness.

Proposed adjustments that result from inadequacies in controls over transaction processing and their summarization in the books and records ordinarily would be indicative of an internal control deficiency, the magnitude of which would depend upon consideration of the other factors discussed above and below. Also, proposed adjustments involving accounting estimates that result from a flawed process, incompetence of client personnel or inaccuracies in the underlying data upon which the estimate is based ordinarily would be indicative of an internal control deficiency.

When an assertion regarding a priority financial reporting element is not met, a “significant deficiency” in internal controls could exist. For example, if material routine transactions are not processed in a manner to satisfy the completeness and accuracy assertion, that condition could be a “significant deficiency” if management is unable to determine that adequate compensating controls are in place or is unable to isolate the magnitude of the potential error.

On the other hand, proposed adjustments that relate to (a) unique and/or complex transactions for which the generally accepted accounting principles are similarly complex and highly judgmental, 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 not be indicative of a control weakness. For example, a proposed adjustment relating to differences 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) ordinarily would not constitute an internal control deficiency.

The first two considerations for evaluating a control weakness – the nature, timing and extent of the audit tests the independent public accountant must perform to reduce residual audit risk to an acceptable level, and the nature of the proposed adjustments arising from those audit tests – clearly illustrate that the independent public accountant will often be heavily involved in evaluating whether a deficiency in internal control is a material weakness.

3) Characteristics of the identified control weakness. The following factors should be considered when evaluating the severity of one or more identified control weaknesses:

- The overall control environment. The overall operating environment and management attitude regarding internal control are important factors. A deficiency in a specified area would be considered much more significant when the 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, 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.
- Nature of the identified control weakness and compensating controls. Control weaknesses may be categorized as relating to either a preventive control or detective control. Sometimes, preventive control weaknesses may be offset 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 preventive control weakness might be fully mitigated by the detective control. However, detective controls are seldom as effective as preventive controls. In a 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 flow (i.e., the control point is not at the source of the risk), it usually is extremely difficult as well as costly to find and fix errors later. Accordingly, weaknesses in preventive type controls often represent significant deficiencies or material weaknesses, notwithstanding the existence of compensating (detective type) controls.
- Nature of assets at risk. The nature of the assets that might be affected by a control weakness is another important consideration. Attributes such as mobility, salability and alternative uses to others can affect the 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.
- Presence of other control weaknesses. Although the definition of a material weakness is directed primarily toward a single condition, it also encompasses circumstances in which several control deficiencies, which are individually immaterial, constitute a material weakness because of the possibility that the combined effect of errors that could result from the deficiencies would be material to the financial statements.
- 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 generally weak. Conversely, even in a situation in which some control weaknesses 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.
- Past experience with the entity. The independent public accountant's experience with the entity is also a consideration. 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?

90. Assume a June 30 reporting 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 89, 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 a “fix” must operate to overcome the “taint” of the control weakness. 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 and legal advisors.

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 error or omission in previous 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.

91. How does a company define a “significant deficiency” or “material weakness” in the so-called “soft control” areas?

With respect to the so-called “soft areas” such as communications, ethical values and management’s operating style, the question as to what constitutes a significant deficiency or material weakness is much more of a judgment call than the assessment of errors in routine transaction flows. Any questions or borderline issues should be brought out into the open for discussion with the independent public accountant and the audit committee.

92. What 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 as quickly as possible. Finally, management must disclose the actions taken to correct the condition, if any.

93. 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?

At this time there is no specific guidance from the SEC on this question. With respect to factors that could affect the adequacy of the internal controls, the SEC, in its proposing release, provided one possible example: the effect of growth on the adequacy of existing disclosure processes. Other 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, introduction of new systems, significant acquisitions and the effects of unexpected catastrophic events.

94. 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.

95. Can management rely on the self-assessments of process owners as the sole basis for rendering the annual internal control report?

We believe that self-assessments by process owners 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, the results of internal audit testing and other separate evaluations performed from time to time.

96. 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 processes.

97. 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 internal 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.

98. 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.

Identifying and Assessing Controls – After Initial Annual Assessment

99. After the initial annual assessment, how does management conduct the quarterly evaluation 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 conclusions regarding effectiveness of disclosure 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 annual 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 36 and 37.
- 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.
- With process-owner feedback every quarter, management, i.e., the certifying officers, will be positioned to focus on change, e.g., changes in processes, systems, operations and other factors, and their impact upon the effectiveness of internal control related to disclosure.

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 "back-up 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 results of the initial annual assessment 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.

100. 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.

101. Will subsequent annual assessments be similar to the initial annual assessment?

Past experience with banks complying with the FDICIA requirements indicates that subsequent annual assessments will be much easier than the initial annual assessment. All of the required documentation will already exist and the emphasis will be on the effects of change. The independent public accountant's requirements will be understood and the quarterly evaluations of internal control over financial reporting should result in issues surfacing with the auditors and the audit committee on a timely basis.

Validation of Operating Effectiveness (“Testing of Controls”)

102. 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.

We view “testing” as a subset of validating operating effectiveness. There are several forms of validating the operating effectiveness of controls, one of which is 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.

Three approaches to validating operating effectiveness are:

- **Self-assessment.** Process and control owners 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 determining that the controls are operating effectively and in identifying material errors and/or omissions not detected by the underlying control processes.
- **Tests of controls.** 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 testing controls. If self-assessment results are comprehensive and positive and there are strong entity-level monitoring controls, testing confidence levels may be lower and sample sizes smaller. 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.

103. Who is responsible for validating operating effectiveness?

Management, with the participation of the company's CEO and CFO, is ultimately responsible for validating operating effectiveness of controls.

104. 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 include inquiries of process and control owners, inspection of relevant control documentation, observation of controls in action, and analysis or reperformance of the operation of a control using selected 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 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. 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.

105. 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 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 philosophy and operating style). Testing of these controls must be accomplished through visual observation of entity activities and interviews with control owners and other appropriate personnel.

106. 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 above, 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 are able to implement it. 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 consistency of responses received. Inquiries also complement other 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 insufficient. 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.

While inquiry is a type of test of controls, we also must acknowledge that self-assessment, which we have asserted is a separate form of validation, is also an inquiry technique.

107. What is reperformance?

Reperformance of controls provides the most tangible form of testing. The external auditors will likely emphasize this form of testing during the attestation process. Reperformance is sometimes confused with a “walk-through” to understand how transactions are processed. While a walk-through is useful during the documentation process and the evaluation of design effectiveness, it is not a test of controls. Reperformance is the reprocessing of a sample of transactions to determine whether they were processed correctly and whether one or more specific attributes exist, e.g., appropriate management authorization, accurate processing, etc.

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. For example, the best evidence that control owners are comparing batch control totals to batch validation reports may be the existence 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.

108. When are tests of controls performed?

They may be performed at any time. In the initial year of assessment, they ideally should be completed prior to the end of the 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 114 for further discussion regarding the update of testing through year-end.

For subsequent years, testing may be performed uniformly throughout the year. An update is then performed through the end of the year.

109. What is a testing plan?

A testing 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 73) 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 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, 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
- 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 testing plan. For example, the certifying officers or the Section 404 Compliance Steering Committee could 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 reduce the risk of surprises arising from disagreement over testing approaches, scopes and sample sizes later during the attestation process. Ultimately, the auditor must evaluate the adequacy of the plan for purposes of supporting management's assertions relating to operating effectiveness.

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 testing 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 testing 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 testing plan needs to consider the three forms of validating controls effectiveness introduced in Question 102 (i.e., self-assessment, monitoring and testing).

110. How does management decide which controls to test?

There are several areas management and the project team will want to address before developing a testing plan. Validating operational effectiveness without a clear understanding as to which controls are the most critical is a blueprint for allocating substantially more resources than necessary to controls testing. It is not necessary to test every control.

The process of “filtering” controls to identify the primary or critical controls on which management relies requires careful thought and judgment. While documenting processes and controls, the project team will identify 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 prioritizing those controls. For example, the project team may choose to label each control as primary, secondary or tertiary. Ranking the controls enables the project team to determine the primary or critical controls. These controls are often at the activity or process level. See Question 73 for a discussion of validating controls at the entity level, including the approach to deciding which controls to validate.

Filtering is the process of identifying the primary or critical controls. Some of the factors considered by management when identifying the critical controls include selecting:

- Controls that are especially critical to the mitigation of 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. For these elements, coverage is important.
- Controls on which other critical controls are dependent. In other words, 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. For example, the extent of reliance upon a key report used as part of an important reconciliation procedure may be dependent upon the effectiveness of controls over the IT application system that generates the report. Validation of these controls on which the effectiveness of other controls depend may also involve some direct testing.
- 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 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 stated risk to an acceptable level and achieving a 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 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.
- Critical controls for which there is a significant risk that they might not operate effectively. Factors that management should consider include:
 - The complexity of the control
 - Whether the control is manual or systems based, i.e., controls that rely on the 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
- Controls on which critical information processes are based, such as controls over IT processes generating critical reports used by management for purposes of entity-level monitoring or by process owners for purposes of process-level monitoring. When monitoring controls are relied upon, it is important to evaluate the IT processes generating the information that makes effective monitoring possible.
- 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.

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 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 internal controls. It is a practical approach because testing requires a great deal of time and resources.

One approach to filtering is for the project team to methodically evaluate the financial reporting assertions for each priority financial reporting element and, applying the criteria above, decide on the key controls to test. While this takes time, it is a preferable approach to testing every control. Where necessary, experts in specific control areas (IT, for example) should be involved in this process. What should be avoided is a mechanical approach in which controls are selected for testing off of a comprehensive list without regard to importance. The time invested up-front in terms of critical thinking about the assertions and the related risks and the key controls that address those assertions and risks will save companies a substantial amount of time over the course of the entire testing process, not only during the initial annual assessment but also in the years to come.

111. Why are control descriptions important and how does management know they are adequate?

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.

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. To simply refer to a control without identifying the person or group responsible for the control or understanding how the control addresses errors and omissions 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 improvements can be made.

- **Inadequate description:** A “was-is” report is used to manage price changes.

Adequate description: An IT-generated “was-is” list is reviewed by the marketing department 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.

112. How are inquiries, inspections and observations 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. One way to accomplish this task is to use a form that includes the following information:

- **Name and title of control owners interviewed** – The “owner” of the control is the one who is accountable for its operation.
- **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** – Sufficient information should be recorded so the independent accountant can retrieve the documents, if necessary, to reperform the 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 there are no errors or exceptions, that may be an indication that the control owner doesn’t understand the control and is not performing it. It could also mean that the technique is merely a processing procedure and not 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.
- **An assessment of operating effectiveness** – The evaluator must conclude as to whether the control is operating effectively.

113. Is testing by process owners acceptable for purposes of supporting management’s assertion?

Yes, at least partially. Another way to phrase this question is what must the process owners have as “evidence” to support their self-assessment determinations on an ongoing basis (through the use of technology, for example)? 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 Question 104. What’s left is the reperformance technique, which many process owners may believe is not necessary due to their day-to-day involvement.

That said, testing by process owners alone is not a sufficient body of evidence for management to base a conclusion. More evidence is needed through direct self-assessment reporting from the process owners, entity-level monitoring and analytics, and tests of controls by internal audit.

114. With respect to the period between the date management completes its evaluation of operating effectiveness and year-end, what must management do to update its evaluation?

Management should complete the evaluation on a timely basis so that the external auditor can evaluate the evidence supporting management’s assertion on internal control.

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. If self-assessment is used at year-end and monitoring controls are strong, the testing required at year-end may be reduced to a minimum. However, for the critical controls over priority

financial reporting elements, the evaluator may want to perform some testing as of or close to year-end. Whether the testing takes place as of year-end or during a period close to year-end is largely dependent on management's confidence in the control structure and the effectiveness of monitoring.

At year-end, management must assess whether there have been changes in internal controls, or in factors that affect the performance of internal controls, that would invalidate or otherwise impact the results of tests of controls performed at an earlier point in time. An example would be that the impact of changes in processes, personnel and application systems needs to be evaluated and, as a result, additional follow-up tests of controls will be necessary. This update should be completed prior to year-end.

The purpose of the suggested approach outlined in our response to Question 55 is to support the development of the body of evidence in Year 1 for the audit to begin while the necessary remediation and repair take place. Assuming that testing is performed through the end of the second or third quarter, that work would need to be refreshed at year-end to address changes that have occurred and other issues that might have affected the internal control structure since the date of management's preliminary evaluation. This 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 Year 2.

The use of technology can provide a very elegant solution to refreshing the third-quarter body of evidence and positioning the company for ongoing quarterly self-assessments. Through the use of technology, self-assessment can be done at any time. For example, one calendar year reporting company plans to use 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. Testing will be applied to risky areas during the fourth quarter.

In addition, management should consider taking advantage of the additional time provided by the SEC to strengthen 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 technology and the entity-level monitoring techniques during the last quarter of the initial annual assessment can serve a dual purpose – first, achieve the objective of updating the preliminary Year 1 evaluation to year-end without having to perform extensive additional testing and, second, provide a “dry run” of management's approach for conducting the ongoing quarterly evaluation during Year 2 and beyond.

In Year 2 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 meaningful, cascading process-based self-assessment approach in place;
- Adequate entity-level monitoring controls and analytics, so a problem in the financial controls would be detected in a timely fashion; and
- Periodic tests of controls by internal audit.

Tests of controls by internal audit would be designed to evaluate the reliability of the self-assessment process and the integrity of the reports that make entity-level monitoring possible.

115. What should management do when exceptions are identified?

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 exception, 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 deviation
- Management became aware of the exception on a timely basis
- Management responds to the deviation on a timely basis (if management was aware of it)

Regardless of the reasons for the deficiency, numerous or repeated instances of the deficiency may constitute 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.

116. How is monitoring evaluated?

Monitoring takes place at both the entity and process levels. Entity-level monitoring includes analytics and metrics. Following are examples:

- Budgetary controls provide an effective mechanism for monitoring results, particularly when the budget is based upon specific factors such as volume, price and mix, enabling the determination of variances for further analysis and investigation. These controls facilitate preparation of P&L attribution reports summarizing how the organization makes or loses money.
- Exception reports provide an indication as to the effectiveness of internal controls, e.g., authorization controls, limit controls, change controls, etc.
- Event reports summarize the number of incidents or near misses, e.g., the number of instances of errors, down time, limit violations, etc.
- Audit reports confirm compliance with established policies, provide assurance that controls are operating as intended and process measures are reliable, etc.
- Process metrics address key factors, e.g., number of shipments during last week of reporting period, sales volume versus plan, store sales per cash register, SG&A spending accountability reports, etc.
- Predictive tests provide an effective means of evaluating 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.

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. Process owners may 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. The evaluation should consider an evaluation of 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 testing plan. The extent of monitoring tests should reflect a representative sample of a sufficient size to include exceptions to be satisfied with appropriate management actions.

A key aspect of monitoring at the process level relates to the actions taken by the control process owner when any exceptions are identified. These actions should include identifying the root cause of the exceptions and ensuring appropriate process improvements or other necessary actions are taken to avoid the occurrence of future exceptions.

117. How are pervasive process controls tested?

Pervasive process controls can have an indirect impact on the operating effectiveness of information process controls. They include entity-level controls such as establishing and communicating objectives and assigning key tasks to quality people. They also include entity-wide 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 provide an overall context to ensure:

- Authorization and control over changes in processes and controls
- Appropriate segregation of incompatible duties, e.g., authorization, custody and record keeping
- Integrity of programs and data that support execution of specific risk controls and monitoring activities

Pervasive process 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 risk controls and monitoring activities.

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 controls. A customized plan for testing process and systems development standards, process change controls and access controls should be developed involving appropriate information technology 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.

118. How are information process controls tested?

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. "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.
- 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 (e.g., by confirmation of counterparties, physical observation and monthly statements received from vendors) of balances by others, and evaluate the appropriate disposition of these differences.
- Evaluate process metrics related to activity levels or the time, cost and quality of process activities.

119. How are sampling methodologies applied?

When designing tests of controls, management must decide on the nature, extent and timing of the tests. Sampling is an important aspect to tests of controls because it affects the number of items selected for testing and 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 that 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 and the results of entity-level monitoring.

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 critical 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

There is no “one size fits all” when deciding the most appropriate testing 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 86 introduced 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 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.

- 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 testing 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 86), 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 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.

Thus management’s testing plan is often influenced by the maturity of the company’s controls, as illustrated using the Capability Maturity Continuum introduced in Question 86. Because there is no “one size fits all,” input from the independent accountant should be obtained before commencing execution of the testing plan.

120. 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 controls 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.

Reporting

121. 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 pervasive IT controls
- The results of controls-design evaluations at the process level
- The results of controls testing at the process level
- 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 internal control over financial reporting.

122. What should be communicated to executive management, project sponsors and the board?

One of the most important aspects of internal control reporting is to ensure the related reporting requirements of Section 302 are met. These matters are discussed in Question 135. 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.

123. What is the internal control report?

Under the final rules, 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 has also 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.

124. When management identifies an internal 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 report?

Yes. The SEC's final rules require management to disclose to the public any material weaknesses in internal control over financial reporting identified by its evaluation.

125. 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.

126. 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. 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.

127. Can the results of the assessment of internal control over financial reporting affect the company's executive certification 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. 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 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.

128. What impact would a conclusion that the internal controls are ineffective have on the company?

First, there is the potential negative impact on market capitalization. The damage to reputation could also be troublesome. This should be enough to get one's attention.

With respect to filings with the SEC, it is unclear at this time what the impact would be. For example, what would happen if management reported a material weakness in internal control and was unable to conclude as to the effectiveness of internal control over financial reporting in the annual internal control report? Or if the auditor issued a qualified report? It is too early in the process to say.

One thing we do know: The 1934 Exchange Act and 1977 Foreign Corrupt Practices Act require public companies to have adequate internal controls in place. Thus there may be legal ramifications to a material weakness issue that management will have to resolve with legal counsel and the board of directors.

Role of Management

129. 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 quality material information is disclosed timely 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 should also 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 and what isn't material in meeting the SEC's requirements to make appropriate disclosure so 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 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 given to quality 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 should also 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 recent survey conducted by the National Investor Relations Institute of almost 400 public companies indicated that 85 percent had established a disclosure committee as defined by the SEC. With respect to the Section 404 project, the disclosure committee is more interested in the results of the project and its disclosure implications than in the management and direction of the project.

130. 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.

131. 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 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.

132. 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 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 may also 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.

133. 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.

134. Who signs off on internal control over financial reporting?

Section 302 of SOA 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 officers will also 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 certifying officers. 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.

135. What communications, if any, are required of management beyond the executive certifications and 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

136. 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.

137. Can management rely solely on self-assessments of process owners for purposes of their evaluation of design and operating effectiveness?

No. We believe that self-assessments by process owners 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, the results of internal audit testing, and other separate evaluations performed from time to time.

138. 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.

139. 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 148, 149 and 150.) 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. Ultimately, the responsibility rests with management to make decisions regarding any recommendations, including decisions to implement.

Role of Internal Audit

140. What is the current status of the NYSE requirement that listed companies have an internal audit function?

The proposed NYSE listing standards would require 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 firm other than its independent auditor.

The NYSE rules allow listed companies up to six months from the date the SEC approves the listing requirements to comply with this mandate. SEC approval has been delayed so that revisions can be made in the NYSE and NASDAQ proposals in order to achieve symmetry where possible. The standards are expected to be published for comment sometime in summer or fall of 2003. They likely will become effective in early 2004. We understand that many companies are choosing to move forward as though the NYSE proposals are effective now, for institutional investor grading purposes.

141. What should companies do if they are listed on other exchanges? Are they required to have an internal audit function?

Currently, NASDAQ and AMEX do not address the internal audit function in their listing requirements. In addition, the SEC may seek to include such a requirement for NASDAQ companies as part of its review of the proposed rules. In today’s world, companies without an internal audit function will be the exception, regardless of the legal requirements. Further, as noted in Question 140, the SEC is looking at harmonizing the various exchange proposals.

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.

142. 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 or to the CEO. 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 have 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 initial annual assessment.

143. 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.

Role of the Independent Public Accountant

144. 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 should also ascertain whether the “body of evidence” provided by the planned approach is acceptable to the independent public accountant and 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.

Following are illustrative examples, not intended as all-inclusive, of relevant checkpoints for the independent public accountant:

- Key financial statement accounts and disclosures
- Documentation standards, i.e., type and depth of documentation
- Format of documentation
- Extent of process documentation
- Extent and depth of validation, including management's testing plan
- Entity-level assessment results, including the breakdown of the enterprise into control units for purposes of performing an entity-level assessment and the key attributes reviewed
- Pervasive IT controls-assessment results
- 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 results of evaluating the financial closing 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.

145. 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.

146. 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, use and 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 144.)

147. 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.

148. 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.

149. 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 150, 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 was 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?

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.

150. 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 made statements to the effect that the documentation of controls and the evaluation of their effectiveness is indeed a management function. Therefore, if the auditor has been asked to perform that role instead of or on behalf of management, that would involve 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 what could very well be an evolving area.

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 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, which has been embraced by one major accounting firm, 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 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. Given today's hypersensitive environment, this issue does not appear to be one in which it is in anyone's interest to test.

151. 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 can also expect the independent public accountant to consider the results of the audit work on the financial statements. 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.

152. What is the Public Company Accounting Oversight Board (PCAOB)?

The Sarbanes-Oxley Act created the PCAOB to provide oversight over the accounting industry. With four of the five board members present, the board held its first public meeting in January 2003, promised to rapidly get started, and announced its budget and staffing plans. For 2003, the PCAOB plans to spend \$36.6 million, with a \$50 million annual budget once it reaches full staffing. The PCAOB will immediately have offices in Washington, D.C., and plans to soon open an office in New York. By the end of 2003, the PCAOB expects to have approximately 200 employees and eventually as many as 300. In April 2003, departing New York Federal Reserve President William McDonough agreed to become the PCAOB Chair. On April 25, 2003, the SEC and the PCAOB jointly announced that the PCAOB was appropriately organized and had the capacity to carry out the requirements of Sarbanes-Oxley, a significant milestone because Section 101(d) of SOA mandated that the PCAOB become fully operational by April 26, 2003.

153. When will the PCAOB issue guidance regarding the independent public accountant's attestation requirements and standards?

In April 2003, the PCAOB voted to take control of the auditing standards setting process, effectively ending more than six decades of self-regulation of the public accounting profession and, in effect, putting the Auditing Standards Board out of business. Interim standards consisting of existing standards from the American Institute of Certified Public Accountants continue to remain in force until further notice. At the time this publication went to print, there was no indication as to when the PCAOB will issue further guidance regarding the independent public accountant's attestation requirements and standards. (For reports on recent PCAOB announcements, guidelines and activities, please visit www.protiviti.com.)

Role of the Audit Committee

154. How and when should the audit committee be involved in management's evaluation process and in the independent public accountant's attestation process?

Audit committees are currently asking this question. During the SEC's open meeting on Section 404, the staff commented that the audit committee is expected to play an important governance role in requiring changes to correct internal control weaknesses. Audit committees want to 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 advising audit committees to use the same type of line of inquiry as on the annual certified audit opinion, i.e., asking what problems and issues were found and how are they being resolved.

Because internal control over financial reporting is a subset of disclosure controls and procedures, we expect the audit committee's role in the quarterly evaluation of internal control over financial reporting to be similar to its role in the currently required evaluation of disclosure controls and procedures. At a minimum, the audit committee 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.

155. What questions are audit committees asking in this initial phase of Section 404 compliance?

With respect to Section 404, the line of questioning has increased substantially as audit committee members learn more about it. The substance of the message points CFOs and independent accounting firms are delivering at this time (March 2003) is usually along the following lines: "Under Section 404 of Sarbanes-Oxley, management has the responsibility to establish adequate internal control over financial reporting, and the independent audit firm must attest to and report on management's evaluation of the company's internal controls." Some of the questions audit committee members have told us they are asking at this time include:

- a) How do you define "internal control" in the context of financial reporting? In English, please.
- b) What are the company and the audit firm doing to take advantage of the SEC's extended transition period to prepare for the Section 404 requirement? Is it being planned for orderly work over the next two years to make it more effective, less disruptive and less costly? How is the project being scoped to ensure the review focuses on what matters?
- c) Is management leveraging the additional time to accomplish more than formally documenting internal control over financial reporting? For example, is management satisfied that the company's entity-level analytics and metrics provide sufficient transparency as to the effectiveness of internal control over financial reporting?
- d) How does the extended transition period impact on the cost of the audit? Is there an opportunity to reduce audit costs by spreading the attestation over a longer period of time out of the audit firm's peak?

- e) What is it going to cost? Assuming an audit firm quotes 20 to 30 percent of the annual audit fee, does that mean it will take 20 to 30 percent of the time the annual audit takes? If not, how much of this fee is a premium for assumption of risk?
- f) 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?
- g) 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?
- h) If you, the independent auditors, had to make this certification for the 2002 financials, knowing what you know now, do you know of anything that would stand in your way in terms of reporting on the company's internal controls?

Impact on Sections 302 and 906

156. What is the impact of the new rules on Sections 302 and 906?

The final rules amend the exhibit requirements for periodic reports to add the certifications required by Sections 302 and 906 of SOA to the list of required exhibits to be included in quarterly and annual reports filed with the SEC. Thus the SEC amended the exhibit requirements of Forms 20-F and 40-F and Item 601 of Regulations S-B and S-K to add the Section 302 certifications to the list of required exhibits. Some firms already follow this procedure, but other companies have supplied the certifications separately, which the SEC said created unnecessary confusion for investors. The intent is to make these certifications easier to locate.

In addition to minor changes in the organization of the certification, the SEC also adopted several amendments to the form of certifications to be provided pursuant to Section 302 of SOA:

- The addition of a statement that the certifying officers are responsible for designing internal control over financial reporting or having such controls and procedures designed under their supervision
- The clarification that disclosure controls and procedures may be designed under the supervision of certifying officers (instead of by the certifying officers)
- The revision of the statement as to the effectiveness of disclosure controls and procedures and internal controls and procedures for financial reporting would be as of the end of the period
- Amendment of the certification relating to changes in internal control over financial reporting, consistent with the final rules regarding evaluation and disclosure, so that it refers to changes that have materially affected or are reasonably likely to materially affect internal control over financial reporting
- Clarification that the statement on the effectiveness of disclosure controls and procedures be made as of the end of the period

With respect to the Section 906 certifications, the SEC amended 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, to 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. According to the final rules, 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.

The amendments will also permit companies 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 will also not be 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.

The rules and form amendments concerning Section 302 and Section 906 certifications apply to any reports due on or after August 14, 2003. The SEC encourages companies to file the 906 certifications as exhibits prior to that date.

157. 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.”

Other

158. What are the new 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. The changes for these accelerated filers will be phased in over three years. The annual report deadline will be reduced from 90 days to 60 days over the three-year period, while the quarterly report deadline will be reduced from 45 days to 35 days. The phase-in period begins for accelerated filers with fiscal years ending on or after December 15, 2002.

The following table illustrates the phased-in filing requirements:

For Fiscal Years Ending On or After	Form 10-K Deadline	Form 10-Q Deadline
December 15, 2002	90 days after fiscal year-end	45 days after fiscal quarter-end
December 15, 2003	75 days after fiscal year-end	45 days after fiscal quarter-end
December 15, 2004	60 days after fiscal year-end	40 days after fiscal quarter-end
December 15, 2005	60 days after fiscal year-end	35 days after fiscal quarter-end

With respect to the public float test, the SEC’s position is that this test serves as a reasonable measure of company size and market interest. This definition of accelerated filers excludes nearly half of all publicly traded companies.

159. When determining the applicability of the accelerated filing requirements under the SEC's final 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." Thus the measure is as of the end of any second quarter. For example, applied to the Section 404 rules, at the end of any fiscal year ending on or after June 15, 2004, a company will have to ask itself: "Was our public common float \$75 million or greater at the end of our most recent second quarter?"

160. 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.

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 (2004, for example), and then meets the other three tests (Items B, C and D) as of December 31, 2004, it must begin complying with the accelerated filing requirements beginning the first quarter in calendar 2005.

Once a company becomes an accelerated filer, it remains an accelerated filer subject to the SEC's abbreviated deadlines unless and until it subsequently meets the definition of a small-business issuer at the end of two consecutive fiscal years and becomes eligible as a small-business issuer to use Forms 10-KSB and 10-QSB for its annual and quarterly reports. A small-business issuer is a U.S. or Canadian issuer that has (i) revenues of \$25 million or less as of its last fiscal year, and (ii) a market capitalization of \$25 million or less. Small-business issuers, by definition, cannot be accelerated filers. However, many small companies that are too big to be small-business issuers are nonetheless still not accelerated filers. The SEC's intent is to minimize a company's fluctuation in and out of "accelerated filer" status while still allowing the company to exit that status if it becomes so small for so long that it becomes eligible to file its reports as a small-business issuer. In that case, the issuer ceases to be an accelerated filer unless and until it again meets the accelerated filer criteria outlined above.

161. 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.

162. 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?

While the SEC didn't address this issue directly, it allowed more time to small-business issuers. If calendar-year reporting company's market capitalization is expected to be less than \$75 million, management doesn't have to comply with Section 404 until fiscal years ended on or after April 15, 2005. Under the current rules, after the transition period the internal control attestation report will be a "standard" of public reporting just as is a report on financial statements. After the transition period, unless the SEC were to issue an exemption, companies getting ready to "go public" in the future will be required to have their controls audited, just as they will be required to have their pre-IPO financial statements audited. Thus during the transition period, a small-business issuer will not be required to have its financial reporting controls audited until fiscal years ended on or after April 15, 2005. After the transition period, a small-business issuer will be required to issue an internal control report for each year for which audited financial statements are required.

If the private company has a market capitalization in excess of \$75 million and is a calendar-year reporting company, the timing of the IPO is a factor to consider during the transition period. The following examples illustrate:

- Assume Company A is a calendar-year reporting company that goes public any time during 2003 with an equity float exceeding \$75 million. Company A cannot be designated an "accelerated filer" until December 31, 2004. A company's status can only change at the end of its fiscal year and, until December 31, 2004, the company will not have been subject to Exchange Act reporting for 12-plus months AND have filed one previous annual report (see Question 160 for conditions for accelerated filers).
- Assume Company B is a calendar-year reporting company that goes public January 15, 2004, with an equity float exceeding \$75 million. Company B cannot be designated an "accelerated filer" until December 31, 2005. A company's status can only change at the end of its fiscal year and, until December 31, 2005, the company will not have been subject to Exchange Act reporting for 12-plus months AND have filed one previous annual report.

In summary, a calendar-year reporting company that goes public in 2003 with a market capitalization exceeding \$75 million will need to comply with the annual internal control reporting requirements when it files the Form 10-K for the year ended December 31, 2004. If this company goes public during 2004, it will need to comply with the annual internal control reporting requirements when it files the Form 10-K for the year ended December 31, 2005.

163. Should a privately held company implement provisions of Sarbanes-Oxley?

This, of course, is a choice that management 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 SOA. 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.

164. What is the impact of the various state statutes on companies complying with SOA, and do these statutes apply to nonpublic companies?

The legislatures of various states are amending corporate statutes to replicate and, in some instances, even exceed the requirements of Sarbanes-Oxley. We understand some of these new state corporation laws will be far-reaching, affecting, for example, private firms as well as public companies. Many states have implemented reforms relating to audit committees and auditors in the wake of Sarbanes-Oxley. There are pending legislative initiatives in about 50 percent of the states at the time this publication went to print.

For example, a new California law requires all public companies operating in the state, including those subject to Sarbanes-Oxley, to report all stock options and loans made to their directors. These companies also must report information on bankruptcies, fraud convictions, and fines and violations of securities or banking laws by the company or its directors or officers. This law significantly expands upon the previous statutory requirements in that state. This is just one example in one state. Space does not permit detailing all of the various laws and initiatives in every state, as they vary significantly. Therefore, each company should inquire of its legal counsel to determine the initiatives, if any, that are pending in their respective state jurisdictions and whether the laws that have been passed require them to do anything different from SOA.

Glossary of Commonly Used Acronyms and Terms

The Act – Refers to the Sarbanes-Oxley Act of 2002 (see below). Also referred to as “SOA.”

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 38 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.

NASDAQ – The computerized stock exchange established by the National Association of Securities Dealers.

NYSE – The New York Stock Exchange.

PCAOB – The Public Company Accounting Oversight Board. Established by the Sarbanes-Oxley Act, PCAOB will oversee the audits of the financial statements of public companies through rigorous registration, standard setting, inspection and disciplinary programs. See Question 152 for more information.

Sarbanes-Oxley Act of 2002 – Corporate governance and oversight legislation signed into law on July 30, 2002. Also referred to as “Sarbanes-Oxley,” “SOA” 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 15 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 16 for more information.

SOA – The Sarbanes-Oxley Act of 2002. Also referred to as “the Act.”

Title IV – Refers to Title IV of the Sarbanes-Oxley Act of 2002.

Protiviti is the leading provider of independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. And we offer a full spectrum of internal audit services, technologies and skills for business risk management and the continual transformation of internal audit functions.