

# GUIDE TO THE SARBANES-OXLEY ACT: INTERNAL CONTROL REPORTING REQUIREMENTS



## Frequently Asked Questions Regarding Section 404

*Third Edition*

**protiviti**<sup>®</sup>  
Independent Risk Consulting

Business Risk

Technology Risk

Internal Audit

# Table of Contents

	Page No.
<b>Introduction</b>	1
<b>Applicability of Section 404 Requirements</b>	
1. Which companies are subject to the requirements of Section 404?	3
2. Are foreign companies subject to the requirements of Section 404?	3
3. Does Section 404 apply to small-business issuers?	3
4. Are unlisted companies with public debt required to comply with Section 404?	3
5. Are municipal utilities or universities that sell bonds required to comply with Section 404?	4
6. Do insured depository institutions (i.e., banks and savings associations) that are already complying with the requirements of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) have to comply with Section 404?	4
7.* What is the distinction between the requirements of FDICIA and the requirements of Section 404?	5
8. Does Section 404 apply to registered investment companies?	5
9. Does Section 404 apply to U.S. divisions of foreign-based companies?	6
10. Does Section 404 apply to not-for-profit entities?	6
11. Does Section 404 apply to asset-backed issuers?	6
12.* Does Section 404 apply to forward-looking financial information?	6
13.* Does Section 404 apply to the MD&A disclosures?	6
<b>What is Section 404 and How Does It Relate to Sections 302 and 906?</b>	
14. What does Section 404 require companies to do annually?	7
15. What does Section 404 require companies to do quarterly?	7
16. How often must management assess internal control over financial reporting?	8
17. Is Section 404 limited to public reports for which executive certification requirements are required?	8
18. What does Section 302 of the Sarbanes-Oxley Act require companies to do?	8
19. What does Section 906 of the Sarbanes-Oxley Act require companies to do?	10
20. How are the requirements under Section 404 and the requirements under Sections 302 and 906 of the Sarbanes-Oxley Act related?	10
21.* How does the Section 404 assessment enhance the Section 302 executive certification process?	11
22. Is there a value proposition from a controls assessment process beyond compliance with Section 404?	12
<b>When is Section 404 Effective?</b>	
23.* When do companies have to comply with the Section 404 requirements?	12
24. Why did the SEC defer the effective date of Section 404 compliance?	13

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

## Table of Contents (continued)

	Page No.
25. What happens if an issuer that is currently not an accelerated filer qualifies as an accelerated filer because of an increase in market capitalization? When does the issuer have to file an internal control report?	13
26. Assume Company A, which reports on a calendar year, plans to go public this year and is expecting a capitalization below the accelerated filing floor. When must it comply with Section 404?	14
27. When is the internal control report due?	14
28. How often must the independent accounting firm attest to management’s assertions regarding internal control over financial reporting?	14
29. As of what date is management’s annual assessment conducted?	14
30. May an issuer comply earlier than required under the final rules?	14
31. Is a quarterly assessment required and, if so, when?	14
32. If management is not required to assess internal control over financial reporting until the first internal control report is issued, what about the references to such internal controls in the quarterly executive certifications required by Section 302?	14
33. Now that the SEC has twice deferred the timing of Section 404, should companies defer their efforts to comply?	15

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

34. What is “internal control over financial reporting”?	16
35. What are “disclosure controls and procedures,” a key component of the certification requirements under Section 302?	17
36. What are examples of disclosure controls and procedures that generate required disclosures?	18
37. How should management design the disclosure controls and procedures so that the disclosure process will not become simply a ritual?	19
38. What should the certifying officers do when evaluating disclosure controls and procedures on a quarterly basis?	20
39. How is internal control over financial reporting distinguished from disclosure controls and procedures?	22
40. Are there examples of internal control over financial reporting that fall outside the realm of disclosure controls and procedures?	23

### **The COSO Internal Controls — Integrated Framework**

41. What is COSO?	23
42. What is the Internal Controls – Integrated Framework?	24
43. How is the COSO framework applied at the entity level in a Section 404 assessment?	25
44. How is the COSO framework applied at the activity or process level in a Section 404 assessment?	28
45.* Must the Section 404 compliance team address each of the five COSO elements in each process?	31
46.* Since the COSO framework includes internal controls over operational effectiveness and efficiency and over compliance with applicable laws and regulations, to what extent must management evaluate these controls to support the internal control report?	32

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

## Table of Contents (continued)

	Page No.
47. If a company already uses the COSO framework, is there anything more it needs to do to comply with Section 404?	32
48. Will the COSO framework on Enterprise Risk Management affect the Section 404 assessment?	33

### Getting Started With Section 404 Compliance

49. How does management get started?	33
50. How is the project team formed?	34
51. How should management articulate roles and responsibilities?	35
52. What should management consider when developing a project plan?	35
53. When planning the project, what key scoping decisions should be evaluated and what criteria should management consider when making these decisions?	36
54.* How does a company decide the “significant areas” to review for purposes of documenting and evaluating its internal control over financial reporting?	37
55.* How does a company assess materiality when prioritizing financial reporting elements?	37
56. What are “control units” and why are they important?	39
57.* How does management select the control units and locations to review?	39
58.* How does management define “a large portion” for purposes of determining multilocation coverage?	42
59. How should management communicate the project effort to the organization?	43
60. What steps should be included in the project plan?	43
61. To what extent can companies rely on prior controls documentation?	44
62. How should companies document and validate their assessments of internal controls?	44
63.* What tools and technologies are used to implement controls repositories, document process maps, facilitate the assessment process and manage overall Section 404 compliance?	45
64. Is there a way to estimate the effort and cost of complying with Section 404 in Year One?	45
65. Will companies need to add internal resources to comply with Sections 404 and 302?	46
66. Is a cultural assessment necessary?	46

### Identifying Reporting Requirements and Relevant Processes

67. Can management use a risk-based approach for determining the extent to which internal controls should be documented and validated?	48
68. What standards and criteria should be set before beginning the project?	50
69. Are all transactions evaluated in a similar manner when understanding transaction flows and the related controls?	50
70.* How are the critical processes identified?	51
71.* What is a “reasonable” number of business processes for purposes of Section 404 compliance?	52
72. What role do process owners play?	52

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

## Table of Contents (continued)

	Page No.
<b>Summarizing Risks and Developing Control Objectives</b>	
73.	Why identify risks? 52
74.*	How are risks identified? 53
75.	What are control objectives and how do they relate to risks? 53
76.	How are control objectives defined? 55
<b>Integrating Fraud Considerations into the Assessment</b>	
77.*	What is the scope of an antifraud program and controls? 55
78.*	What's new and what really matters with respect to fraud? 56
79.*	What suggested steps should management take with respect to fraud? 56
80.*	How are fraud risks assessed? 58
81.*	How should management get started with integrating fraud considerations into the Section 404 assessment? 58
<b>Identifying, Documenting and Assessing Controls</b>	
82.	Does the SEC provide any guidance to management for purposes of evaluating internal control over financial reporting? 59
83.	Does the SEC provide any guidance to management for purposes of documenting its evaluation of internal control over financial reporting? 59
84.	How is the entity-level assessment conducted? 60
85.*	How are entity-level controls validated? 61
86.	Are entity-level controls the same thing as entity-wide controls? 64
87.*	How are IT risks and controls considered? 64
88.*	What if transaction processing is outsourced? 66
89.*	Do SAS 70 reports apply to processes other than IT and to specialists? 69
90.	Where does an entity-level controls review end and a process controls review begin? 69
91.	How is the process- or activity-level assessment conducted? 70
92.*	What are walkthroughs, why are they necessary and how should the Section 404 compliance team prepare for them? 71
93.*	How are processes and transaction flows documented? 73
94.	What are some examples of control activities? 76
95.	When and how should the period-end financial reporting process (close the books) be evaluated? 78
96*	What are examples of controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles? 79
97.*	What should the Section 404 compliance team consider when documenting controls over estimation transactions? 79
98.*	What is the external auditor looking for with respect to the period-end financial reporting process (close the books)? 80

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

## Table of Contents (continued)

	Page No.	
99.*	What factors are considered when evaluating the design effectiveness of controls?	80
100.	What factors are considered when evaluating the operating effectiveness of controls?	81
101.*	Must a company link its key controls directly to financial statement accounts?	82
102.	What level of assurance must management attain when reaching a conclusion on the design and operating effectiveness of internal controls?	82
103.	How does management define “reasonable assurance” for purposes of evaluating the effectiveness of controls?	82
104.	How should control gaps be identified and summarized?	83
105.	What should be done to address control gaps if any are found during the assessment?	86
106.*	How does a company define a “control deficiency”?	87
107.*	How are compensating controls considered?	88
108.*	How does a company define a “significant deficiency” in internal control?	88
109.*	How does a company define a “material weakness” in internal control?	90
110.*	Why is the distinction between a significant deficiency and a material weakness so important?	93
111.	How does a company define a “significant deficiency” or “material weakness” in the so-called “soft control” areas?	93
112.	What if there is a “significant deficiency” or a “material weakness” in internal control?	93
113.	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?	94
114.	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?	94
115.	Can management rely on the self-assessments of process owners as the sole basis for rendering the annual internal control report?	94
116.	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?	94
117.	What does it mean that the Section 404 assessment is based on a point in time and why is it important?	94
118.	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?	95

### Validation of Operating Effectiveness (“Testing of Controls”)

119.*	What approaches are recommended for “testing” the effectiveness of internal control over financial reporting?	95
120.*	Who is responsible for validating operating effectiveness?	96
121.	What is “testing of controls”?	96
122.	How does management test controls that do not leave a trail of documentary evidence?	97
123.	How can inquiries or interviewing be considered “tests” of controls?	97

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

## Table of Contents (continued)

	Page No.
124. What is reperformance?	97
125. When are tests of controls performed?	98
126.* What is a testing plan?	98
127.* Why is it important to define the failure conditions before beginning testing?	101
128.* How does the evaluation team ascertain the test period?	102
129.* How does management select testing method(s) to apply in specific circumstances?	103
130.* How does management determine the appropriate sampling method?	105
131.* How is judgmental sampling applied?	106
132.* How is statistical sampling applied?	107
133.* How does management determine sample size?	108
134.* How is the sample selected from the population?	109
135.* How does management finalize the formal testing plan?	109
136.* How often must the testing plan be executed?	110
137.* How are testing results documented?	110
138.* How are testing results evaluated?	111
139.* How does management decide which controls to test?	113
140.* How does management decide the extent of testing?	116
141. Why are control descriptions important and how does management know they are adequate?	118
142.* How should the Section 404 compliance team classify individual control techniques so that the team, as well as the independent auditor, can more effectively plan the required tests of controls?	118
143. Is testing by process owners acceptable for purposes of supporting management's assertion?	120
144.* With respect to the period between the date management completes its preliminary evaluation of operating effectiveness and year-end, what must management do to update its evaluation?	120
145. What should management do when exceptions are identified?	121
146. How is monitoring evaluated?	122
147. How are pervasive process controls tested?	123
148. How are information process controls tested?	123
149. How are IT controls tested?	124
150.* How much testing should management perform relative to the testing the external auditor performs?	125
151.* What should the Section 404 compliance team do if a significant level of exceptions is encountered during testing?	125
152.* How many exceptions are acceptable before a control deficiency is deemed to exist?	125
153. What if the external auditor's testing results differ from management's results?	126
154.* Should the external auditor participate during management's testing process?	127

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

## Table of Contents (continued)

	Page No.
<b>Remediation</b>	
155.* If control deficiencies or gaps are identified, how should we remediate them?	127
156. Assume a company identifies a material weakness in internal control and remedies that deficiency during the year it is required to comply with Section 404 under the SEC's rules. How soon before the end of the fiscal year must the deficiency be corrected?	127
157.* Since this Section 404 project requires a point-in-time review, for how long do remediated controls need to be in place and in operation to be considered effective?	128
<b>Special Circumstances and Situations</b>	
158.* How does management evaluate the company's internal control with respect to unconsolidated investments accounted for under the equity method?	128
159.* How are material acquisitions occurring during the fiscal year handled for purposes of determining the scope of the Section 404 assessment?	128
160.* How are divestitures of significant entities (or net assets) and discontinued operations considered for purposes of evaluating internal control over financial reporting?	129
161.* How does a lag in reporting of the financial results by certain foreign subsidiaries for financial reporting purposes affect the assessment of internal control over financial reporting?	130
162.* How are certain entities consolidated based on characteristics other than voting control, including certain variable interest entities and entities accounted for via proportionate consolidation, handled for purposes of determining the scope of the Section 404 assessment?	130
163.* If controls are replaced or eliminated during the period before the end of the year, must the evaluation team test them?	131
<b>Reporting</b>	
164. How should management formulate conclusions with respect to internal control over financial reporting?	131
165. What should be communicated to executive management, project sponsors and the board?	132
166.* What is the internal control report?	132
167.* When management identifies a control deficiency that is deemed to be a material weakness in internal control over financial reporting, must the company disclose the weakness in its public reports even though the weakness may be corrected prior to the end of the year? If so, when is this requirement effective?	133
168.* If the Section 404 compliance team determines at year-end that there are control deficiencies deemed to be significant deficiencies in internal control over financial reporting, are there circumstances requiring public disclosure of these deficiencies in connection with the filing of the internal control report?	133
169.* How is materiality considered for purposes of evaluating the effects of changes on internal control over financial reporting?	133
170.* Must management disclose improvements to internal controls?	134
171. What are the form and content of the internal control report?	134
172. Where is the internal control report included in Form 10-K?	134

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

## Table of Contents (continued)

	Page No.
173. Can the results of the assessment of internal control over financial reporting affect the company's executive certification under Sections 302 and 906?	134
174.* What impact would a conclusion that the internal controls are ineffective have on the company?	135
175.* What happens if a company completes its Section 404 assessment and files an unqualified internal control report, and subsequently restates its financial statements for the applicable period?	135
176.* What documentation does management need to support the assertions in the internal control report?	137
177.* How long must management retain the documentation supporting the assertions in the internal control report?	139

### Moving Beyond the Initial Year One Assessment

178.* Why should certifying officers care about the SOA Section 404 compliance structure going forward after the first internal control report is filed?	139
179.* What are the elements of an effective SOA Section 404 compliance structure after the initial annual assessment is completed?	140
180.* How are process owners engaged going forward?	141
181.* How does self-assessment work going forward?	141
182.* Why do process owners need support going forward?	142
183.* What are alternative structures for supporting process owners in complying with SOA Section 404 after the initial annual assessment?	143
184.* How does the maturity of a company's business processes affect the sustainability of its internal control structure?	146
185.* How do companies "find the value" from Section 404 going forward?	147
186. After the initial annual assessment, how does management conduct the quarterly evaluations of those elements of internal control over financial reporting that are a subset of disclosure controls and procedures?	147
187. After the initial annual review of control effectiveness is completed, should management assess changes to the company's risk profile on a quarterly basis?	148
188. Will subsequent annual assessments be similar to the initial annual assessment?	149
189.* Going forward, what will happen to Section 404 compliance costs?	149

### Role of Management

190. What is the role of the disclosure committee?	149
191. What is the role of the Section 404 compliance project sponsor?	151
192. What is the role of the Section 404 compliance project steering committee?	151
193. 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?	151
194. What is the role of other executives?	152
195. Who signs off on internal control over financial reporting?	152

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

## Table of Contents (continued)

	Page No.
196. What communications, if any, are required of management beyond the quarterly executive certifications and annual internal control report?	152
197. What is the role of operating and functional unit managers?	152
198. Can management rely solely on self-assessments of process owners for purposes of their evaluation of design and operating effectiveness?	153
199. Can management rely on the work of the internal auditors?	153
200. To what extent can management rely on the work of the independent public accountant in making the assessment of internal controls effectiveness?	153

### Role of Internal Audit

201.* What is current status of the NYSE requirement that listed companies have an internal audit function?	153
202.* What should companies do if they are listed on other exchanges? Are they required to have an internal audit function?	153
203. 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?	154
204. What is the role of internal audit in the evaluation process?	154
205* What changes in internal audit can be expected as a result of Section 404?	154

### Role of the Independent Public Accountant

206. When and how should the independent public accountant be involved during management's annual assessment process?	155
207. How should management prepare for the attestation process?	155
208. Did the SEC provide any guidance with respect to the attestation report?	155
209.* What does the PCAOB require with respect to the attestation report?	156
210.* How will the auditor evaluate management's assessment of internal control over financial reporting?	156
211.* What happens if management decides to forego the documentation and testing necessary to support a conclusion on internal control over financial reporting?	156
212. What internal control "design" assistance can the independent public accountant provide without impairing independence?	156
213. Can the independent public accountant perform any testing on behalf of the audit client?	156
214. Can the company use its independent public accountant's software and/or methodology to support management's assessment?	157
215. Can the company engage the independent public accountant to create original documentation of its internal control over financial reporting without impairing independence?	158
216. What kind of work can management expect of the company's independent public accountant during the attestation process?	160
217.* Can management share interim drafts of the financial statements with the auditor?	160

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

## Table of Contents (continued)

	Page No.
218.* Can management discuss accounting issues with the auditor?	160
219. Can management rely on the statutory audit work performed by the external auditor for significant subsidiaries or joint ventures?	161
220.* Can the external auditor use the work of the internal audit function and others for purposes of performing an audit of internal control over financial reporting?	161
221.* Can the independent auditor issue a report to management or the audit committee indicating that no significant deficiencies were noted during an audit of internal control over financial reporting?	162
222.* Will the SEC accept an adverse opinion on internal control over financial reporting?	162
223.* What is required of the independent auditors each quarter?	162
224.* Can the same audit firm issue an opinion on internal control over financial reporting of a user organization and also issue the SAS 70 letter pertaining to a service organization to which the user organization has outsourced a significant process?	163

### Role of the Audit Committee

225.* With respect to the financial reporting process and internal control over financial reporting, what is expected of the audit committee?	163
226. How and when should the audit committee be involved in management's evaluation process and in the independent public accountant's attestation process?	164
227. What questions are audit committees asking with respect to Section 404 compliance?	164

### Impact on Sections 302 and 906

228. What is the impact of the Section 404 rules on Sections 302 and 906?	165
229. What is the effective date of the new exhibit requirements for Sections 302 and 906?	166
230. May certifying officers cite "reasonable assurance" when referring to the company's disclosure controls and procedures?	166
231.* Why are companies reporting control deficiencies that are not material weaknesses?	166
232.* What are the common types of control deficiencies being reported by public companies?	167
233.* What are the demographics of companies reporting control deficiencies?	167

### Accelerated Filing Requirements

234. What are the new filing requirements with respect to Form 10-K and Form 10-Q?	168
235. 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"?	168
236. 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?	169
237.* If a calendar year reporting company meets the requirements as an accelerated filer for SEC reporting purposes as of December 31, 2003, what is its Section 404 compliance status if its market cap subsequently falls below \$75 million as of June 30, 2004?	169

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

## Table of Contents (continued)

	Page No.
<b>Private Companies and Initial Public Offerings</b>	
238. 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?	170
239. 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?	170
240. When must a calendar year reporting company comply with Section 404 when it goes public and has an initial capitalization below the accelerated filing floor?	171
241. Should a privately held company implement provisions of Sarbanes-Oxley?	171
242. What is the impact of the various state statutes on companies complying with SOA, and do these statutes apply to nonpublic companies?	171
243.* Assuming a June 30 year-end company goes public on September 30, 2004, is the first Section 302 certification required to be included in the first 10-Q for the quarter ended December 31, 2004, or will the company be required to certify as of September 30?	171
<b>U.S. Nonaccelerated Filers</b>	
244.* Is Section 404 applied differently to smaller companies?	172
245.* Can public companies rely on their external auditor to compute the tax provision and reserves included in their financial statements?	172
<b>Foreign Filers and Locations</b>	
246.* Are foreign filers subject to the Section 302 executive certification requirements?	172
247.* Based on experiences to date by U.S. accelerated filers, what are the lessons for foreign filers who have just begun their compliance efforts?	172
248.* Must the Section 404 documentation prepared in countries outside the United States be presented in English?	173
<b>Other Specific Matters Relating to PCAOB Auditing Standard No. 2</b>	
249.* What is the Public Company Accounting Oversight Board (PCAOB)?	174
250.* What is the impact of the PCAOB's conclusion that business continuity and contingency planning are not part of the audit of internal control over financial reporting?	174
251.* What is the PCAOB's view on the applicability of safeguarding of assets to an assessment of internal control over financial reporting?	175
252.* Will the PCAOB issue further guidance regarding the independent public accountant's attestation requirements and standards? If so, when?	175
<b>Glossary of Commonly Used Acronyms and Terms</b>	
	176

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

This booklet supplements the one we issued pertaining to the rules of Sections 302 and 906. While those rules have not significantly changed since *Frequently Asked Questions Regarding the Sarbanes-Oxley Act Executive Certification Requirements* was published, there have been some important changes. The SEC’s Section 404 rules modify the existing requirements of Section 302, including the executive certification itself. These modifications are discussed in this publication.

This publication is a third edition. It addresses the effects of changes arising from the SEC’s final rules released in June 2003 and as amended by the Commission’s extension of these rules released February 24, 2004. It includes questions directed to foreign filers and U.S. domestic non-accelerated filers and is updated for relevant requirements of Auditing Standard No. 2 issued by the Public Company Accounting Oversight Board and other questions we have received from time to time. It also reflects responses to frequently asked questions the SEC and PCAOB have published through the date this book was released to print.

Other Protiviti publications addressing questions germane to Section 404 compliance are also available. These publications include *Guide to Internal Audit: Frequently Asked Questions About the NYSE Requirements and Developing an Effective Internal Audit Function* and *Guide to the Sarbanes-Oxley Act: IT Risks and Controls*. Both are available at [www.protiviti.com](http://www.protiviti.com).

*continued*

This publication is not intended to be a legal analysis. Nor is it intended to be a detailed “cook book.” Accordingly, companies should seek legal counsel and appropriate risk advisors for advice on specific questions as they relate to their unique circumstances. Companies should also seek input from their independent auditors on appropriate issues. They should also expect some of the issues addressed in this publication to continue evolving. Companies can obtain a copy of the SEC’s final rules and the SEC staff’s responses to frequently asked questions at [www.sec.gov](http://www.sec.gov). Companies can also obtain a copy of the PCAOB’s Auditing Standard No. 2 and the PCAOB staff’s responses to frequently asked questions at [www.pcaobus.org](http://www.pcaobus.org).

Protiviti Inc.  
August 2004

---

## 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 as to whether nonpublic subsidiaries of public companies must comply with Section 404. Although the subsidiary has no obligation to file a separate report with the SEC, the subsidiary’s issuer parent will need to evaluate the subsidiary’s controls and procedures if the subsidiary or any part of it is deemed to be significant to an understanding of the issuer parent’s overall internal control structure. The PCAOB reaffirmed this point of view when it issued Auditing Standard No. 2.

### 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 July 15, 2005 (instead of the November 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 their conclusions regarding the effectiveness of their internal control over financial reporting and disclosure controls and procedures only in their annual report and not on a quarterly basis. These issuers are not subject to the quarterly reporting requirements under the Exchange Act.

### 3. Does Section 404 apply to small-business issuers?

Yes. The final rules apply to all companies that file Exchange Act periodic reports, regardless of their size (except registered investment companies and asset-backed issuers). The SEC recognized, however, that many 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 July 15, 2005 (instead of the November 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 Section 302 executive certification and Section 404 internal control assessment requirements because the SEC has made those requirements an integral part of Forms 10-Q and 10-K (and the accompanying exhibits). 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 Section 302 certifications and internal control report. However, Section 906 certifications are not required of voluntary filers.

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

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

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

- (1) A statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting
- (2) Management's assessment of the effectiveness of the institution's internal control structure and procedures for financial reporting as of the end of the fiscal year
- (3) An attestation report prepared by the institution's independent accountant

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

After consultation with the staffs of other federal agencies, the SEC decided to provide flexibility in satisfying both sets of requirements to insured depository institutions subject to Part 363 of the FDIC's regulations (as well as holding companies permitted to file an internal control report on behalf of their insured depository institution subsidiaries in satisfaction of these regulations) and also subject to the final rules implementing Section 404 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. What is the distinction between the requirements of FDICIA and the requirements of Section 404?**

Although the Commission's rules are similar to the FDIC's existing internal control reporting requirements, they differ in several respects. For example, the SEC's rules do not require a statement of compliance with designated laws and regulations relating to safety and soundness, whereas the FDIC's rules do require such a statement. However, if a compliance issue arose, it would clearly have disclosure implications. Conversely, the following provisions in the 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 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 the company's internal control over financial reporting is effective if there are one or more material weaknesses
- The requirement that the company state 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

## **8. Does Section 404 apply to registered investment companies?**

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

#### **9. 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.

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

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

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

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

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

No. Section 404 is focused on the historical financial statements (which, by definition, include the footnotes). With respect to the disclosure of financial projections and similar forward-looking information on analyst calls and in other public venues such as shareholder meetings, such disclosures must be consistent with information provided in public reports. For example, the SEC has said disclosures of financial information for a completed fiscal period in a presentation that is made orally, telephonically, by webcast, by broadcast, or by similar means will not be required to be filed, if (1) the presentation occurs within 48 hours of a related release or announcement that is filed on Form 8-K; (2) the presentation is broadly accessible to the public; and (3) the information in the webcast is posted on the company's website. The information in these various venues must be consistent with the information included in financial and public reports.

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

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

---

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

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

Section 404 of 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 also an assertion by management that there are no material weaknesses in such internal control. The new rules require disclosure to the public of any material weaknesses identified by management during the assessment.

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. In Auditing Standard No. 2, the PCAOB adopted a "single auditor/multiple report" model in which, in addition to opining on the financial statements, the external auditor must express two additional opinions: (1) one on management's assessment of internal control over financial reporting, and (2) the other on the effectiveness of internal control over financial reporting. Therefore, in addition to auditing and expressing an opinion on internal control over financial reporting, the auditor also evaluates and expresses an opinion on the assertions expressed in management's internal control report. For most companies, this new attestation requirement under Section 404, as further articulated by the SEC and PCAOB, expands the scope of the accounting firm's audit procedures beyond the work required solely to render an opinion on the financial statements.

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

With regard to internal control over financial reporting, the SEC decided not to require quarterly evaluations that are as extensive as the annual evaluation. The Commission is of the view that management should perform 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 disclose any change in controls that occurred during a fiscal quarter that has materially affected, or is reasonably likely to materially affect, the company's internal control over financial reporting. Although the final rules do not explicitly require the company to disclose the reasons for any change that occurred during a fiscal quarter (including the fourth quarter), or to otherwise elaborate

about the change, a company will have to determine, on a facts and circumstances basis, whether the reasons for the change, or other information about the circumstances surrounding the change, constitute material information necessary to make the disclosure about the change not misleading.

The quarterly certification requirement under the Section 302 rules with respect to management's timely disclosure of significant deficiencies and 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 8 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.

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

The SEC's rules for compliance with Section 404 require management to make an annual assessment of the company's internal control over financial reporting and to evaluate quarterly the impact of changes on such controls. These evaluations are accomplished in conjunction with each filing of a quarterly report and with the filing of the annual report (in which an internal control report must be included).

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

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

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

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 230).

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 32). 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.

## 19. 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.

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

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

Comparison of Sections 302, 404 and 906			
	302	404	906
When is it effective?	August 29, 2002	Fiscal years ended on or after: • November 15, 2004, for accelerated filers • July 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 39.

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

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

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

The SEC’s rule on Section 302 recommends a disclosure committee. Many companies also have formed a Section 404 project steering committee. Question 193 provides commentary as to the interrelationships between these two committees as they address common issues of mutual interest, e.g., formatting the internal control report, criteria for identifying and reporting significant deficiencies and material weaknesses, evaluating internal control-related disclosures, etc.

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

These are some of the ways the Section 404 assessment process enhances the Section 302 executive certification process. See Questions 178 through 189 for a discussion of alternative structures for complying with Sections 302 and 404 after the first internal control report is filed.

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

Yes. 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?

### 23. 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 November 15, 2004, amounting to a delay of 13 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 16, 2005 (75 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 July 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 during March 2006. This additional eight-month extension (beyond the November 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 and if they wisely take advantage of the additional time to prepare.

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 November 15, 2004. In addition, similar to other companies (as noted in Question 32), 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.

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

The Commission has twice deferred the effective compliance date. With respect to the first deferral, the SEC staff indicated in its May 27, 2003, open meeting 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 needed time to gear up for these new requirements.
- Finally, the PCAOB, created by Congress in summer of 2002, needed additional time to develop its rules on the independent auditor's attestation report on management's assertions as to 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 control deficiencies to close gaps can now be accomplished over a longer period of time, provided that companies take advantage of the additional time. The longer transition period was appropriate in light of both the substantial time and resources needed by companies to properly implement the rules, and the corresponding benefit to investors that would result from companies' proper implementation of the new requirements.

With respect to the second deferral, the Commission noted that companies with June, July and August fiscal year-ends that were in the process of documenting and evaluating controls have based their processes on the PCAOB's proposed standard. These and other companies requested the Commission and the PCAOB provide additional time for compliance. The SEC concluded that an extension of compliance dates for the internal control over financial reporting requirements was necessary to minimize the cost and disruption of implementing a new disclosure requirement under a current standard that was about to be superseded. The SEC therefore provided companies and their auditors more time to perform additional testing or remediation of controls based on the final standard, which the PCAOB issued on March 9, 2004.

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

The significance of this question to Section 404 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 235 and 236. Market capitalization is relevant to determining whether a company is an accelerated filer. The breakpoint is \$75 million and, for a given fiscal year, 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 23 and 236, 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 must pay close attention to this determination. For example, depending upon their current market capitalization, business plans and the market in general, smaller companies that are dynamic, growing, acquisitive and/or planning to tap the

equity markets need to be careful about deferring compliance with Section 404 because they could find themselves in crisis mode to comply.

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

As noted in Question 23, 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 November 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. Therefore, if the company goes public in 2004, it need not comply until its first 10-K for a fiscal year ending on or after July 15, 2005. However, the result might be different for a voluntary filer that goes public during 2004.

**27. 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 16, 2005.

**28. 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.

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

Management’s annual assessment of internal control over financial reporting is a point-in-time assessment as of the end of the company’s fiscal year. Management may test and evaluate the controls over a period of time during the year, but the assessment must be made at a single point in time (i.e., did the necessary controls exist at the end of the financial period and were they operating effectively at that time?). However, to support this assessment, it is necessary to demonstrate operating effectiveness over a sufficient period of time (see Questions 128 and 157).

**30. 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 evolving 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.

**31. 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.

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

As noted in Question 18, the executive certification makes references to internal control over financial reporting. The SEC’s 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 weaknesses in internal control, as well as any fraud involving employees who have a significant role in internal control.

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

Given the calendar, this question primarily applies to companies that are not required to comply until 2005 and beyond. If these companies hold out hope of a third deferral by the SEC, they are making a huge casino bet.

By twice deferring the effective date, the SEC intended to provide companies and their auditors more time to do a thorough job. Regardless of their timetable for compliance and whether they are an accelerated filer, a domestic non-accelerated filer or a foreign filer, companies should think through what they need to do, when they need to do it and why. For example, for companies that must comply with Section 404 in annual reports filed in 2005, what does management want to accomplish during 2004 in preparing for compliance and why do they want to accomplish it? What is the external auditor’s deadline for completing the evaluation during the initial year of compliance? What external message is management planning during the months prior to filing the first internal control report? How can management accomplish the project and the attestation process more cost effectively given the time available?

For companies that do not have to comply until later in 2005 or in 2006, we recommend they plan to complete the evaluation of “control design effectiveness” as soon as possible, so that they can focus on evaluating the effects of change on design during the year they must comply. These companies should also plan 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. These practices are consistent with the efforts of many accelerated filers during 2003 as they prepared for compliance during 2004.

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? For 2004, most auditors have asked their clients to have everything documented for their attestation process by no later than the end of the second or third quarter. In many instances, auditors are reviewing controls documentation prior to the end of the second quarter.

- 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.
- 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 with preparations for Section 404 compliance 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.

This advice is as timely now as it was in 2003.

---

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

### 34. What is “internal control over financial reporting”?

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

A process designed by, or under the supervision of, the issuer’s principal executive and principal financial officers, or persons performing similar functions, and effected by the issuer’s board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

- pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;
- provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and
- provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer’s assets that could have a material effect on the financial statements.

While the above definition is consistent with the COSO Framework, it also incorporates language from 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).

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

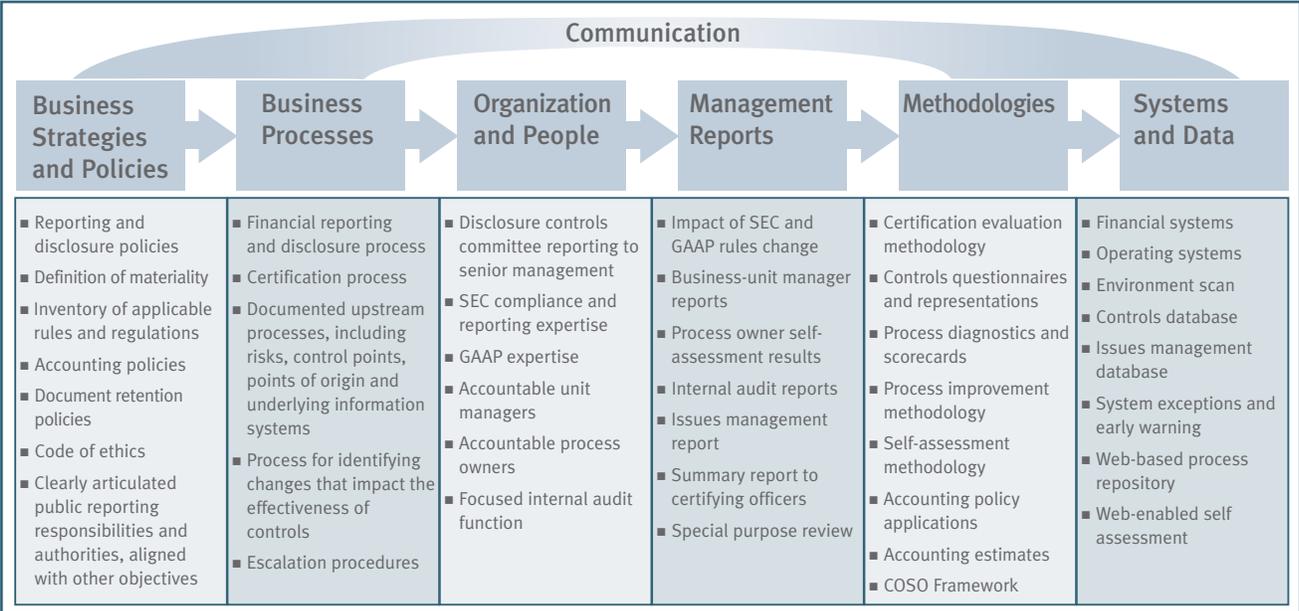
The SEC introduced “disclosure controls and procedures” as a new term in its August 29, 2002, release. Disclosure controls and procedures are controls and other procedures designed to ensure that information required to be disclosed by the company in its Exchange Act reports is recorded, processed, summarized 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 36, 37 and 38.

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

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

- Form a disclosure committee to organize and oversee the disclosure process. Many companies have adopted some form of a disclosure committee. For example, based on a study published in September 2003, Protiviti found that almost 75 percent of companies with more than \$500 million in annual revenues had formed a disclosure committee. This committee considers the materiality of information, determines disclosure requirements on a timely basis, identifies relevant disclosure issues, and coordinates the development of the appropriate infrastructure to ensure quality material information is disclosed in a timely manner to management for potential action and disclosure. If a company forms a disclosure committee, it is important that the committee discharges its assigned functions and activities as articulated in its charter. It doesn't help to form a disclosure committee and define its tasks, only then to fail in execution. However, if a disclosure committee isn't in place, the company's certifying officers must address how they will achieve the specified tasks a committee is intended to achieve. See Question 190 for further discussion.
- Use a standard reporting package or process to engage the appropriate unit managers and process owners, and funnel the required information upward. This upward communication is vital to effective disclosure controls and processes. While a standard reporting package is a common practice followed by many companies, we see companies enhancing their reporting packages to facilitate upward communications of material information from unit managers and process owners and making them an integral part of the disclosure process. For example:

One company developed a standard monthly reporting package for all operating units that included, among other things, a representation letter, an analysis of variations and fluctuations in operations, an internal control evaluation, a risk assessment relating to changes in operations (e.g., changes in personnel, changes in systems, changes in business practices, etc.), a summary of related parties, and the financial statements. The company's disclosure committee reviews each reporting package, follows up on questions and significant unresolved issues, and documents the results of that follow-up. The reporting packages are subject to review by internal audit and the independent public accountant. This process funnels upward information about new risks, changes and issues to management and, ultimately, to the certifying officers.
- Inventory the reporting requirements and maintain a current inventory. Regulation S-K, Regulation S-X, up-to-date GAAP checklists and other checklists provide a basis for determining the universe of reporting requirements. Management or the disclosure committee should use these checklists to determine the applicable requirements and ensure the requisite policies, activities and subject-matter expertise are brought to bear so that an effective infrastructure is in place to identify, record, process, summarize and report the required information.
- Design and implement a process to address each required disclosure. Once the disclosure requirements are identified, management should 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 into appropriate segments, assigning segments by responsible function (e.g., operations, HR, GC, treasury, insurance, investor relations, etc.) and working backwards to identify the relevant processes that record, process, summarize and report that information. These processes should be ranked according to criticality using appropriate criteria, such as pervasiveness of importance to the company's operations, impact on public reports, susceptibility to change, potential for material errors, etc.

Every company must decide the level of granularity that is appropriate for their circumstances.

Following are some points to consider:

- The owner of the period-end financial reporting process manages the accumulation of the necessary data and information through a disclosure control used to monitor completion, much like a project management organization (PMO) (see Question 49). As noted earlier, an up-to-date disclosure checklist is useful for reviewing submitted drafts for completeness.
- For items that are relatively simple and straightforward, the appropriate disclosure control might be to focus on using the disclosure checklist and reporting timeline, assigning the relevant segment by function, as noted above, and the date due. Often, there is a presumption that the requisite information and data within a given disclosure segment would be provided consistent with the prior year. Take the description of facilities, for example. Does the company need to document the process that the real estate function uses to generate the list of facilities or is the responsibility for the disclosure assigned to the real estate function with a firm deadline? If the facilities are relatively stable year-to-year and can even be reviewed for reasonableness by financial statement preparers who are knowledgeable of the business, it probably is adequate to include the item on the disclosure checklist with responsibility assigned to the real estate function. On the other hand, if there are numerous acquisitions and divestitures during the year and such activity is expected in future years, it may be appropriate to document the process.
- When a particular disclosure segment has multiple data sources to generate, it may be necessary to understand and document the process by which the required data is obtained, compiled and organized. The supplementary schedules might be an example of this. The MD&A might require specific calculations, but many of those can be referenced to the financial statements. Operating data comes from operating information, and the source of that information and its reliability should be understood due to the criticality of ensuring the MD&A disclosures are reliable. A good portion of the MD&A is variance explanation from operations. Accordingly, the MD&A should be supported by operating reports and have direct input and review by operating management.
- Decide how the company's collective knowledge will be captured and summarized for certifying officers to ensure timely action and disclosure. At least initially, a simple process should be in place to facilitate the flow of material information. This could be nothing more than formalizing existing disclosure processes. For the company requiring monthly reporting packages, as illustrated earlier, the disclosure committee forwards each unit's package to the CEO and CFO – the certifying officers – who review them as part of their ongoing evaluation process. Some companies use regular conference calls with business-unit managers to identify new risks and emerging issues requiring attention.

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

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

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

- Monitor change, both externally and internally. Changes in the environment and in the company's operations require special emphasis to evaluate their impact on the business, the financial statements and the required disclosures. Examples of changes requiring evaluation include mergers and acquisitions, divestitures, new innovative business practices, new systems, changes in personnel, significant market declines, and changes in laws and regulations. The disclosure committee, or an equivalent group of executives, should be designated with the responsibility to monitor change for purposes of identifying material information requiring disclosure. As noted in Questions 179 and 187, a change-recognition process is a critical element of an ongoing SOA Section 404 compliance structure.
- Identify the primary business risks associated with company operations and the critical information essential for measuring, monitoring and reporting on each risk; in view of such risks, evaluate current disclosures to determine whether additional information is needed. Senior management and the board should concur as to the company's primary business risks, the appetite or tolerance for such risks, and the plans for managing and monitoring the company's exposure to losses and potential for profits from such risks. As management recommends to the board specific strategies and plans for action, they should articulate the risks inherent in such strategies and plans, and evaluate the consistency of their recommendations with their expressed risk tolerance. The board, in turn, must understand and agree with management's assessment of and tolerance for risk and the impact of their recommendations on the organization's risk profile. An explicit understanding of the organization's risks and the uncertainties inherent in its performance goals will assist management in identifying material information for disclosure in public reports. Management's assessment of business risk and the related impact on disclosure in public reports should be continuously updated over time. Our point of view is that an enterprise risk management capability would facilitate an organization's disclosure process.
- 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. See Question 179 for a discussion of the key elements of an ongoing Section 404 compliance structure, which enhances the quality of a company's disclosure controls and procedures.

### **38. 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 deficiencies, the impact of changes from prior periods and other areas of concern representing changes from previously issued annual or quarterly reports. Thus management may decide that a complete evaluation is not needed every quarter to satisfy the spirit of the certification requirements and that the certification process should focus on change. Even though there is an expectation that an evaluation of overall effectiveness is conducted each quarter, the emphasis should be on the impact of changes in controls and procedures and in their performance.

Disclosure controls and procedures are the means by which the certifying officers assume responsibility to ensure they (or someone they designate) receive in a timely manner the reliable material financial and nonfinancial information needed to enable them to certify to the fairness of public reports. We believe that disclosure controls and procedures should evolve over time until a process-based "chain of accountability" is in place. This begins with understanding and documenting key 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 periodic public reports, including the related disclosures?
- Discuss with key personnel involved in the process whether there are any unresolved issues with respect to disclosures or financial reporting?
- Take a close look at areas where there is a 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.
- Keep a close eye on areas where potential control deficiencies may exist? For example, certain types of control deficiencies occur most frequently, based on disclosures by public companies. These include inadequate financial personnel, revenue recognition, account reconciliations, segregation of duties and review, monitoring and analysis.
- Discuss with the independent public accountants whether they have any concerns that could increase the company's compliance risks?
- Discuss the company's disclosure controls and procedures with the audit committee to confirm it is satisfied with them?
- Follow up on open areas, e.g., disagreements with the independent public accountants, prior SEC comments, concerns of the audit committee, violations of the code of conduct, significant audit or other adjustments, issues raised by whistleblowers, instances or allegations of fraud, questions from analysts, and unresolved issues in the internal audit report?

### **39. 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

**40. 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

**41. 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.

**42. What is the Internal Controls – Integrated Framework?**

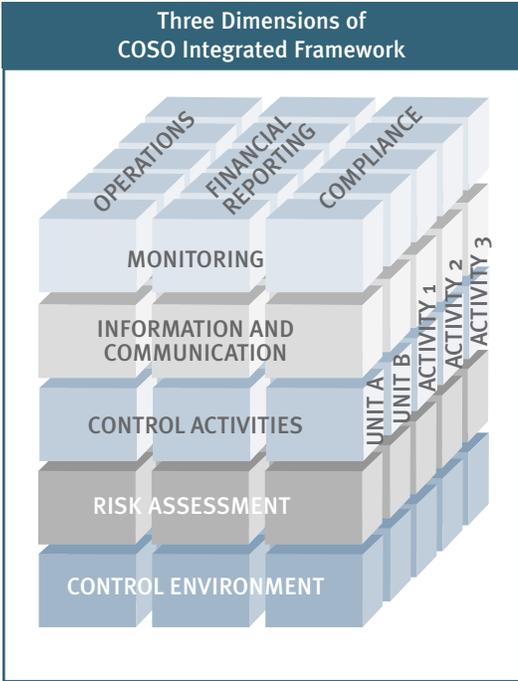
The COSO Internal Controls – Integrated Framework defines internal control as a “process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (a) reliability of financial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

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

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.



Source: COSO Internal Controls – Integrated Framework

- 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 historically has embraced the COSO framework since it was issued. When the PCAOB issued Auditing Standard No. 2, the Board reaffirmed the COSO report as providing “a suitable and available framework for purposes of management’s assessment” of internal control over financial reporting. Banks complying with FDICIA (see Questions 6 and 7) have used COSO.

If management decides not to use COSO, an alternative framework must be selected. Any framework management chooses to use must meet the SEC’s criteria. If a company chooses to use a non-COSO framework, 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.

#### **43. 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.

The PCAOB refers to entity-level controls as “company-level controls.” These are the controls that management relies on to establish the appropriate “tone at the top” relative to financial reporting. They often have a pervasive impact on the effectiveness of controls at the process, transaction or application level. At the entity level, management must address the various attributes COSO provides for each component. The illustration on the next page 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"> <li>■ Entity-wide objectives</li> <li>■ Activity-level objectives</li> <li>■ Risk identification and assessment</li> <li>■ Managing change</li> </ul>	<ul style="list-style-type: none"> <li>■ Are there policies, procedures and effective processes for hiring, compensating, promoting, training and terminating employees?</li> </ul>
Control Environment	<ul style="list-style-type: none"> <li>■ Integrity and ethical values</li> <li>■ Commitment to competence</li> <li>■ Board of directors or audit committee</li> <li>■ Management's philosophy and operating style</li> <li>■ Organizational structure</li> <li>■ Assignment of authority and responsibility</li> <li>■ Human resource policies and practices</li> </ul>	<ul style="list-style-type: none"> <li>■ Are employees made aware of their roles, responsibilities, authorities and performance expectations?</li> <li>■ Are everyone's control-related responsibilities clearly articulated?</li> <li>■ Are employees accountable for results and are performance expectations reinforced with appropriate performance measures?</li> </ul>
Information and Communication	<ul style="list-style-type: none"> <li>■ External and internal information is identified, captured, processed and reported</li> <li>■ Effective communication down, across, up the organization</li> </ul>	<ul style="list-style-type: none"> <li>■ Are employee retention and promotion criteria clearly defined, and is the performance evaluation process effective?</li> </ul>
Control Activities	<ul style="list-style-type: none"> <li>■ Policies, procedures and actions to address risks to achievement of stated objectives</li> </ul>	<ul style="list-style-type: none"> <li>■ Does management take appropriate remedial action in response to departures from approved policies and procedures?</li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>■ Ongoing monitoring</li> <li>■ Separate evaluations</li> <li>■ Reporting deficiencies</li> </ul>	<ul style="list-style-type: none"> <li>■ Is the established code of conduct reinforced and disciplinary action taken when warranted?</li> <li>■ Are the background and experience of prospective employees checked and references obtained?</li> </ul>

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 as to how the COSO framework is applied at the entity level:

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

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

- COSO recommends the following:
  - Responses should be documented for each point of focus rather than for the more granular criteria. Responses should be based on management’s conclusion that the stated policies, processes, competent people, reports, methodologies and systems actually exist and are effectively functioning.
  - A response should generally not be a “yes” or a “no” answer, but rather should address specifically what the entity does to address the point of focus.
- Management should conclude as to the effectiveness of internal controls with respect to each attribute supporting a given component of internal control. The responses providing information with respect to the points of focus, as described 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 (see Question 107).
- A response of “ineffective” or “requires improvement” for a given attribute should lead management to evaluate whether improvements are needed in internal controls and to take appropriate action to close any gaps. If management believes there is an absence of one or more key controls that, if not compensated for in other areas, increases the likelihood that there are significant control risks, 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 56 and 57), 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

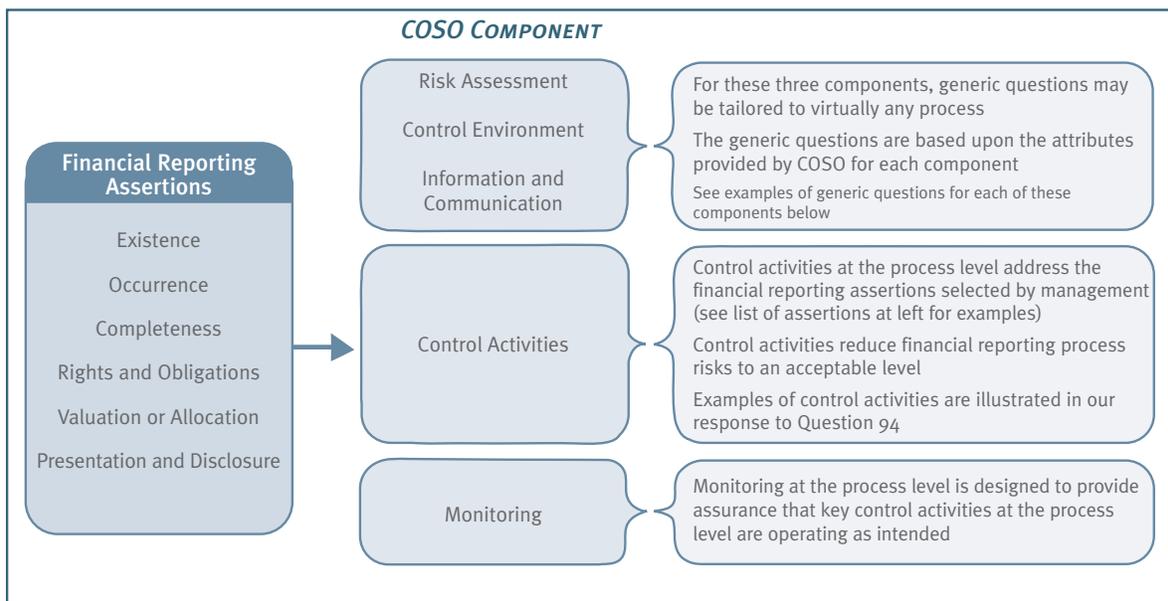
control environment). The reporting entity establishes the organizational structure (another separate attribute), provides overall HR policies (part of the “human resource policies and practices” attribute), etc.

- 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.

#### 44. 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 shown in the following illustration:



From a practical standpoint, when performing a review of internal control over financial reporting, most of the attention at the process level focuses on control activities and the monitoring of those activities. Once the assertions related to reliability of financial reporting are generally understood and documented (see Questions 74 and 75 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 74 and 75 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 94.

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?

### **45. Must the Section 404 compliance team address each of the five COSO elements in each process?**

At the process level, most of the controls will consist of control activities and monitoring. The remaining three COSO components – control environment, risk assessment and information/communication – can be addressed by tailoring relevant questions listed in Question 44 to appropriate processes. There are a variety of ways these three components can be documented at the process level. Some auditors insist that all five components be addressed for each process. Others point out that the risk assessment component is generally applied at the entity and business-unit levels. Elements of the control environment and information/communication clearly apply to the processes because process owners set the tone for their subordinates, must have information with which to manage the process and communicate with others on many important

topics. Monitoring at the process level often includes ongoing supervisory activities by process owners, including review and follow up on exceptions and issues identified through reports, reconciliations, comparisons, confirmations and other sources of process performance information (see Question 44 for other examples). Monitoring also includes separate evaluations by internal auditors and others.

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

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

There are potentially strong sources of value extending beyond mere compliance with Section 404. Sections 302 and 404 of SOA provide the “launching pad” to improve processes and the control structure and enhance entity-level monitoring of the financial reporting process. Because SOA forces public companies to assess weaknesses in their business processes, including their controls over processing information, the line between reliable financial reporting and operational effectiveness and efficiency can be a blurry one. Financial reporting processes for many companies are often dependent on people and detective controls and are sometimes inadequately defined. This dependency provides a significant opportunity to “build in” (versus “inspect in”) quality, optimize costs and compress time within the organization’s processes while simultaneously reducing its financial reporting risks. Compressing time in the close process can be especially important as SEC filing deadlines accelerate (see Question 234). In today’s environment, it is impossible to improve cost, quality and time-process performance without also automating controls and improving the balance of preventive and detective controls.



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

Management 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. If management chooses to do so, however, that action is a business decision and not an SOA-driven initiative. (See Question 22.)

**47. 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.

#### **48. Will the COSO framework on Enterprise Risk Management affect the Section 404 assessment?**

No. COSO is releasing the Enterprise Risk Management Conceptual Framework and the accompanying Application Techniques in September 2004. This 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**

#### **49. How does management get started?**

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

***Organize the project*** – In organizing the project, management should identify the appropriate project sponsor. The sponsor should be a senior executive who can assume responsibility for providing overall direction to the project team and for communicating the project to the organization with credibility. One of the certifying officers should fulfill this role, i.e., the CEO or CFO. In addition to the sponsor, management should identify the project team members, their roles and responsibilities, the resources required and the source and funding of those resources, both internal and external. A team leader, such as the chief accounting officer or corporate controller, should also be appointed. Reference is also made to Questions 190 and 192 for discussions of the role of the disclosure committee and the role of the Section 404 compliance project steering committee.

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

***Agree on project approach and reporting requirements*** – Obtaining agreement up front 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 74 and 75 for examples of common language of risks or assertions. See Questions 69 and 70 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 53.)
- 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 60 and 61.)
- Define the control units by which to break down the organization for purposes of evaluating entity-level and process-level controls. (See Questions 56 and 57.)
- Identify the tools and technology that are needed to support management's controls evaluation process. The methods, tools and technology should be robust enough to ensure consistency across the organization. When evaluating the technology solution, management must consider the collaboration required in the approach, the level of coordination expected and the extent of accessibility of information desired by different individuals. (See Question 63.)
- Agree on control framework by which management will evaluate effectiveness. (See Question 42.)
- Validate approach and requirements with the independent public accountant to ensure everyone is in agreement. (See Question 206.)
- Define the internal communication plan for management to execute during the project. (See Question 59.)

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

## **50. 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 PMO (see Question 49) 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 191, may chair this committee. The project leader reports to this committee.

### **51. 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 52, 53, 54, 57 and 58 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.

### **52. 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.

### **53. 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)
- Accounting and reporting complexities associated with an account
- 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 (see Questions 55 and 58)
- 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
- Changes in account characteristics since the prior year
- 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
- The extent of reliance on third parties, including specialists and service organizations
- 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, exposure to losses, likelihood of significant contingent liabilities, 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.

#### **54. 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 53), 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. Many auditors have articulated the point of view that there is also a presumption that ALL line items and captions and ALL footnote disclosures included in published financial statements are significant. Furthermore, when decomposing financial statement line items and captions (as well as disclosures) into specific account balances and components, many auditors are also requiring the use of a quantitative materiality measure (see Question 55), i.e., all account balances and components exceeding the defined quantitative threshold (sometimes referred to as “planning materiality”) must be included within scope. Decomposition must also consider accounts or components that are affected by different transaction streams subject to different risks and controls.

Prioritization of financial reporting elements 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. Based on the SEC’s guidance (see Question 55), many auditors have taken the approach that materiality is first applied quantitatively to identify the significant financial reporting elements, and then applied qualitatively to identify the elements below the quantitative threshold that should also be included in scope. Therefore, applied in this manner, qualitative considerations become additive.

The results of the scoping exercise should be validated with the independent public accountant. Practice has indicated that “scoping dialogues” with the auditors almost always result in the company scoping in additional accounts that were previously scoped out. This iterative “give and take” is understandable given the judgmental nature of scope setting and caption decomposition to specific accounts.

#### **55. How does a company assess materiality when prioritizing financial reporting elements?**

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

The PCAOB provided guidance on evaluating materiality in Auditing Standard No. 2. The auditor applies the concept of materiality to internal control over financial reporting in much the same manner as the application to financial reporting. Materiality is applied at both the financial-statement level and at the individual account-balance level. At the financial-statement level, materiality is applied to differentiate significant deficiencies (or a combination of significant deficiencies) from material weaknesses. Materiality is applied at the account-balance level in determining whether an internal control deficiency is a significant deficiency. The standard points to both quantitative and qualitative considerations when evaluating materiality.

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

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

No. The staff is aware that certain registrants, over time, have developed quantitative thresholds as "rules of thumb" to assist in the preparation of their financial statements, and that auditors also have used these thresholds in their evaluation of whether items might be considered material to users of a registrant's financial statements. One rule of thumb in particular suggests that the misstatement or omission of an item that falls under a 5% threshold is not material in the absence of particularly egregious circumstances, such as self-dealing or misappropriation by senior management. The staff reminds registrants and the auditors of their financial statements that exclusive reliance on this or any percentage or numerical threshold has no basis in the accounting literature or the law.

The use of a percentage as a numerical threshold, such as 5%, may provide the basis for a preliminary assumption that – without considering all relevant circumstances – a deviation of less than the specified percentage with respect to a particular item on the registrant's financial statements is unlikely to be material. The staff has no objection to such a "rule of thumb" as an initial step in assessing materiality. But quantifying, in percentage terms, the magnitude of a misstatement is only the beginning of an analysis of materiality; it cannot appropriately be used as a substitute for a full analysis of all relevant considerations. Materiality concerns the significance of an item to users of a registrant's financial statements. A matter is "material" if there is a substantial likelihood that a reasonable person would consider it important.

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

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

The SEC staff makes it clear that the above list is not intended as an exhaustive one of the circumstances that may affect the materiality of a quantitatively small misstatement. For example, the demonstrated volatility of the price of an issuer's securities in response to certain types of disclosures may provide guidance as to

whether investors regard quantitatively small misstatements as material. The SEC staff states that when “management or the independent auditor expects (based, for example, on a pattern of market performance) that a known misstatement may result in a significant positive or negative market reaction, that expected reaction should be taken into account when considering whether a misstatement is material.”

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

### **56. What are “control units” and why are they important?**

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

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

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

The choice of control units is an important decision and requires careful thought and judgment in considering how management structures, runs and controls the organization. It requires an understanding of the extent of common processes and IT platforms and the degree of centralization versus decentralization. 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.

### **57. 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. The two primary criteria emphasized by the PCAOB in Auditing Standard No. 2 are:

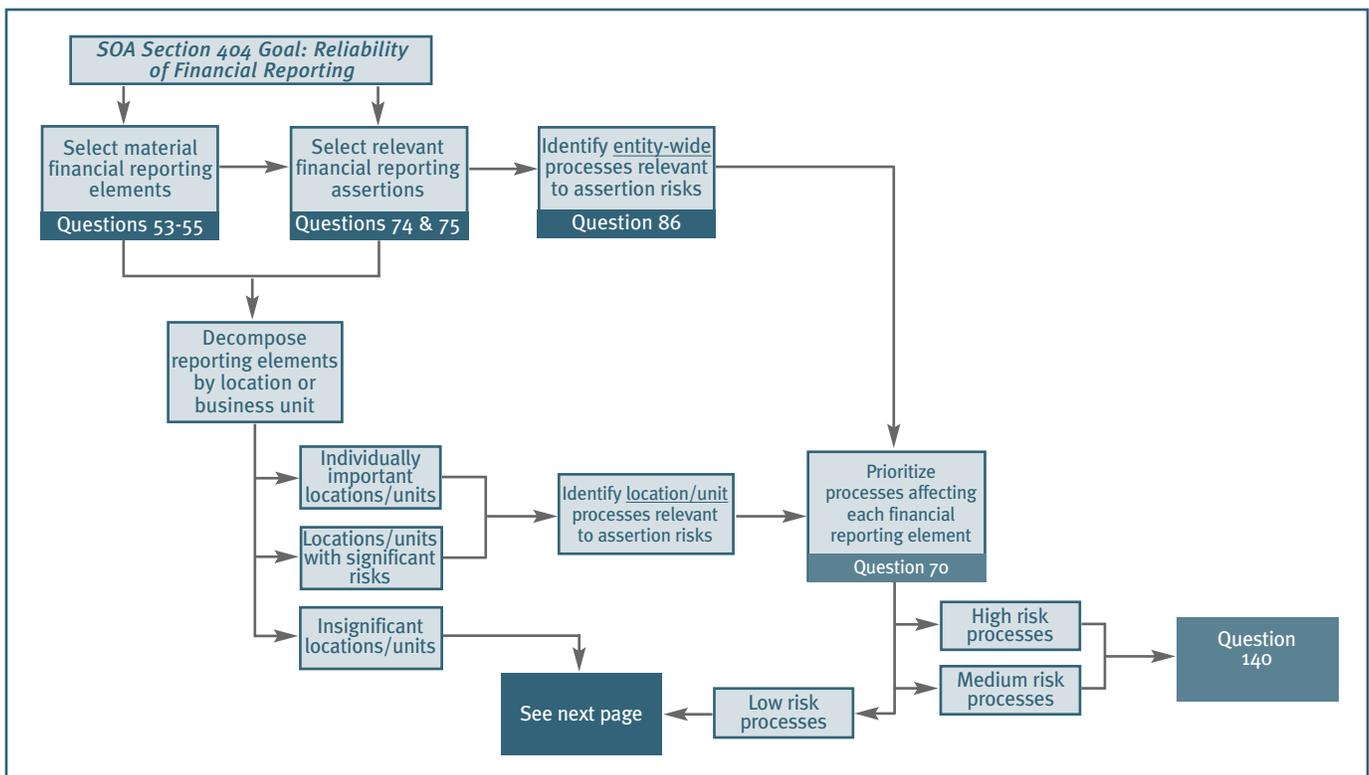
- Individually important locations and units. These business units or locations are selected based on their relative significance of assets and contributed sales and profits. For many companies, the individually important business units or locations often represent a relatively small number of units or locations that

encompass a large portion of the consolidated entity’s operations and financial position. See Question 58 for discussion of what constitutes a “large portion.”

- Locations and units with 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 decision-making authority of a given unit or location can result in creation of obligations on behalf of the reporting entity or encumber significant assets of the reporting entity.
  - There is a potential for surprise at a unit that may be immaterial based on traditional financial measures, but through its actions or inaction can have a huge impact on the organization, such as involvement in a catastrophic environmental disaster.
  - There is exposure to material unrecognized obligations or contingent liabilities at a given location or unit (e.g., loss reserves).
  - Due to the environment in the country in which it does business, a particular unit or location is exposed to fraud, sensitive payments or other factors impacting the reporting company’s reputation.
  - A unit that previously has reported significant control deficiencies may continue to present key risks.
  - An otherwise insignificant location or unit includes a material account balance (e.g., inventory or fixed assets) that warrants attention because of inadequate coverage of the account balance at other locations on a consolidated basis.

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

The above criteria carry substantial weight in the process of selecting control units and locations. Following is a schematic illustrating the thought process:

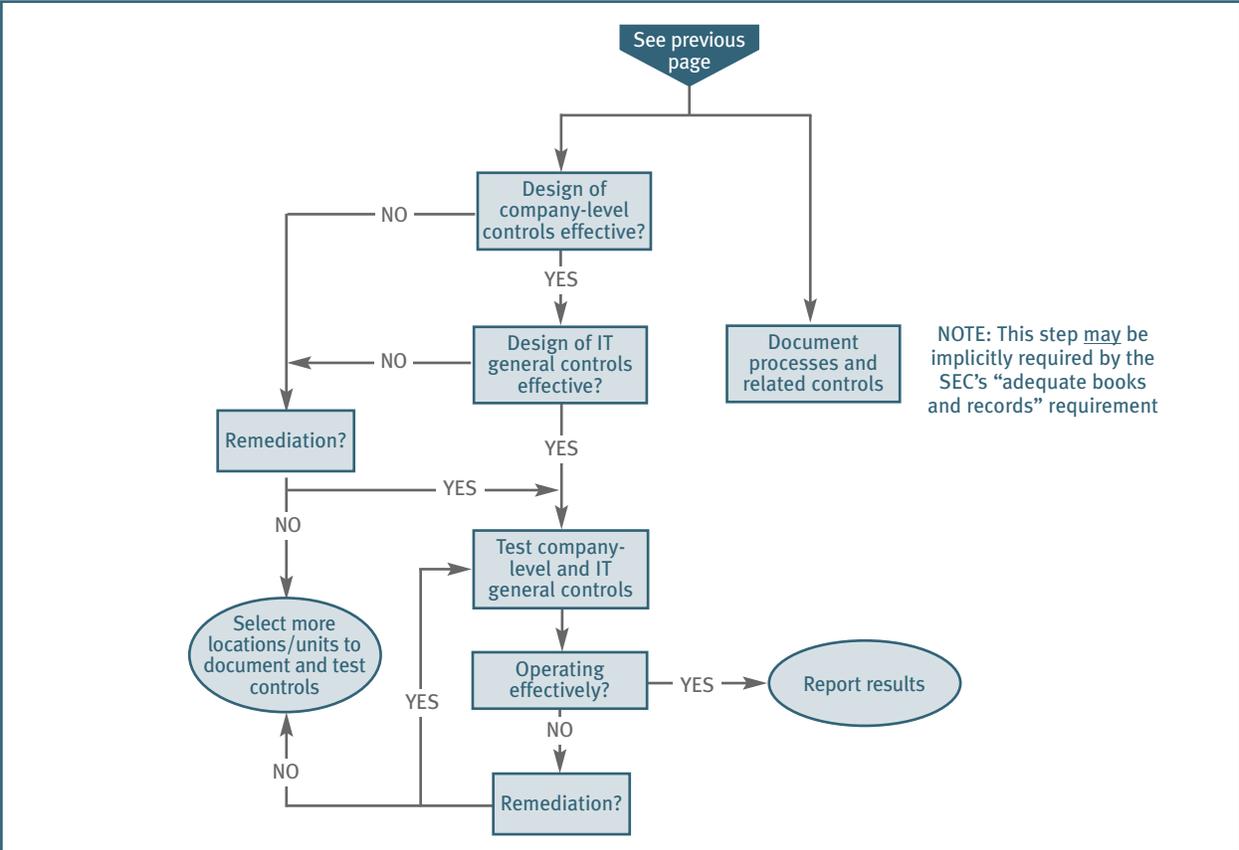


In many cases, application of the above criteria of “individually important locations and units” and “locations and units with significant risks” should result in selecting enough locations and units that will provide sufficient coverage of the consolidated entity’s operations and financial position for purposes of Section 404 compliance. There will, however, be instances when more locations and units must be selected. Other criteria may be used to select additional locations and units that are not individually important or do not present significant risks. The following criteria may be used to evaluate these remaining locations and units for purposes of aggregating them to determine whether additional locations and units should be considered for purposes of further increasing multilocation coverage:

- 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 and are subject to common processes and controls
- The extent to which the accounting records and systems are centralized for selected units and locations
- 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 at multiple locations and units and whether what is reported is consistent with economic reality

After applying the criteria above, the company must aggregate insignificant, lower-risk locations and units to determine whether they are significant in the aggregate. If they are significant, management should evaluate the company-level controls and IT general controls related to these locations and units. If these entity-level controls are effective, no further work is needed at these individually insignificant and lower-risk locations and units. If the entity-level controls are not effective, then additional locations and units must be selected for purposes of documenting and testing controls.

As a continuation of the visual on the previous page, the schematic below illustrates:



Reading between the lines, the message is clear. Companies with numerous locations and units must have effectively operating company-level controls. If they don't, the company-level controls must be improved. If there is an absence of company-level controls, the company may be required to expand the evaluation of controls at the location and business unit level because management is unable to rely on the operation of monitoring, oversight and other entity-level controls. In addition, most auditors begin with a presumption that there will be a minimum level of testing at the process level. Ineffective company-level controls will result in an increase in scope in terms of the nature, timing and extent of testing at the process level, resulting in increased audit fees.

Once the criteria are determined, management should select the most significant control units and locations for purposes of assessing controls. As illustrated above, the process involves judgment. Once the locations and units are selected, management should document the supporting rationale and obtain concurrence of the independent public accountant. For large and complex companies with dispersed assets and operations, management should expect the auditors to offer a point of view that will likely result in further refinements in the company's articulation of multilocation coverage.

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

#### **58. How does management define “a large portion” for purposes of determining multilocation coverage?**

How many locations and units must management perform testing on to achieve appropriate coverage? PCAOB Auditing Standard No. 2 states that testing coverage must comprise “a large portion” of operations and financial position using the decision tree provided in Appendix B of the PCAOB's standard. The question often arises as to what “a large portion” means in practice. Many have different points of view that often are influenced by a company's specific facts and circumstances. The PCAOB staff has indicated that the definition of “a large portion,” for purposes of defining testing coverage, is intended to be principles-based and is left to auditor judgment. The PCAOB staff has also pointed out that auditors are defining “a large portion” differently, citing as examples 60 percent and 75 percent of operations (revenues, operating profit and net income) and financial position (total assets and stockholders' equity).

When addressing this question, the best course of action is to work with your independent accountant to define the appropriate threshold. Note that the coverage must include individually important locations and business units, where management should assess controls related to relevant assertions for all significant accounts and disclosures, as well as locations and units not individually important but with specific risks that make them important. If, after considering locations and units that are individually important or that have significant risks, the coverage falls short of a 60 percent to 75 percent threshold, more locations and units should be selected with the emphasis placed on risk.

It is also possible that a company may consist of a number of significant locations and units that, in the aggregate, comprise more than 75 percent of operations and financial position. In other words, the 60 percent and 75 percent thresholds cited by the PCAOB are “de minimus” thresholds, meaning facts and circumstances could drive the multilocation coverage to a higher level. For example, the external auditor may apply an arbitrary threshold (e.g., five percent or 10 percent of consolidated operations or financial position, as defined) to identify “significant” locations and units. Application of this threshold can result in overall coverage exceeding the general guidelines.

While the PCAOB has not provided further guidance on this question as of the date this publication went to press, the Board states in Auditing Standard No. 2, “The evaluation of whether controls cover a large portion of the company’s operations or financial position have been tested should be made at the overall level, not at the individual account level.” The PCAOB staff has also advised that auditors may not rely solely on company-level controls without also testing controls over all relevant assertions related to significant accounts and disclosures. Ultimately, the multi-location coverage is a function of three things – 1) the company’s facts and circumstances, 2) management’s criteria and judgment, and 3) the auditor’s policies and judgment. For example, the auditor’s policies related to the minimum size of a significant location or unit that must be included for purposes of testing overall coverage can greatly impact the coverage ultimately obtained.

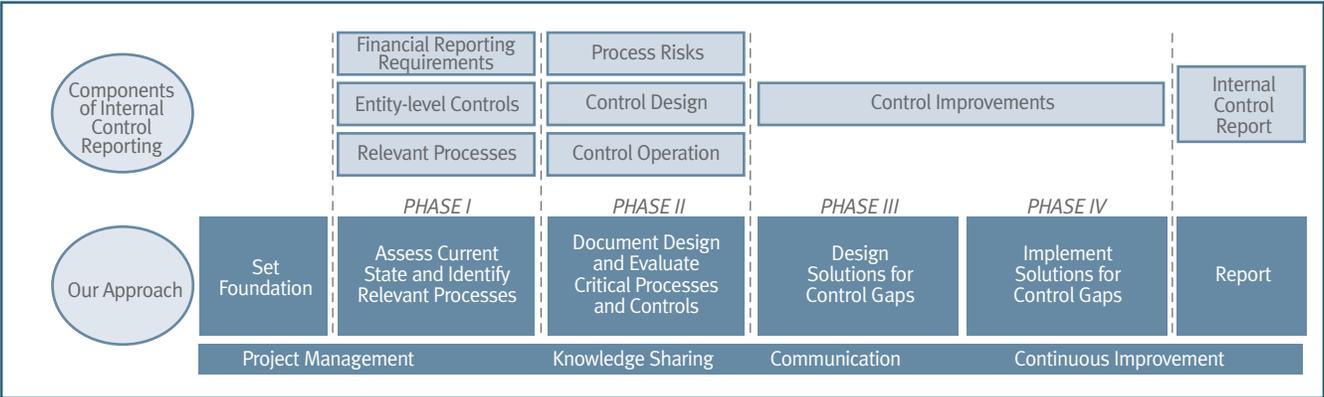
When management is allowed to exclude certain entities from the company’s assessment by the SEC, disclosure in the form of an explanatory paragraph is required in the internal control report. See Question 159.

**59. 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, particularly with unit managers and process owners. The sponsor and team leader should articulate the purpose and importance of the project, the sponsorship of the project, the project timing and approach, and everyone who is primarily responsible for critical internal controls, including what is expected of them now, what is expected of them during the project and what is expected after completion of the project.

**60. What steps should be included in the project plan?**

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



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

**Phase I (Assess current state and identify relevant processes)** – Identifies priority financial reporting elements, assesses current state of critical processes and points of origin from public report requirements, inventories available internal controls documentation, documents the financial close process, and develops a critical process scorecard (see Question 61 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 and remediation.

**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 and remediate internal controls, including the related policies, processes, controls, reports and systems.

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

**Report** – Communicates the results 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. See Questions 178 through 189.

#### **61. 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.

#### **62. 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 walkthrough of the process using the relevant documents is an effective method of ascertaining the procedures and controls as they really function. (See Questions 119 through 154 for guidance with respect to validating operating effectiveness of internal controls.)

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

Technology is a key enabler for SOA compliance. There is a wide range of software tools available in the marketplace. These tools can be segmented into either “point solutions” (which are applications designed specifically for SOA compliance) or “platform solutions” (which are software infrastructure designed for another purpose such as business process automation, document management, financial management, or broader compliance, and is adapted for SOA compliance). Point solutions typically support deeper analysis and reporting requirements for SOA compliance, while platform solutions provide extended capabilities and could serve as infrastructure for broader compliance, governance, and risk management activities over time. The “total” solution for broader compliance, governance and risk management does not currently exist, and will likely emerge over time through integration of several applications and platforms and as companies evolve toward enterprise risk management.

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

Tool functionality required for short-term compliance includes, but is not limited to: methodology framework; project management; workflow review and approval (including e-mail integration); documentation management (including template libraries, issue tracking and corrective action plans); standard and ad hoc reporting; integration or export to third-party reporting tools; and the ability to import consulting partner content and existing documentation. Functionality required for long-term compliance includes, but is not limited to: direct linkage to ERP controls; dynamic and graphical process modeling; control monitoring and enforcement through alerts and early warning; enterprise content management (including versioning and records archiving); and integration of business intelligence and analytical tools.

Many companies are using project management tools and spreadsheets to document the required analyses, and are experiencing problems with this “low tech” approach. Others have been using certain point solutions, which are showing signs of stress or are otherwise being divested. Those companies that have opted for platform solutions soon realize that many of these solutions do not perform as advertised as they fail to deliver required functionality to support deep analysis and reporting. There are different versions of SOA repository tools available. Some of these proprietary tools are sold only as part of a consulting arrangement, some are populated with libraries of controls content and others are mere shells. The tools and technologies supporting SOA compliance are in constant state of flux as providers upgrade them to meet ever-changing buyer needs.

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

Estimates are hard to come by without some analysis. Ultimately, the effort and cost are a function of many factors, including the number of locations and units 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) determining the sufficiency of useful policies and procedures, the availability of quality process and control documentation and the extent of IT controls documentation; and (c) determining the nature of the control gaps that exist and must be corrected. Once resource requirements are estimated, management must decide the nature and extent to which internal resources are available. The complexity of the organization and its underlying processes must also be considered.

For these reasons and because there is no “one size fits all,” it is difficult to generalize estimates. At the time this book went to print, few companies had completed their Section 404 assessment and attestation processes. However, some studies have been conducted. For example, Financial Executives International found that companies with revenues of \$1 billion to \$5 billion are estimated to be expending an average of approximately 14,000 hours to comply with Section 404.

One can speculate about the percentage breakdown of planning, documentation and design evaluation, testing, and so forth. For example, planning is not likely to exceed five to 10 percent of total costs. But estimating the split between documentation and design evaluation and testing operating effectiveness is another matter. For example:

- The number of processes, the number of control units, the number of systems and the number of locations and units impact controls documentation and design evaluation.
- The total testing effort will be driven by such factors as the desired confidence level, the desired level of precision, the resulting sample sizes, the number of controls tested and the number of exceptions encountered during the testing process.
- As noted above, the extent of remediation and the resulting need to retest are a significant unknown for many companies.
- The impact of reliance on outside service organizations.
- The extent to which the company has a repeating, defined and managed internal control structure is an important factor influencing Section 404 compliance costs. The more mature a company’s processes, the less the expected costs to comply with Section 404.

The message here is this: The Section 404 project is a phased project in which the results of each phase provide clarity as to the magnitude of the effort required for the next phase. To illustrate, referring to the approach in Question 60, we recommend that the project team should first complete both Set Foundation and Phase I before committing to an estimate. Further, many companies are using pilots to develop realistic estimation guidelines as they progress through Phase II, as introduced in Question 60.

In summary, as of the time this book went to print, it is still early in the compliance process and there are many variables making realistic rules of thumb difficult to find, much less trust. The total effort ultimately is a function of many things, as noted above. The total cost is also not necessarily the best indicator of the extent of the burden as viewed by management, since the size, structure and complexity of the company will often dictate how costly these requirements will be. Accordingly, many companies that have their compliance projects substantially underway remain uncertain as to what the total costs of first-year compliance ultimately will be, including the internal costs.

#### **65. Will companies need to add internal resources to comply with Sections 404 and 302?**

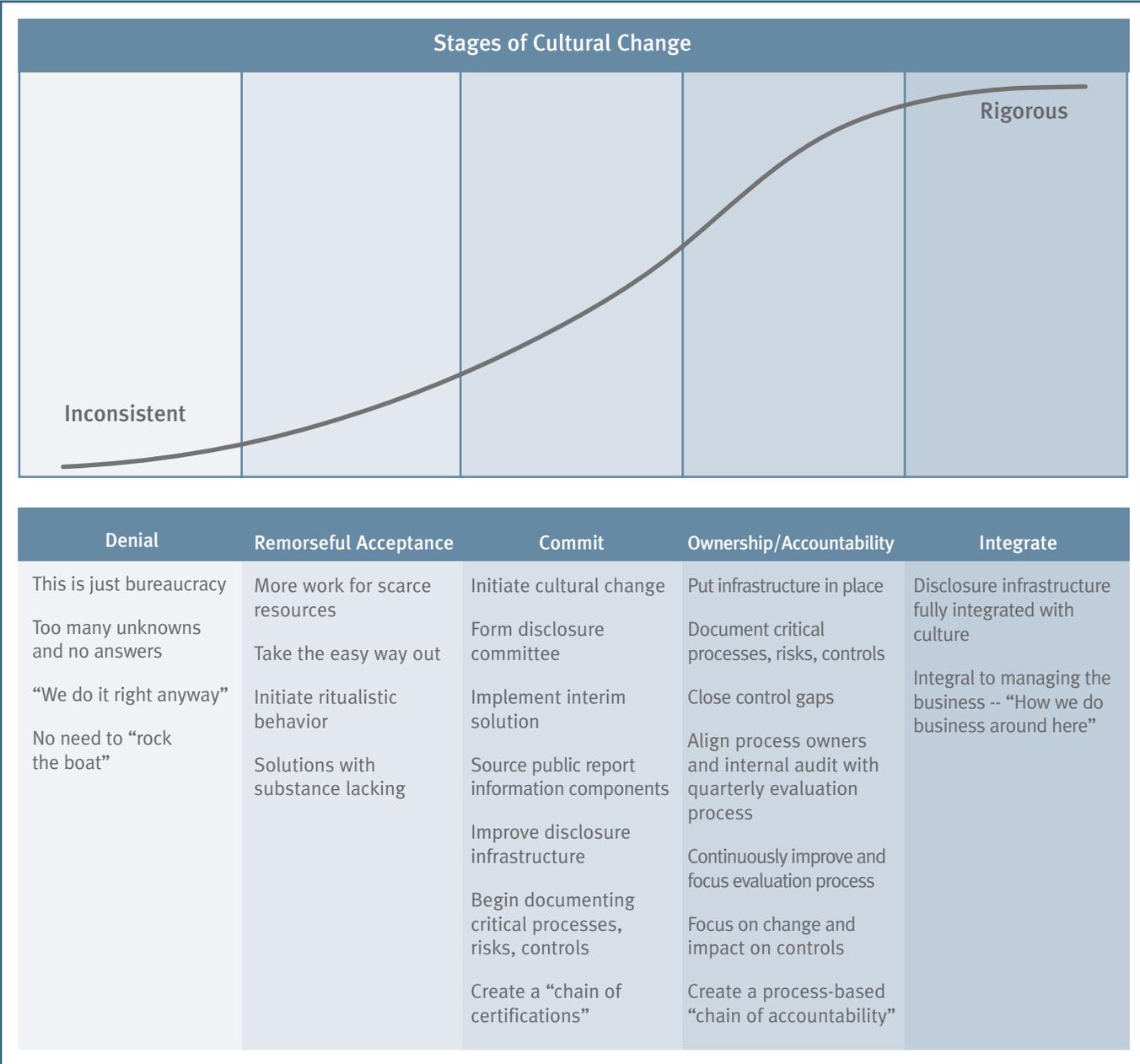
Not necessarily. With respect to the initial annual assessment, external resources may be used to supplement gaps that internal resources are unable to address. The key is to deploy qualified resources with the requisite knowledge of processes, risks and controls as well as appropriate knowledge of the 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, internal audit and risk control specialists, to execute it.

#### **66. 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 U.S. “accelerated filer” 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 formed a disclosure committee. Some companies created a chain of certifications (see Question 186 for explanation). Others began documenting their processes, such as the financial close process.

As the realities of the Section 404 compliance process became clearer, companies moved further 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.

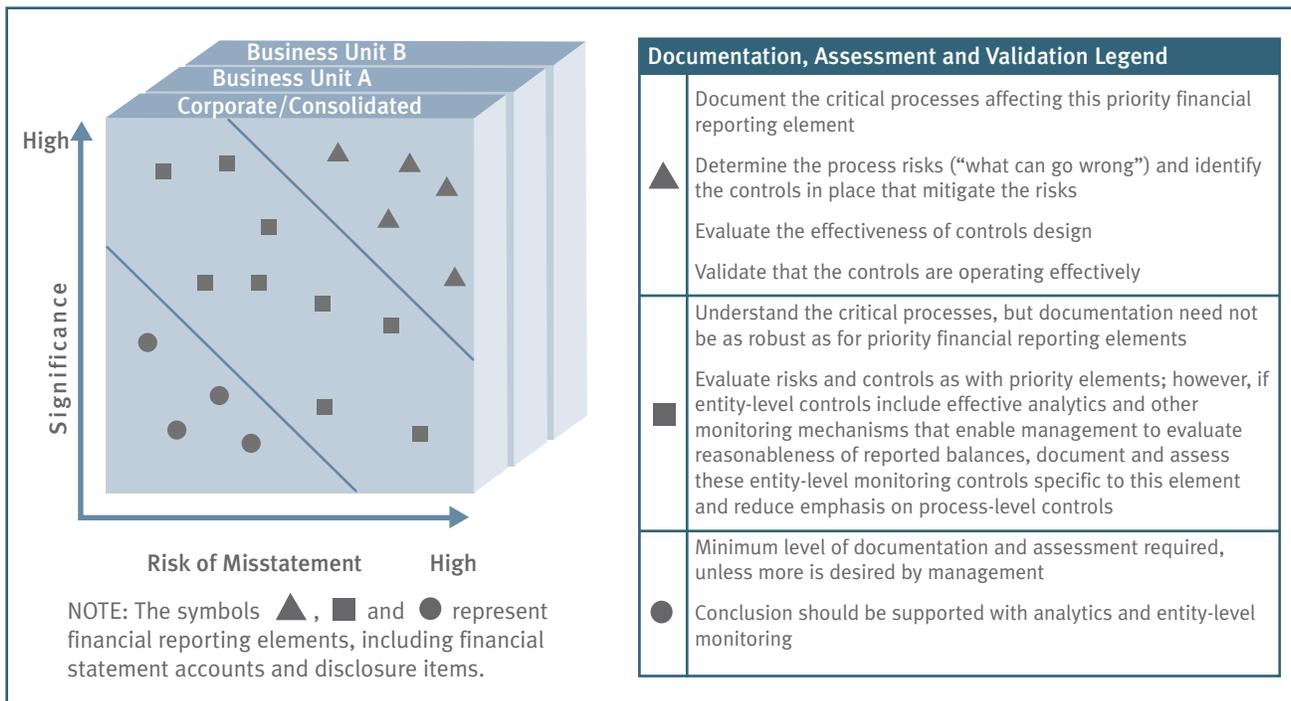
A cultural assessment survey could be useful in evaluating what stage a company is at, as well as checking its preparedness for compliance with Section 404. This assessment can be particularly useful to foreign filers and U.S. non-accelerated filers who may find their personnel in the same stage of readiness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

## Identifying Reporting Requirements and Relevant Processes

### 67. 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 line item or caption, account balance, 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.

When evaluating specific accounts, it is always appropriate to aggregate accounts affected by similar transaction flows. These accounts often have similar risk characteristics and similar controls.

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, reserve accounting, etc.
- 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 testing at the process level 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.

In summary, keep in mind four 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.
- Break out separate accounts that are affected by separate transaction flows.
- Last, but certainly not least, understand the independent public accountant’s expectations and requirements, particularly with respect to the definition and application of materiality during the scope-setting process. A scoping exercise is only as good as the independent accountant’s concurrence with the result. We have seen instances where the external auditor insisted on scoping back in financial reporting elements that management decided to scope out after evaluating the relative risks. Due to the judgmental nature of the process, this iterative dialogue with the auditor should be expected.

## 68. 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 Questions 53, 54 and 55.)

## 69. 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, omissions or fraud 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, authorize, record, process and report the transactions affecting key financial reporting elements on a daily basis. A less formal transaction flow could simply be the calculation of a month-end accrual or deferral, or the estimation of a reserve for doubtful accounts in conjunction with closing the books. The controls over these transaction types often vary in terms of formality – the less formal the processes generating the transactions, the less formal the controls.

Each transaction type is discussed further below.

- ***Routine transactions*** – Most of the relevant processes affecting financial reporting will be those that initiate, authorize, record, process and report routine transactions. These transactions represent frequently recurring data recorded in the books and records, or nonfinancial data used to manage the business. They are the recurring financial activities reflected in the accounting records in the normal course of business. For example, sales and accounts receivable, procurement and accounts payable, payroll, cash receipts and disbursements are routine transactions in the ordinary course of business. Standard journal entries booked every close, such as amortization of long-lived 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. They occur only periodically involving data that is generally not part of the routine flow of transactions. Examples include calculations of income taxes, accrued interest on investments and loans, depreciation expense, accrued liabilities for goods and services received but not invoiced, prepaid expenses, adjustments for foreign currency, and liabilities for advance payments for services not yet delivered.

Transactions arising from accounting estimates often involve management judgments or assumptions in formulating account balances in the absence of a precise means of measurement. They result in adjustments for loss contingencies that reduce recorded assets or record additional liabilities for the estimated effects of future events that are likely to occur and are reasonably estimable. Examples include estimating the allowance for bad debts or loan losses, allowance for excess and obsolete inventory, and warranty reserves. Estimation transactions often arise due to the uncertainty inherent in measuring assets and liabilities in the financial reporting process, i.e., there is uncertainty in measuring certain amounts or in valuing certain accounts. If the outcome of future events is uncertain (i.e., not likely to

occur) or relevant data concerning events that have already occurred cannot be accumulated on a timely and cost-effective basis (i.e., not reasonably estimable), such matters should be disclosed and not be recorded. An example is pending litigation.

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

With respect to unusual or 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.

#### **70. 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 deficiency 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.

One thing to keep in mind is that coverage of all core business processes may not satisfy the external auditors, whose definition and application of materiality may lead them to conclude that there are additional financial statement accounts or components warranting analysis. These additional accounts or components may be derived from separate classes of transactions subject to different risks and controls or exceeding the auditor's planning materiality, and may even be peripheral to what management regards as the core processes of the business. Nevertheless, they may be material to financial reporting. For example, revenue streams having different characteristics (e.g., product sales versus service revenues, sales on account versus sales-type leases or cash sales, sales through retail outlets versus direct sales from distribution centers, etc.) must be assessed separately.

## 71. What is a “reasonable” number of business processes for purposes of Section 404 compliance?

We are asked this question a lot. While this is a straightforward question, there isn't a straightforward response because rules of thumb are hard to come by. The answer depends on how the Section 404 compliance team chooses to define a process as well as the nature and complexity of the business. Processes can be defined as broadly as the major transaction flows, such as revenue, purchasing, payroll, conversion, treasury and financial reporting. They can be defined at a more granular level, e.g., “purchasing” can consist of procurement, receiving, accounts payable, etc. It is within these processes where 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. What is more important here is the objective, which is to provide a sufficient understanding of the flow of transactions impacting the key elements of the financial statements. That understanding is needed to support an effective risk assessment that makes the approach risk-based.

As discussed in Question 69, the processes of any business generate different types of transactions, which can be classified as routine transactions, unusual or non-routine transactions, and transactions from accounting estimates. A more formal transaction flow consists of the records, documents and basic processing procedures used to initiate, authorize, record, process and report the transactions affecting key financial reporting elements on a daily basis. A less formal transaction flow could simply be the calculation of a month-end accrual or deferral, or the estimation of a reserve for doubtful accounts in conjunction with closing the books. The controls over these transaction types often vary in terms of formality – the less formal the processes generating the transactions, the less formal the controls. Controls must be evaluated for all types of transactions and processes, if they affect the significant elements of the financial statements. The process breakdown to decompose the business is intended to enable the compliance team to identify the relevant controls. For these and other reasons, it is difficult to generalize the number of processes.

## 72. 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. See Question 183.

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

### 73. 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.

#### 74. 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:

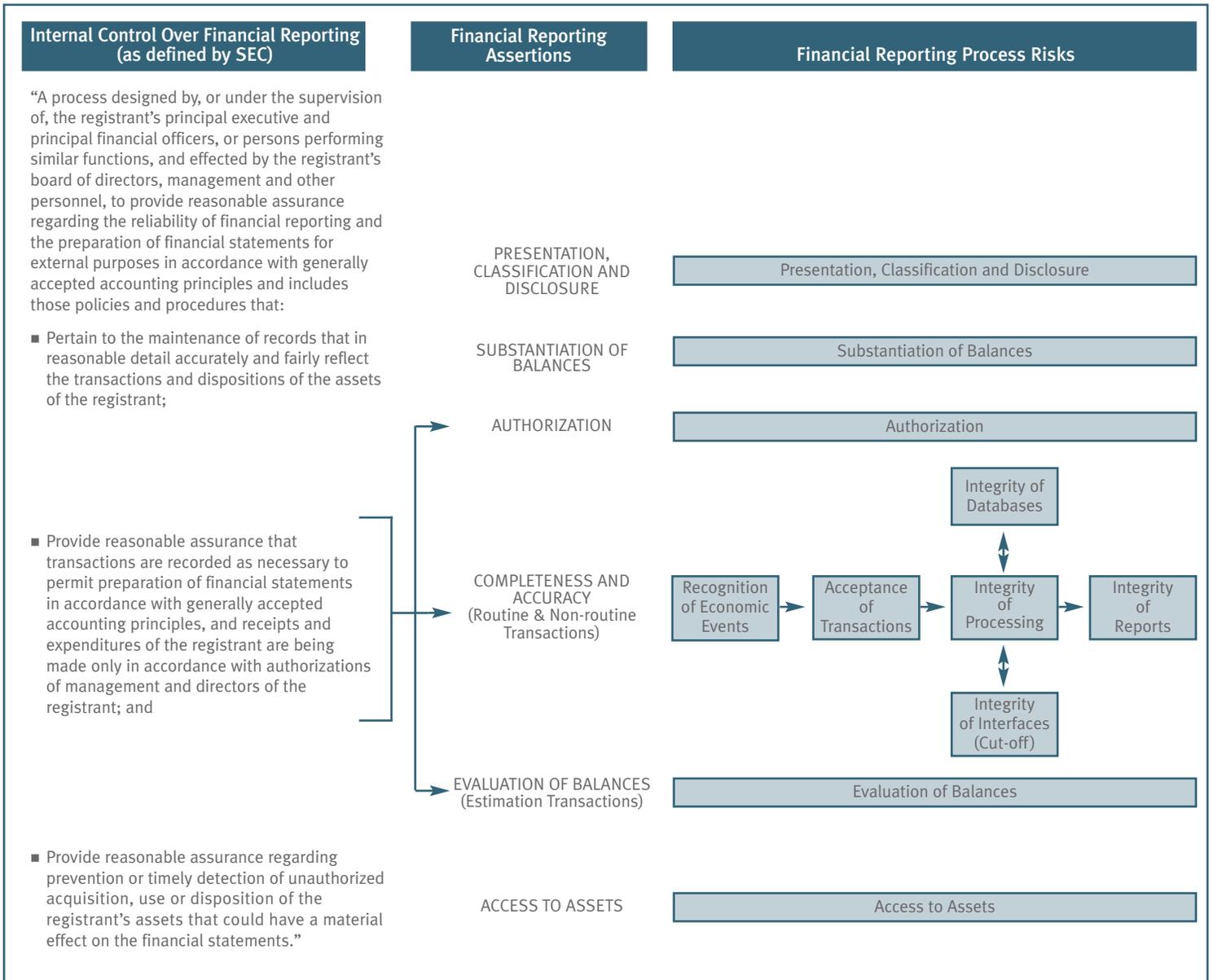
- **Existence** – Assets, liabilities and ownership interests exist as of a point in time.
- **Occurrence** – Recorded transactions represent economic events that actually occurred during a stated period of time.
- **Completeness** – All transactions and other events and circumstances that occurred during 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.

These assertions were reinforced by the PCAOB in Auditing Standard No. 2.

When analyzing the critical routine processes (see Questions 69 and 70), 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 PCAOB staff has stated that it is not an absolute requirement to use the above assertions. The staff also noted that management must use assertions that have a “reasonable bearing as to whether accounts are fairly stated.” Therefore, the above assertions (or alternative assertions – see Question 75, for example) are used to identify points within the transaction process, estimation methodology or disclosure generation process where things can go wrong. The Section 404 compliance team should determine the sources of likely potential misstatements in each significant account. These sources of risk provide the focal point for evaluating controls to provide reasonable assurance that the assertions are being met.

#### 75. 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, authorization, recording, processing and reporting of transactions. For example, “processing” is reflected in integrity of databases, processing and interfaces. Interfaces are particularly important as they represent the “hand-offs” between units and processes. Intercompany transactions, related party transactions, transfer pricing issues, and transfers between processes and functions must be understood and controlled, because they create processing issues requiring careful attention.

For examples of financial reporting assertions from the COSO framework, see Question 74. Some companies selected the above assertions or similar assertions prior to the release of Auditing Standard No. 2. While the PCAOB’s standard reinforced the assertions defined in Question 74, the PCAOB staff has indicated that these assertions are not absolute requirements. As long as the assertions used are defined in a manner so they are equivalent to the COSO assertions, they are acceptable for use now and in the future.

Thus the message is one of flexibility. That said, for companies just getting started, we recommend the use of the COSO assertions provided in Question 74.

**76. How are control objectives defined?**

Our responses to Questions 74 and 75 illustrate the use of financial reporting objectives or assertions for purposes of focusing an evaluation of internal control over financial reporting. These assertions may be defined more specifically as objectives in the context of a process or alternatively they may be defined more granularly in the form of specific risk statements (i.e., risks to the achievement of the assertions). In practice, the more specific objectives related to an assertion and the granular risks related to an assertion are often “mirror images” of each other. Therefore, we see some variability in practice with some companies evaluating controls in the context of achieving objectives and others in the context of mitigating risks. Either approach gets the job done, provided they are appropriately linked to the financial reporting assertions.

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

---

## **Integrating Fraud Considerations into the Assessment**

**77. What is the scope of an antifraud program and controls?**

An antifraud program and controls are those controls related to the prevention, deterrence and detection of fraud. They are the controls that are intended to mitigate the risk of fraudulent actions that could have an impact on financial reporting. Examples include:

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

The PCAOB provides that there be an annual assessment of all controls specifically intended to address the risks of fraud that could have a material effect on the financial statements. The approach to evaluating the design and operating effectiveness of the antifraud program is no different than it is for other controls, except that the focus is primarily on management fraud and the risk of management override of controls. This evaluation takes place at the company level because the control environment includes, but is not limited to, controls specifically established to prevent and detect fraud that is reasonably possible to result in a material misstatement of the financial statements. It also takes place at the process level with the identification of specific controls that mitigate the risk of fraud within key processes. See Question 84 for additional discussion of the entity-level assessment and its impact on the assessment conducted at the process level.

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

There is relatively little new with respect to the nature and causes of fraud itself. However, the fraud regulatory environment has changed dramatically, elevating expectations of management and auditors in recent years. SOA, Statement on Auditing Standards (SAS) 99, the SEC, the Federal Sentencing Guidelines as well as others require stronger antifraud programs and related controls. For example, SOA sets the expectation for reliable financial reporting. SAS 99 sets requirements for external auditors and, in Auditing Standard No. 2, the PCAOB makes the consideration of fraud more explicit during the assessment of internal control over financial reporting. The Federal Sentencing Guidelines have been enhanced and require stronger antifraud programs. In addition, corporate fines have been substantially increased and stiff jail terms have been set for obstruction of justice and securities fraud.

In Auditing Standard No. 2, the PCAOB also clarifies that the focus on fraud, from a financial reporting context, is directed to matters that could result in a material misstatement of the financial statements. It is within this context that management has the responsibility to prevent, deter and detect fraud. The PCAOB also takes the position that deficiencies in the antifraud program and controls are at least a significant deficiency in internal control over financial reporting. Furthermore, the SOA and revised NYSE and NASDAQ listing requirements as well as Auditing Standard No. 2 place greater responsibility on audit committees to provide oversight with respect to financial reporting and internal control over financial reporting. This oversight extends to reporting, documentation, investigation, enforcement and remediation related to fraud.

For many companies, the current antifraud model:

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

The above model is inadequate to accomplish the new regulatory initiative in the post-SOA world, as outlined above. While there is no “one size fits all” and the various regulations allow for some flexibility in approach, companies need an effective antifraud program in place with senior management involved in supervising it. That said, management must be prepared to demonstrate they have developed an effective antifraud program. Following are attributes of an effective program:

- There should be strong emphasis on creating a culture of honesty and high ethics, evaluating antifraud processes and controls, and developing an appropriate oversight process.
- Both management and the audit committee are focused on an effective antifraud program. Both receive reports evidencing effective operation of the antifraud program.
- Ineffective “silo” management of fraud risk is eliminated as the fraud risk focus is broadened and integrated with other aspects of the business. For example, enterprise, business unit, industry and geographic fraud risk assessments are conducted.
- Audit committee, board, external auditors, internal audit, and other advisors collaborate on a regular basis to ensure the antifraud program is effective and meets the requirements of all applicable regulations, laws and rules.

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

Following is a list of 10 suggested steps for management:

- *Ascertain comprehensiveness of the program.* Determine that the antifraud program has all requisite elements. For example, does the program have the key elements of the Federal Sentencing Guidelines? Does it consider the key elements of SAS 99, The IIA fraud guidelines, and the AICPA fraud task force Antifraud Program Guidelines? Does the program involve all key business processes, business units and divisions that significantly impact financial reporting? Is there an effective pre-employment screening process? Is there segregation of duties? Is there due diligence with respect to suppliers and business partners? Does management determine whether the antifraud program is integrated throughout all new acquisitions and expansion efforts of the organization? These and other questions facilitate the assessment of the antifraud program to ensure it is sufficiently comprehensive.
- *Maintain tone at the top.* Evaluate the evidence of tone at the top, including the policies and processes prohibiting management override of controls. For example, does senior management actively support the antifraud program efforts? Is there consistency in the way the code of conduct is enforced across all locations and units? Are there controls over non-routine transactions? Are company-level controls adequately documented? Do company-level controls include codes of conduct and fraud prevention that apply to all locations and units?
- *Assess fraud risk.* Determine the specific industry, geographic and other relevant fraud risks and ensure the antifraud program considers these risks. What are the specific industry fraud risks? What are the geography-specific fraud risks (e.g., risks pursuant to the Foreign Corrupt Practices Act)? Fraud risks may be assessed using a scenario approach, by evaluating risks with specific processes and by considering applicability of relevant fraud risk indicators. See Question 80 for further discussion of these approaches.
- *Identify mitigating controls.* Does the antifraud program consider the identified fraud risks? For example, controls should be linked to specific fraud risks identified at both the entity and process levels. With regard to the design of controls, the PCAOB states that a company's documentation should encompass "the design of controls to prevent or detect fraud, including who performs the controls and the related segregation of duties."
- *Conduct fraud testing.* Management must determine the controls that should be tested, including the antifraud program and controls. Internal audit activity relating to fraud should be adequate and the internal audit function should report directly to the audit committee. The audit committee should demonstrate an adequate level of involvement and interaction with internal audit on fraud matters.
- *Maintain effective code of conduct.* The PCAOB requires documentation of the code of conduct provisions, especially those related to conflicts of interest, related party transactions, illegal acts and the monitoring of the code by management and the audit committee or board. If there is a code, is it public? Is it communicated adequately throughout the organization? Is it periodically reinforced? Is it enforced consistently?
- *Exercise antifraud program oversight.* Fraud needs to be on the agenda of audit committee meetings, disclosure committees and fraud program management at appropriate times. There should be clear documentation of such considerations to establish the viability of the antifraud program.
- *Identify and investigate complaints.* There should be adequate procedures for handling complaints and for accepting anonymous, confidential submissions of concerns about questionable accounting or auditing matters. Determine whether the audit committee has established procedures to handle anonymous, confidential complaints and submissions regarding financial reporting and/or audit irregularities. Is there a "whistleblower" process in place in accordance with SOA Section 301? What is the frequency of reported frauds? Is there a procedure in place to ensure independent investigations and remediation? What testing is conducted to determine if fraud is reported, investigated, and resolved in the manner described in the antifraud program?
- *Remediate deficiencies timely.* When deficiencies in the antifraud program are identified, they should be remedied in a timely manner.

- *Consult with advisors.* Management should consult with legal advisors, fraud specialists and the external auditors as the company documents, evaluates and refines the antifraud program.

## 80. How are fraud risks assessed?

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

When using the “common scenarios” approach to conduct a risk assessment, management’s approach is to first identify relevant scenarios that potentially could occur within the organization, resulting in a material impact on the financial statements. For each identified scenario, the Section 404 compliance team describes how the scenario would be perpetrated within the company, the individuals who could make it happen and the financial statement accounts that would be affected. Based on the documented scenarios, the team then identifies the controls that would prevent, deter or detect each scenario. These controls documented through this step would be compared with the controls in place and gaps would be identified. An action plan would be developed to remediate significant gaps.

When using the “process-by-process” approach to document the antifraud program and controls, management should, according to PCAOB Auditing Standard No. 2, “identify and document the points within [each significant] process where a misstatement – *including a misstatement due to fraud* – related to each relevant financial statement assertion could arise.” Then management must identify and document the controls that have been implemented to address these potential misstatements. Risk and Control Matrices (RCMs) can be useful in this regard. For example, the Section 404 compliance team can review the RCMs to ascertain whether the fraud risks already identified are complete. When applying this approach, remember it is important to move beyond third-party fraud to consider risk of management override, particularly in the financial close process and in non-routine and estimation processes.

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

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

There are three key words going forward: “Make fraud explicit.” Make fraud explicit in the company’s risk assessment and controls design and testing. Make fraud explicit during the entity-level controls assessment. Make it explicit during the review of the financial reporting process and when identifying assertion risks at the process level.

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

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

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

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

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

The approach to evaluating the design and operating effectiveness of an antifraud program and related controls is no different than it is for other controls. In fact, many elements of the antifraud program and controls are often already in place. Many companies are implementing other elements of the antifraud program and controls, e.g., initiatives relating to SOA Sections 301, 406 and 407. The documentation of controls on risk and control matrices often identifies some controls that serve a dual purpose of mitigating risks of inadvertent and intentional errors. All told, fraud prevention and deterrence and the mitigation of related financial reporting risks must become a more active part of the management and audit committee agenda.

---

## Identifying, Documenting and Assessing Controls

### **82. 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, authorizing, recording, processing and reconciling account balances, classes of transactions and disclosure and related assertions included in the financial statements
  - Controls related to the initiation and processing of 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 126, and review that plan with the independent auditor.

### **83. 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.

#### **84. 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 43, 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 56 and 57 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 43 for further explanation). Overall results and documentary evidence should be validated (see next question).

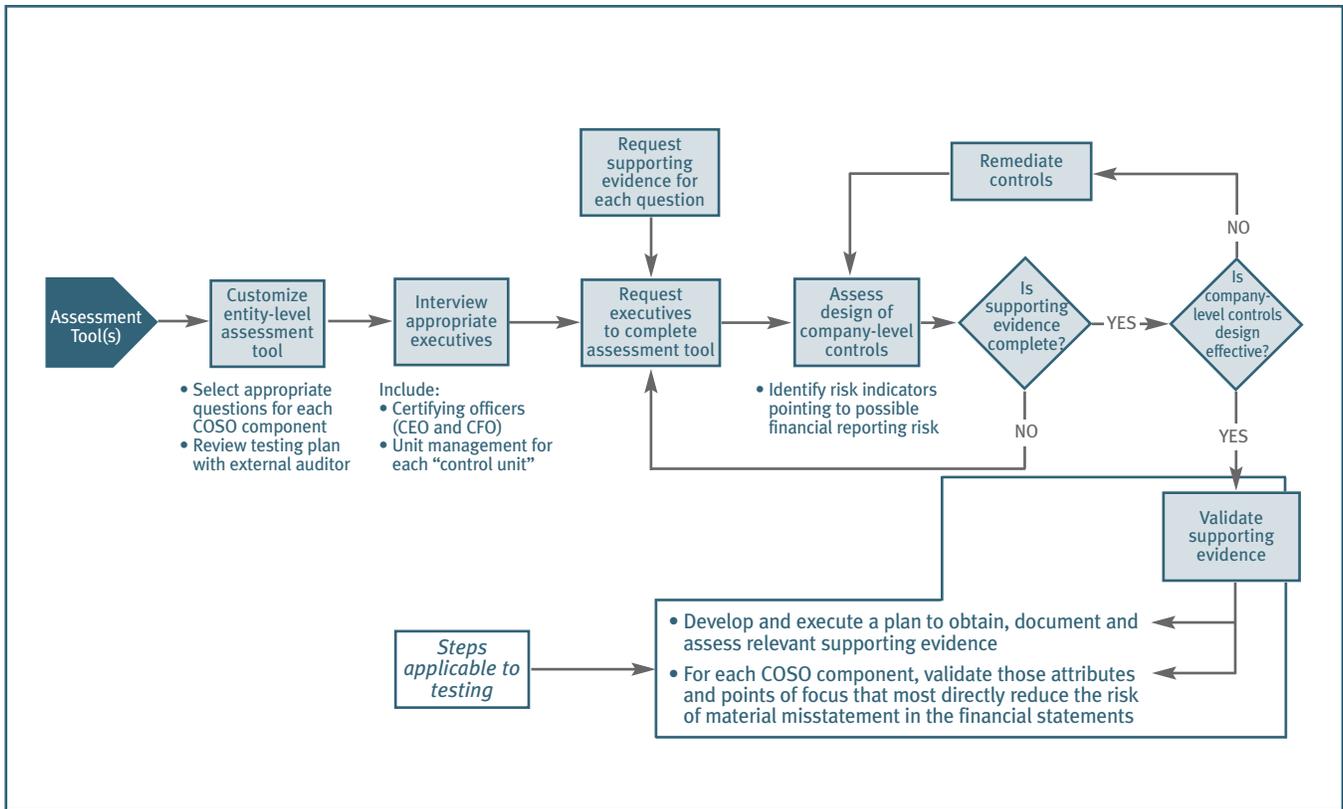
Based on the results of the assessment and validation activities, a conclusion that the entity-level controls are effective may reduce the need to document processes, risks and controls in less significant areas that are not susceptible to material misstatements. Negative assessments about the entity-level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

## **85. 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.

Following is an approach to evaluating company-level controls:



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

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. These are common techniques for validating “tone at the top” and supplementing the use of inquiry and observation techniques.
- Validation procedures might include steps such as:
  - Periodic discussions with key members of the management team regarding operating issues and the resulting financial reporting implications
  - Reviews of evidence documenting the effective operation of specific control activities, including financial and operating reports, written explanations and analyses of variances, internal audit reports, written plans for corrective action, written codes of conduct, board minutes, conflict-of-interest policies, HR policies, etc.
  - Evaluation of the process for communicating the code of conduct and handling exceptions to the code
  - Obtaining an understanding of documented authorizations and job descriptions for key financial reporting functions and determining there is an adequate understanding of roles, responsibilities and authorities
  - Review management’s process for identifying and prioritizing risk
  - Corroboration of important discussions with key members of senior management by review of pertinent company reports, and analyses and inquiries of line management and process owners
  - Reviews of company reports evidencing the planning and budgeting process
  - Obtaining an understanding of processes for updating accounting policies whenever there are changes in policies
  - Observations of senior management personnel in the performance of their duties to understand the processes they use to control the business, e.g., attendance at regular budget review meetings, loan approval committee meetings, etc.

Note that the project team need not validate the existence and effectiveness of each and every response supporting the various points of focus underlying each attribute at the entity level (see Question 43 for an explanation of these terms), but rather only those responses considered most significant to management’s overall assessment of internal control over financial reporting. For example, assume a company’s budgetary control process includes evaluation of external and internal environmental factors, interactive participation of top management and line personnel, timely comparison of actual results against plan, appropriate management investigation and review of actual results and significant variations from plan, and effective corrective action. In order to be satisfied that the budgetary control process is functioning effectively as an ongoing monitoring process, the project team need not observe or review evidence supporting each step of the process.

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

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

#### **86. Are entity-level controls the same thing as entity-wide controls?**

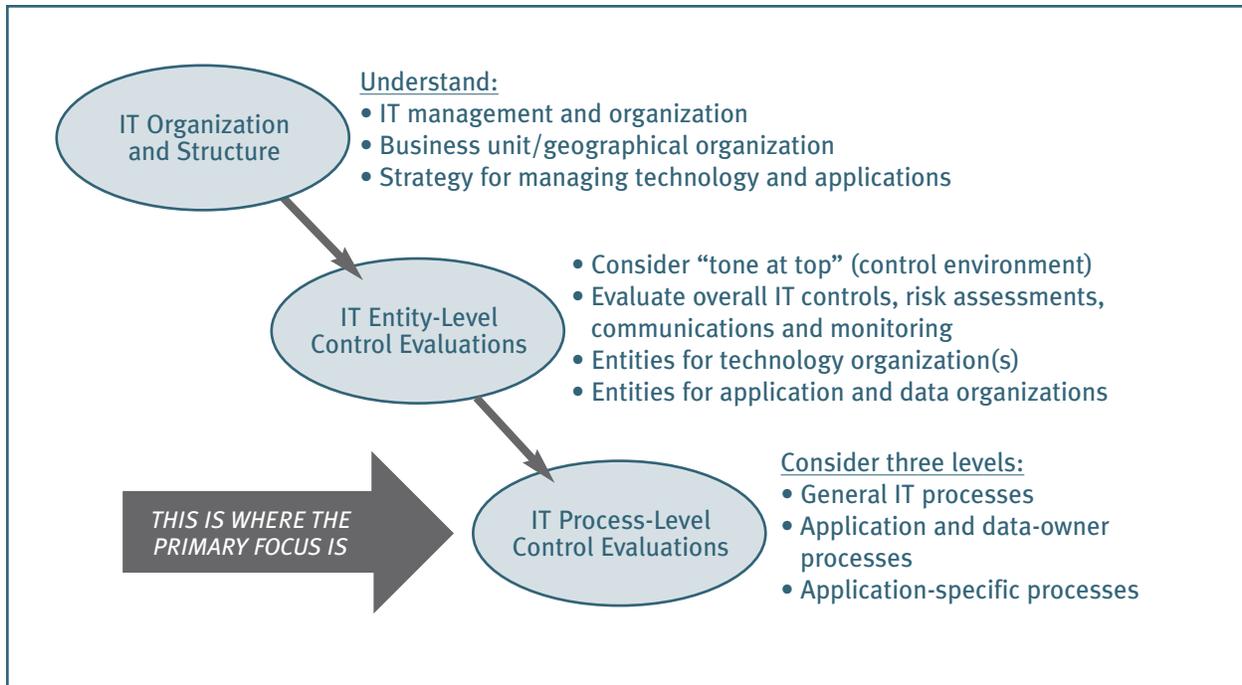
No. Entity-wide controls include entity-level controls plus controls over processes that are entity-wide in scope. For example, entity-wide controls include:

- 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 period-end financial reporting process
- Board-approved policies that address significant business control and risk management practices

#### **87. How are IT risks and controls considered?**

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

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



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

- **General IT Processes** – The review of general IT controls addresses the critical IT processes within each entity or for each key location that supports key financial reporting-related applications. General controls typically impact a number of individual applications and data in the technology environment. As a general rule, these controls impact the achievement of the financial statement assertions germane to critical processes by supporting an environment that provides for the integrity of processing and data. The general IT processes which should be evaluated in almost every instance include:
  - Security administration
  - Application-change controls to ensure that changes to application systems (through systems development, upgrades and maintenance) are authorized, tested and approved before they are implemented
  - Data management and back-up/recovery
  - Data center operations and problem management
  - Asset management

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

- **Application and Data-Owner Processes** – The processes evaluated in this area are those that should be controlled and owned directly by the application and data owners. Typically, application and data owners are part of the business process. Often they also own the overall business process from a controls design and operations perspective. The overall process owner can delegate this ownership to someone, but the process owner must clearly communicate what is expected out of the delegate. The application and data

owner must take responsibility to understand, design and maintain the controls within the application. These individuals must understand computerized controls so that they can knowledgeably design such controls and communicate these needs to IT personnel. The application and data owner also must understand the limitations of computerized controls, and be able to assist in the design of detective and monitoring controls that may be needed to compensate for weak general controls for certain IT processes.

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

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

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

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

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

#### **88. What if transaction processing is outsourced?**

When transaction processing is outsourced, management must still assess controls over processing that are significant to the company's systems which impact financial reporting and disclosures and the related controls. IT and other control issues exist regardless of whether the processing takes place internally or externally. Under the provisions of Section 404 of SOA, management must evaluate the controls over the process activities and applications that are critical to the company's internal control over financial reporting. This evaluation must be directed to processes and applications that the company operates and

processes and applications that the company outsources to external service providers. The PCAOB has reinforced this point of view.

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

The evaluation of internal controls resident in business processes should consider the controls needed to achieve all relevant financial statement assertion objectives, which are likely to require appropriate controls residing at the service organization (outsourcer). During a Section 404 compliance project, these controls must be evaluated and tested like any other controls for a process or an application managed and controlled directly by the company. The SEC and the PCAOB have made it clear that the use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting. Organizations may accomplish this evaluation and testing through either an SAS 70-type report provided by the outsourcer (provided the issues noted 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 also map key master file maintenance processes and user organization security administration procedures for the application because, typically, the key controls over authorization and segregation of duties are internal to and under the control of the user organization.

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

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

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

- First, while a reading of an SAS 70 report clearly indicates that it is an auditor-to-auditor communication and it is possible that the now-defunct Auditing Standards Board did not intend for it to be used for management reliance from a regulatory standpoint, the PCAOB has a different idea. In Auditing Standard No. 2, the PCAOB clearly extends the use of SAS 70 reports to management. If the outsourcing agreement is appropriately modified to articulate the SAS 70 report requirements, then the letter and reporting relationship can be conformed to satisfy those requirements. Both user and service organizations may want to seek advice from legal counsel as they review the legal aspects of this reporting and the reliance on it.
- Second, the scope of the SAS 70 review needs to be evaluated carefully. Prior periods' scope to satisfy the auditors for purposes of expressing an opinion on the financial statements may need to be expanded, perhaps significantly, to satisfy the additional requirements of management. For example,

the SAS 70 report must address relevant financial reporting assertions and focus on both design and operating effectiveness. Again, this is an area for which management is clearly responsible under 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 user's financial statements.

- Finally, we expect companies and their service providers to take advantage of the SEC's extension of the Section 404 transition period by renegotiating their service agreements. For example, management may specify its testing requirements in the outsourcing agreement, and the report issued by the service provider's auditor can refer to those requirements. Many outsourcing service providers may, in fact, look to coordinate these types of requirements with all of their clients and their independent accountants in order to avoid a time-consuming, case-by-case approach.
- There is also the matter of the point-in-time internal control report that management must issue to comply with Section 404 as of its annual report year-end. An SAS 70 report may cover either a point in time or a period of time, with a warning about projecting the results into the future. Typically an SAS 70 report is a point-in-time report with a warning about projecting the results into the future. How would this requirement affect management's ability to sign off on its assertion about the controls as of year-end if the date of the SAS 70 report differs significantly from that date?

From a practical standpoint, unless service organizations choose to have their auditors issue periodic (e.g., quarterly) SAS 70 reports that they can provide to interested user organizations, there will almost always be a difference between the time period covered by the SAS 70 report and the date of management's assessment. The PCAOB decided not to provide a "bright line" test as to when a significant period of time has elapsed between the period covered by the service auditor's report and the date of management's assessment. The Board probably anticipated a difference of six months or more when it provided guidance as to the procedures necessary to address such differences. For example, management should understand at a minimum whether there have been changes in the service organization's controls subsequent to the period covered by the service auditor's report. Such changes might include:

- changes communicated from the service organization to management;
- changes in service organization personnel, with whom management interacts;
- changes in reports or other data received from the service organization; or
- errors identified in the service organization's processing.

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

While there are many issues that should be considered, it is clear that for significant applications some work at the service organization is required. A satisfactory SAS 70 report is a useful tool for obtaining evidence as

to the effectiveness of internal controls at a service organization. The financial reporting implications of the outsourcing arrangement are 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.

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

#### **89. Do SAS 70 reports apply to processes other than IT and to specialists?**

SAS 70 reports apply to all outsourced business processes. In Auditing Standard No. 2, the PCAOB states, "When the service organization's services are part of the company's internal control over financial reporting, management should consider the activities of the service organization in making its assessment of internal control over financial reporting ...." For example, SAS 70 reports apply to processes that include more than IT, such as payroll processing, tax return preparation, tax provision and reserve calculation, and accounts payable processing.

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

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

The auditing literature requires the auditor to evaluate the above matters; therefore, management should be prepared to respond to questions regarding these matters.

#### **90. Where does an entity-level 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, authorizing, 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.

## **91. How is the process- or activity-level assessment conducted?**

Question 44 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 Questions 74 and 75 for illustrations). 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 risks and controls discussed in Question 87.

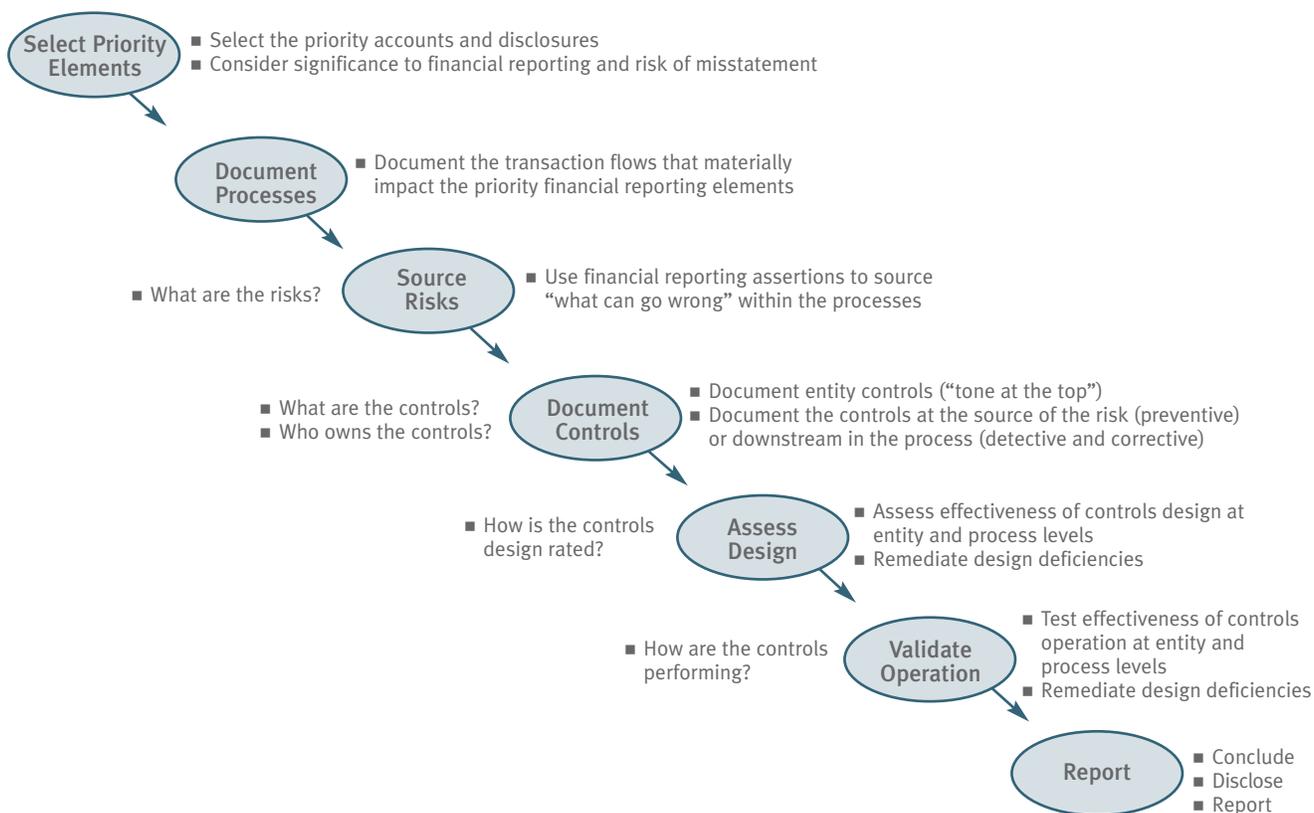
**Assess design effectiveness** – After the risks and controls are documented, the project team evaluates whether the controls, as designed, provide reasonable assurance that the risks have been reduced to an acceptable level, i.e., the stated financial control objectives have been met. If there are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

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

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

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

## A PLAIN ENGLISH SUMMARY



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

The PCAOB requires the independent auditor to perform walkthroughs for all major classes of transactions that are significant to the company’s financial statements. Major classes of transactions are broken down into routine transactions, non-routine transactions and estimation transactions. See Question 69.

The purpose of walkthroughs is to enable the auditor to obtain a sufficient understanding of the organization’s processes, risks and controls so he or she can effectively evaluate controls design and plan effective tests of controls. The PCAOB acknowledges that the goals of a walkthrough might in certain circumstances be achieved by performing a combination of procedures (i.e., inquiry, inspection, observation and reperformance). The Board also points out that, as a test of controls, inquiries might be made concurrently with performing walkthroughs.

The focus of a walkthrough is on the activities to initiate, authorize, record, process and report transactions. It includes procedures for correcting and reprocessing previously rejected transactions and for correcting erroneous transactions through adjusting journal entries.

For purposes of the external audit, walkthroughs **MUST** be performed by the auditor and not by management or internal audit. However, to provide additional evidence, the auditor may also review the work of others who have performed and documented walkthroughs.

In preparing for the walkthroughs, management and Section 404 compliance teams should prepare process maps for all major classes of transactions. We believe that process maps provide an excellent tool for

providing the auditor the transparency he or she needs for an effective walkthrough (see Question 93 for further discussion about process mapping). In addition, process owners must be prepared. For example, to facilitate the walkthrough, they should have available legible copies of the most up-to-date materials, key control reports, screenshots and forms. Process owners need to focus on describing their processes and avoiding speculation about who does what in other groups, departments or units. They should ascertain that the documentation provided is consistent with the documentation requested. They need to be prepared to demonstrate the control activities for which they are responsible. For example, if the signature block is supposed to be locked, they should be sure to lock up after showing it to the auditors.

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

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

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

We are aware of companies training their process owners to facilitate preparation, using the new standard to provide insights as to what the auditor will be looking for. We believe this is a smart approach. All told, process owners must understand that during the walkthrough the auditor is carefully evaluating them and their subordinates in terms of their skill and competence in performing the process and the related controls. The auditor will be looking for answers to the “how do you know” questions. For example, how do you know the process results are reliable? How do you know all transactions that should be processed during the period are in fact processed? How do you know that transactions are processed accurately? Expect a stronger emphasis on understanding the application of manual controls, including who is responsible for performing them, how often and when.

The Board also states in Auditing Standard No. 2 that unless significant changes in the process flow of transactions, including in the supporting computer applications, make it more efficient for the auditor to prepare new documentation of a walkthrough, the auditor may carry his or her documentation forward each year, after updating it for any changes that have taken place.

### 93. 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, authorized, recorded, processed and reported. This understanding will enable the team to source the risk of errors and omissions and assess the controls that mitigate these risks. Furthermore, the nature of the documentation will vary according to the nature of the transactions involved. In Question 69, 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.
- AUTHORIZE
  - Describe the procedure by which transactions are approved for processing, including what specifically is approved, who approves and timing of approval.
- RECORD
  - Describe how authorized transactions are accepted for input into processing, including online entry procedures.
- PROCESS
  - Describe the significant processing activities, including processes for correcting rejected transactions and re-entering them into processing.
  - Identify the critical data files used during processing (e.g., customer, pricing, accounts receivable, credit, perpetual inventory, 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?

In Auditing Standard No. 2, the PCAOB provides insights to answering these questions with the following direction:

For each significant process, the auditor should:

- Understand the flow of transactions, including how transactions are initiated, authorized, recorded, processed and reported.
- Identify the points within the process at which a misstatement – including a misstatement due to fraud – related to each relevant financial statement assertion could arise.
- Identify the controls that management has implemented to address these potential misstatements.
- Identify the controls that management has implemented over the prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets.

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

Process mapping is a valuable tool for documenting processes and transaction flows; however, it is 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.
- **Supports auditor walkthroughs** – Facilitates the walkthrough process by providing a visual depiction of all important aspects of each critical process.
- **Enables focus on change** – Provides a way to identify process changes during subsequent reviews.
- **Provides operating benefits** – 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 might 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

#### **94. 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, authorizing, recording, processing and reconciling account balances, classes of transactions, and disclosure and related assertions included in the financial statements
- Controls related to the initiation and processing of 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:

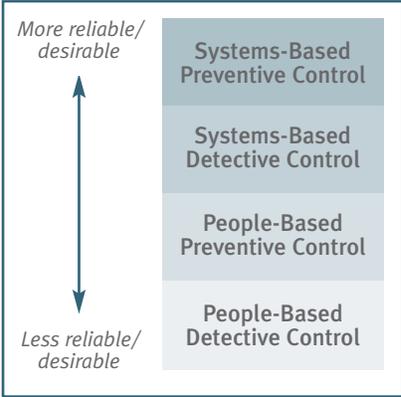
- Controls, including general controls, on which other significant controls are dependent
- Each significant control in a group of controls that functions together to achieve a control objective
- Controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; initiate, authorize, 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"> <li>• Establish and communicate objectives</li> <li>• Authorize and approve</li> <li>• Establish boundaries and limits</li> <li>• Assign key tasks to quality people</li> <li>• Establish accountability for results</li> <li>• Measure performance</li> <li>• Facilitate continuous learning</li> <li>• Segregate incompatible duties</li> <li>• Restrict processing system and data access</li> <li>• Create physical safeguards</li> <li>• Implement process/systems change controls</li> <li>• Maintain redundant/backup capabilities</li> </ul>	<ul style="list-style-type: none"> <li>• Obtain prescribed approvals</li> <li>• Establish transaction/document control</li> <li>• Establish processing/transmission control totals</li> <li>• Establish/verify sequencing</li> <li>• Validate against predefined parameters</li> <li>• Test samples/assess process performance</li> <li>• Recalculate computations</li> <li>• Perform reconciliations</li> <li>• Match and compare</li> <li>• Independently analyze results for reasonableness</li> <li>• Independently verify existence</li> <li>• Verify occurrence with counterparties</li> <li>• Report and resolve exceptions</li> <li>• Evaluate reserve requirements</li> </ul>

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"> <li>• Define processes</li> <li>• Describe procedures</li> <li>• Supervise activities</li> <li>• Evaluate processes to eliminate, simplify and focus nonessential tasks</li> <li>• Test and pilot improvements</li> <li>• Organize cross-functional teams</li> <li>• Design interactive feedback systems</li> <li>• Appraise performance and link to reward system</li> <li>• Capture and share relevant knowledge and information</li> </ul>	<ul style="list-style-type: none"> <li>• Monitor the legal and regulatory environment</li> <li>• Assess impact of environment change</li> <li>• Articulate clearly compliance policies</li> <li>• Communicate compliance policies</li> <li>• Integrate compliance activities into business processes</li> <li>• Manage and monitor compliance</li> <li>• Take remedial and disciplinary action when necessary</li> <li>• Involve counsel in key business affairs</li> <li>• Manage the cost of litigation</li> <li>• Establish a fraud-preventing organization</li> </ul>

As noted in our response to Question 46, some operational and compliance controls may be relevant to reliable financial reporting.

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

The financial reporting process should be evaluated as early in the assessment process as possible to identify the significant upstream processes that “feed” the priority financial reporting elements. Desirably, the financial reporting process should be documented using a LEVEL 3 map, as discussed in Question 93. This analysis should document:

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

Once the 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

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

In Auditing Standard No. 2, the PCAOB states the auditor must determine that management has addressed “controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles.” The question arises as to what these controls are. We believe these controls are integral to the company’s period-end financial reporting process and disclosure controls and procedures.

These controls ensure the company is using appropriate accounting policies, has communicated its accounting policies throughout the organization and is applying the selected policies consistently from period to period. Examples of such controls include the following:

- Qualified financial personnel with the requisite knowledge and subject-matter expertise
- Clear articulation in writing of the critical accounting policies, particularly for the more complex and significant financial reporting areas
- Effective procedures in place that provide reasonable assurance the company is in touch with new developments in financial reporting requirements, including new and emerging releases by regulatory authorities and standard setters
- Appropriate training of personnel who are assigned the task of applying critical accounting policies
- Periodic assessment of accounting policies in high-risk areas to evaluate whether they are sufficiently developed, articulated and documented to ensure objective and consistent application
- Audit committee understanding and approval of the critical accounting policies

Controls over the selection and application of accounting policies are important because the PCAOB states that deficiencies in them are at least a significant deficiency in internal control over financial reporting.

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

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

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

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

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

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

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

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

**99. 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. The independent accountant may refuse to issue an audit report without sufficient control documentation on which to base attestation decisions. In its final rules, the SEC stated:

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

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. That said, there may be occasions where a single control is so critical to the achievement of an assertion, it stands alone because if it fails there may not be adequate compensating controls in place.

In Auditing Standard No. 2, the PCAOB states that the evaluation of controls design effectiveness involves a determination as to whether the controls in place would be expected to prevent or detect errors or fraud that could result in material misstatements in the financial statements. This determination requires three steps: (1) identify the control assertions or objectives in each area, (2) identify the controls that satisfy each assertion or objective, and (3) determine whether the controls, if operating properly, can effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements.

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

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

After the controls design is determined to be effective in reducing financial reporting risks to an acceptable level, selected controls should be validated or tested over 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.

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

Paragraph 84 of PCAOB Auditing Standard No. 2 states, “The auditor should clearly link individual controls with the significant accounts and assertions to which they relate.” How is this linkage achieved?

We do not believe this linkage requirement literally means a list of controls for each significant account. Controls are embedded within processes and processes feed the accounts. Therefore, we believe that assertions provide the vital link between accounts and controls, as follows:

- First, show the linkage of significant *accounts* to relevant financial statement *assertions* (see Questions 74 and 75).
- Second, link the key *accounts* to the *processes* that affect them and assign the relevant financial statement *assertions* to the appropriate processes.
- Finally, show the linkage of *controls* to the *assertions* for the *processes* affecting the priority *accounts*.

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

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

“Reasonable assurance” is the standard that internal controls must meet. Management must attain this level of assurance when formulating a conclusion regarding the effectiveness of internal controls in achieving specific objectives or assertions. This is intended to be a practical standard. No matter how well designed, most systems of internal controls can only provide reasonable assurance to management and the board of directors. There are inherent limitations in any internal control system such that absolute assurance is a cost-prohibitive standard, if not an impossible one. Human judgments in decision-making, breakdowns due to human error and simple mistakes, collusion by two or more people, and even management override can circumvent an effective system of internal controls. Reasonable assurance is a more realistic standard than absolute assurance because of these inherent limitations.

The concept of reasonable assurance is built into the definition of internal control over financial reporting adopted by the 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 230.

**103. 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.

In Auditing Standard No. 2, the PCAOB illustrated the reasonable assurance standard by introducing a “reasonable person test” to facilitate the evaluation of the magnitude of a potential misstatement that might result from a control deficiency. If a “reasonable person” would conclude, after considering the possibility of undetected misstatements, that the misstatement, either individually or when aggregated with other misstatements, would clearly be immaterial to the financial statements, then the control deficiency is not a significant deficiency. If a reasonable person could not reach such a conclusion regarding a particular misstatement, that potential misstatement is more than inconsequential. Thus management must consider what a reasonable person might conclude given the facts and circumstances.

#### **104. How should control gaps be identified and summarized?**

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

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

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

## Internal Controls Capability Maturity Continuum

Capability Level	Capability Description	Capability Attributes	Section 404 Implications
<b>Optimizing</b>	<p>CONTINUOUS IMPROVEMENT</p> <p>Continuously improving controls enterprisewide</p> <p>“Chain of accountability” sustained</p>	<ul style="list-style-type: none"> <li>■ Best practices identified and shared</li> <li>■ World-class financial reporting processes</li> <li>■ Organized efforts to remove inefficiency</li> <li>■ External and internal change monitored for impact on control structure</li> </ul>	<ul style="list-style-type: none"> <li>■ Internal Controls – Integrated Framework fully implemented</li> <li>■ Entity-level analytics and monitoring fully operational</li> <li>■ Faster decisions on improving controls</li> <li>■ Controls preventive and systems-based</li> </ul>
<b>Managed</b>	<p>QUANTITATIVE</p> <p>Risks managed quantitatively enterprisewide</p> <p>“Chain of accountability” is in place</p>	<ul style="list-style-type: none"> <li>■ Control process performance standards established and managed</li> <li>■ Rigorous estimation methodologies and analysis</li> <li>■ Risks are managed quantitatively and aggregated at corporate level</li> <li>■ Process-based solution</li> </ul>	<ul style="list-style-type: none"> <li>■ Controls effectiveness continuously assessed and validated</li> <li>■ Process owners report to management</li> <li>■ Internal audit plans aligned</li> <li>■ Entity-level analytics and monitoring emerging</li> </ul>
<b>Defined</b>	<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"> <li>■ Internal control uniform across the entity</li> <li>■ Transaction flows documented</li> <li>■ Risks of errors and omissions sourced</li> <li>■ Control processes for mitigating risks better documented and integrated</li> </ul>	<ul style="list-style-type: none"> <li>■ All groups accountable to use organization’s control standards</li> <li>■ Remaining <u>known</u> gaps closed</li> <li>■ Control reports not very robust</li> <li>■ Assurance lacking that all deviations from control standards detected</li> </ul>
<b>Repeatable</b>	<p>INTUITIVE</p> <p>Process established and repeating; reliance on people continues</p> <p>Controls documentation lacking</p>	<ul style="list-style-type: none"> <li>■ Common control framework</li> <li>■ Increased controls awareness</li> <li>■ Basic policies and control processes established</li> <li>■ Processes are repeating but not necessarily documented</li> </ul>	<ul style="list-style-type: none"> <li>■ Quality people assigned to support control activities</li> <li>■ Some control gaps identified and fixed</li> <li>■ Communication is lacking</li> <li>■ Limited monitoring activities</li> <li>■ Control structure still not sustainable</li> </ul>
<b>Initial</b>	<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"> <li>■ Reliance on individual initiative</li> <li>■ “Just do it”</li> <li>■ Ad hoc disclosure activities</li> <li>■ Policies not articulated</li> <li>■ Few processes are defined</li> <li>■ Institutional capability lacking</li> </ul>	<ul style="list-style-type: none"> <li>■ Overemphasis on detective controls</li> <li>■ Controls are not periodically evaluated for deficiencies</li> <li>■ Success depends on manual efforts and validation by seasoned managers</li> <li>■ Gaps result when key people leave</li> </ul>

- 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, improved quality and reduced risk – often a result of simplifying, focusing and automating processes and eliminating non-essential tasks – 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.

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

Assume the assessment of controls design and operational effectiveness is complete and 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. Control deficiencies vary in significance. They may be either inconsequential or significant. If significant, they could also constitute a material weakness.

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

So what happens after the evaluation of design and operating effectiveness is completed? An action plan should be developed to close the identified gaps. First, management must design a solution to close the gap. Then management must implement the solution. An action plan for designing solutions to close identified control gaps should differentiate between design and operating deficiencies. For design deficiencies, a detailed design is critical to ensure the proposed solution improves control and meets the company’s needs. 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 104) and measure performance to ensure control operates in accordance with the design. Such remediation efforts will often focus on increasing controls design effectiveness by automating manual controls, improving the mix of preventive and detective controls, placing the point of control at the source of the risk, simplifying overly complex control procedures, and improving monitoring and analytics. For operating deficiencies, management often will focus on updating and publishing policies to clarify roles and responsibilities, implementing hiring and training initiatives to ensure the requisite competence and resources are brought to bear, and measuring performance for evidence of reduced exceptions and deviations.

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

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

#### 106. How does a company define a “control deficiency”?

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. When testing controls to determine whether they are operating effectively, exceptions will

be noted. The existence of control exceptions does not necessarily mean a control deficiency exists. Internal controls are not expected to operate perfectly, all the time, to be effective. Auditing Standard No. 2 recognizes the inherent limitations of internal control. However, as noted in Question 127, the PCAOB has stated, “A control with an observed non-negligible deviation rate is a deficiency.”

#### **107. How are compensating controls considered?**

Compensating controls are not considered when determining whether a control deficiency exists. Control deficiencies must be considered individually and in isolation. Compensating controls are appropriately considered when evaluating whether a significant deficiency or a material weakness exists; however, to have a mitigating effect, a compensating control must operate at a level of precision that would prevent or detect a misstatement that is more than inconsequential or material, respectively.

#### **108. 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. However, the PCAOB defined the term “significant deficiency” in a different manner that would likely result in reporting more control deficiencies than have been reported historically as so-called “reportable conditions.” The Board concluded that the auditing literature’s definition of the term “reportable condition” was inadequate because it primarily relied on the auditor’s judgment. While judgment will always be a factor, the Board indicated that it believes that auditors as well as management need a more rigorous definition that they could apply when complying with Section 404. Thus the Board defined a significant deficiency as follows:

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

The Board defined “remote likelihood” consistent with how that term has been used in accounting for loss contingencies for many years, i.e., the likelihood of occurrence is more than remote when it is either “reasonably possible” or “probable.” In defining “more than inconsequential,” the Board introduced a “reasonable person” test. That test provides that if a reasonable person could not conclude that potential misstatements resulting from a control deficiency (or a combination of deficiencies) would clearly be immaterial to the financial statements, the potential misstatement is “more than inconsequential.”

When evaluating whether a significant deficiency exists, the PCAOB staff has explained that the threshold for “more than inconsequential” is not necessarily equivalent to the amount the auditor establishes for purposes of listing proposed audit adjustments arising from the auditor’s substantive tests during the financial statement audit. The Board’s explanation of this point basically boils down to the auditor’s exercise of professional judgment as to what constitutes a “more than inconsequential” amount. Therefore, there is no requirement to align that threshold with the auditor’s scope for accumulating proposed audit adjustments.

The Board supplemented its guidance with a list of deficiencies that are considered at least significant deficiencies in internal control over financial reporting because of the interaction of qualitative considerations with quantitative considerations. The list included deficiencies in:

- Controls over the selection and application of accounting policies that are in conformity with GAAP;
- Antifraud programs and controls;
- Controls over routine and non-systematic transactions; and
- Controls over the period-end financial reporting process, including controls over procedures used to

enter transaction totals into the general ledger; initiate, authorize, record and process journal entries into the general ledger; and record recurring and nonrecurring adjustments to the financial statements.

In addition, the Board listed circumstances representing de facto significant deficiencies as well as “a strong indicator” that a material weakness in internal control over financial reporting exists:

- Restatement of previously issued financial statements to reflect the correction of a misstatement
- Identification by the auditor of a material misstatement in financial statements in the current period that was not initially identified by the company’s internal control over financial reporting
- Oversight of the company’s external financial reporting and internal control over financial reporting by the company’s audit committee is ineffective
- The internal audit function or the risk assessment function is ineffective at a company needing such a function to have effective monitoring and risk assessment
- An ineffective regulatory compliance function for complex entities in highly regulated industries
- Identification of fraud of any magnitude on the part of senior management
- Significant deficiencies, previously communicated to management and the audit committee, remain uncorrected after some reasonable period of time
- An ineffective control environment

The Board provided guidance with respect to the above circumstances that is not repeated here.

In summary, the PCAOB concluded that a deficiency in internal controls is significant if it could adversely affect the company’s financial reporting process and the critical processes that feed data and information to the financial reporting process. Consistent with the Board’s risk-based approach, the context for evaluating the significance of a deficiency in internal control over financial reporting is management’s assertions as to the fairness of presentation of financial condition, results of operations and cash flows, as expressed in or implied by both the financial statements and the executive certifications.

A significant deficiency in internal controls could arise 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 on financial reporting is more than inconsequential 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” in accordance with the PCAOB’s criteria, 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 control deficiency that it believes could adversely affect the company’s ability to record, process, summarize and report financial data (and, therefore, could be a significant deficiency), it should discuss that deficiency with the independent public accountant, the internal auditors and the audit committee before finalizing a conclusion that the deficiency does not have an adverse impact. This is particularly important because, as explained above, 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 during the year. This situation could potentially increase management's exposure if these matters resulted in errors or omissions in the company's interim financial reporting and were not reported on a timely basis, particularly if they came to management's attention earlier.

### **109. How does a company define a “material weakness” in internal control?**

For many years, the AICPA defined 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 Section 404 release, indicating that the term “material weakness” has the same meaning as in the definition under GAAS and attestation standards. The PCAOB, however, decided to encourage more consistent application by defining a “material weakness” using the same general framework as used to define a “significant deficiency.”

The PCAOB defines a material weakness as follows:

A significant deficiency, or a combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected.

The Board's framework for evaluating deficiencies in internal control over financial reporting is therefore based on an assessment of the magnitude of the potential misstatement and the likelihood of occurrence. When evaluating likelihood a deficiency could result in a misstatement of an account or disclosure, many factors are considered including:

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

When evaluating magnitude of a potential misstatement, many factors are considered including:

- The financial statement accounts or the total of transactions exposed to the deficiency
- The volume of activity in the account balance or class of transactions exposed to the deficiency that has occurred in the current period or that is expected in future periods

With respect to evaluating the potential for overstatement, the maximum amount is the recorded amount. The recorded amount, however, is not a limitation on the amount of potential understatement.

In the final Section 404 rules, the SEC points out that a “material weakness” and a “significant deficiency” both “represent deficiencies in the design or operation of internal control that could adversely affect a company’s ability to record, process, summarize and report financial data consistent with the assertions of management in the company’s financial statements, with a ‘material weakness’ constituting a greater deficiency than a ‘significant deficiency.’” Due to the need for guidance, the PCAOB provided its “likelihood” and “magnitude” framework.

What’s the message? 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 deficiency is identified, management should evaluate the severity of the control deficiency and determine whether the control deficiency is an insignificant deficiency, a significant deficiency or a material weakness. For purposes of this evaluation, both the Board and the SEC assert that an aggregation of significant deficiencies could constitute a material weakness in a company’s internal control over financial reporting. Further, the PCAOB staff has indicated that a control deficiency, which in isolation is not a significant deficiency, may be considered in combination with one or more significant deficiencies to determine whether a material weakness exists.

Needless to say, this is a complex determination that often must consider the financial statements taken as a whole and the overall financial reporting picture before an informed conclusion can be reached. There are many issues that come into play when making an assessment as to whether a control deficiency is a material weakness. For example, the effectiveness of the overall control environment, the nature of the identified control deficiency and compensating controls, the nature of the assets at risk, the presence of other control deficiencies and the extent of changes in company practices and procedures are examples of such issues. Because of the complexity of these issues, management may want to consult with the independent public accountant if there is any question as to whether a deficiency or a combination of deficiencies in internal control is a material weakness. These issues are discussed further below:

Management will often consider the characteristics of the identified control deficiency. The following factors should be considered when evaluating the magnitude and likelihood of one or more identified control deficiencies:

- The overall control environment. The overall operating environment and management attitude regarding internal control over financial reporting are important factors. A deficiency in a specified area would be considered much more significant when the environment is weak (for example, incompetent personnel and/or general understaffing, high employee turnover, liquidity problems, lack of written policies and procedures, lack of senior management concern about controls, excessive reliance on manual detection controls, etc.) than when the environment is strong and well controlled due to established policies, documented procedures, competent personnel, adequate training, proper supervision and prompt follow-up.
- Nature of the identified control deficiency and compensating controls. Control deficiencies may be categorized as relating to either a preventive control or detective control. Sometimes, preventive control deficiencies 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 deficiency might be fully mitigated by the detective control. However, detective controls are seldom as effective as preventive controls. In a mature, well-controlled company, there are usually effective, systems-based controls in place to control errors at or near the start of information flows (an example of controlling risk at the source). If a company doesn’t implement the right controls at the start of the flow (i.e., the control point is not at the source of the risk), it is extremely difficult as well as costly and inefficient to find and fix errors later. Accordingly, weaknesses in preventive-type controls often represent a significant deficiency or material weakness, notwithstanding the existence of compensating (detective type) controls. The reason for this point of view is that the internal control structure is not sustainable if it is totally reliant on detective controls.

- Nature of assets at risk. The nature of the assets that might be affected by a control deficiency 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 deficiencies. 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. Both the SEC and PCAOB have made this point clear.
- The extent of changes in company practices and procedures. The extent of recent changes, if any, in the company's accounting procedures or business practices is yet another factor to consider. For example, significant changes in operations, personnel, procedures and/or accounting systems not only increase the potential for material errors in the processing of transactions, but also reduce the chances for detection when controls are generally weak. Conversely, even in a situation in which some control deficiencies are present, if there have been no changes in processing routines or business practices, the probability that material errors could occur and go undetected by detective controls may not be as great as in the former situation. This is why reliance on manual, ad hoc processes results in a sustainability issue during stressful times.

Notwithstanding the above, the independent auditor will take into account factors related to the integrated audit model required by the PCAOB when applying the Board's evaluation framework. For example, the auditor must consider the results of substantive 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 audit adjustments to determine whether they result from a control deficiency. To illustrate:

- Proposed adjustments that are the result of fraud (intentional misstatements, misappropriation of assets or illegal acts) may be indicative of a material weakness.
- The PCAOB listed several circumstances, each of which is "a strong indicator" that a material weakness in internal control over financial reporting exists. These are listed in the response to Question 108.
- Proposed adjustments that result from inadequacies in controls over transaction processing and their summarization in the books and records ordinarily would be indicative of a control deficiency, the magnitude of which would depend upon consideration of the other factors discussed above and below.
- Proposed adjustments involving accounting estimates that result from a flawed process, incompetence of company personnel or inaccuracies in the underlying data upon which the estimate is based ordinarily would be indicative of at least a significant deficiency and, depending on the magnitude, could possibly be a material weakness.
- When an assertion regarding a priority financial reporting element is not met, at least a significant deficiency in internal controls exists and possibly a material weakness exists. For example, if material routine transactions are not processed in a manner to satisfy the completeness and accuracy assertion, that condition is at least a significant deficiency and very possibly a material weakness if management is unable to determine that adequate compensating controls are in place or is unable to isolate the magnitude of the potential error (see Question 107).
- 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 or may not be indicative of a control deficiency. For example, a proposed adjustment relating to a difference of opinion between the independent public accountant and management as to the

need for and/or amount of an accrual for a significant and unusual uncertainty (e.g., litigation) may not constitute a control deficiency if there aren't any underlying questions about the fact base.

- The independent public accountant's experience with the entity is also a consideration. For example, does the auditor's experience with the entity indicate that management's processes for making accounting estimates and measuring values that involve significant judgment consistently result in estimates and measures that are overly optimistic, misstated or intentionally biased?

The nature, timing and extent of the audit tests the independent public accountant must perform to reduce residual audit risk may also be a factor. The severity of an identified control deficiency 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 deficiency is a material weakness.

#### **110. Why is the distinction between a significant deficiency and a material weakness so important?**

If a deficiency is a significant deficiency, management must disclose it to the auditors and audit committee as soon as practicable. Generally, disclosure to investors is not required of significant deficiencies, unless (a) the remediation process materially affects or is reasonably expected to materially affect internal control over financial reporting, or (b) a combination of significant deficiencies is considered a material weakness and disclosure of the significant deficiencies is necessary to adequately explain the material weakness.

If a deficiency is a material weakness, management must disclose it to the auditors and audit committee as soon as practicable. In addition, if the deficiency is uncorrected as of year-end, management cannot issue a positive assertion in the internal control report and the external auditor must issue an adverse opinion in the attestation report. Generally, disclosure to investors is required because there is a presumption that the remediation process usually materially affects or is reasonably expected to materially affect internal control over financial reporting.

The distinction between these two types of control deficiencies is important because of the obvious impact on disclosure. It is also important because, in practice, reasonable men and women can differ in distinguishing them. For example, what is a "remote likelihood"? What is the meaning of "more than inconsequential"? What is "material"? How is the "prudent official test" applied? How are deficiencies "aggregated"? There is such a significant level of judgment to be applied in the process of answering these questions, management is advised to fix significant deficiencies as soon as practicable rather than letting them accumulate unresolved. Management should avoid the scenario of having many unresolved significant deficiencies to discuss with the independent auditor at the end of the reporting year.

#### **111. 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.

#### **112. 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 such actions constitute a change that materially affects (or is reasonably likely to materially affect) internal control over financial reporting, as early as possible in the process.

**113. 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 on Section 404, 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. As discussed in Questions 167 and 231, significant improvements in internal control require disclosure if they materially affect, or are reasonably likely to materially affect, the effectiveness of the company’s internal control over financial reporting.

**114. 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.

**115. 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.

**116. 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. In practice, however, most auditors are applying these company-level controls as a justification for minimum testing scopes at the process level. If the entity-level controls are not effective, then scopes at the process level are expanded.

**117. What does it mean that the Section 404 assessment is based on a point in time and why is it important?**

A point-in-time assessment is an evaluation of internal control effectiveness as of a specific date, usually at the end of a reporting period, i.e., a year-end date or quarter-end date. A point-in-time assessment is different from an assessment of controls for a period of time, say the three months of a quarter or the 12 months of a year. A benefit to a point in time assessment is to give management an opportunity to develop and test controls during the course of a financial period, with sufficient time to correct significant control deficiencies prior to the “point in time” at which they must be evaluated. Notwithstanding this advantage, management must disclose to investors any actions that have materially affected, or are reasonably likely to materially affect, the company’s internal control over financial reporting.

From a practical standpoint, the testing plans of many companies spread the effort out over a period of time rather than confine it to year-end. So why the emphasis to a point in time? The point-in-time focus was written into the statute, so the SEC had to work within that construct. As much as commenters have expressed concern about the costs of complying with Section 404, the costs would be even greater if the statute had required a *period* assessment in lieu of a *point-in-time* assessment. Under a point-in-time assessment, the auditor's testing is not as extensive and timing can be directed in subsequent years to the fourth quarter, although as a practical matter auditors may spread out their testing over the third and fourth quarters. It is likely the legislators crafting SOA understood financial reporting and the auditing process well enough to realize this and structured Section 404 accordingly. Point in time also makes it easier for management to remediate a deficiency.

**118. If evaluation and testing are done throughout the year but management's required evaluation and the internal control report are as of year-end, what type of evaluation is necessary as of year-end for management to render the internal control report as of that date?**

Management's approach to testing and evaluating controls at year-end is impacted by the strength of the internal controls and the nature and extent of the evaluation and testing during the year. If the controls are strong, the evaluation and testing during the year have been ongoing and comprehensive, and there have been no significant changes in the company's processes, one approach is to have process owners confirm as of year-end that the key controls for which they are responsible are in place and operating effectively. The self-assessments used by the process owners address the key controls documented during the evaluation and tested during the year. That said, some refresh testing is also required at or close to year-end, particularly for critical routine controls, and controls over non-routine and estimation processes. Controls executed *at* year-end may require testing *after* year-end.

---

## Validation of Operating Effectiveness (“Testing of Controls”)

**119. 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. As it relates to testing, paragraph 40 of PCAOB Auditing Standard No. 2 states the following with respect to management's responsibilities: [Management must evaluate] “the operating effectiveness of controls based on procedures sufficient to assess their operating effectiveness ... such procedures include testing of the controls by internal audit, testing of controls by others under the direction of management, using a service organization's reports, inspection of evidence of the application of controls, or testing by means of a self-assessment process, some of which might occur as part of management's ongoing monitoring activities.”

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 and analytics, 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.

#### 120. 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. Internal auditors, other company personnel or third parties retained by management and under its direction may assist during the validation process so long as management takes responsibility for the work. Management must be satisfied that the testing procedures provide sufficient evidence to support management’s assessment that internal control over financial reporting is operating effectively. In addition, management must be satisfied that assisting personnel are sufficiently objective and competent to perform the required testing procedures. Factors management may consider when selecting an evaluator include the evaluator’s knowledge of the process, internal controls and accounting (competence), the evaluator’s knowledge of the business and industry, limitations of the evaluator’s schedule, and the evaluator’s ability to perform tests in the future.

#### 121. 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.

### **122. 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). Documentary evidence for certain aspects of the control environment, such as management’s philosophy and operating style, might not exist. In circumstances in which documentary evidence does not exist and is not expected to exist, testing of controls must be accomplished through visual observation of entity activities and interviews with control owners and other appropriate personnel.

### **123. 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 the related control objectives and are able to implement the control effectively. Do the control owners know what to look for and how to handle exceptions when they occur? In making appropriate assessments based on interviews, it is often appropriate to crosscheck results with several interviewees to determine the 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.

### **124. 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 “walkthrough” to understand how transactions are processed. While a walkthrough 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.

Quality of evidence is often a factor. To illustrate, a signature on a voucher is not, in and of itself, persuasive evidence of a careful review of the voucher package before signing. Therefore, inspection of the voucher might not be enough. Reperformance of the control through checking prices, extensions and additions may be necessary.

Reperformance of the transaction process is different from reperformance of a control over that process and is often a common source of confusion. Reperformance of the process only provides negative assurance that the controls are not malfunctioning, because accurate processing is not necessarily indicative that the controls

were all operating effectively. Information can be processed correctly even when controls do not exist. Thus it is important to design the reperformance test to validate the controls themselves (through testing for attributes, for example) rather than the results of processing.

In some instances, reperformance might not be the most effective test. For example, the best evidence that control owners are comparing batch control totals to batch validation reports may be the inspection of a log that documents the results of the comparison plus observation of the person preparing the log. If this is a key control, reperformance of the process could miss the control entirely. Reperforming steps of processes and controls based on a selection of transactions recorded on the books is not a test of completeness. To test completeness, it is necessary to move upstream to apply inspection, observation and inquiry techniques to test controls at the point of entry, during processing, at interface or handoff points (if any), and over correction and re-entry of errors.

### **125. 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 second or third quarter, if possible, so that the external auditor is able to begin his or her review. An update is then performed through the end of the year. See Question 144 for further discussion regarding the update of testing through year-end.

For subsequent years, testing of controls over routine processes may be performed uniformly throughout the year with an update performed through the end of the year. Controls over non-routine and estimation processes may be performed during the last half or, ideally, the last quarter of the year.

### **126. 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 85) and at the activity or process level, and where and how those controls are documented
- The testing standards and sampling methodologies for each area, including population size, the significance of the population, desired confidence levels, the accuracy required of sample results and other key population characteristics
- The process for reporting exceptions and the criteria for evaluating them
- The actions to take when failure conditions occur, i.e., when a control fails to pass a test
- The person or persons responsible for performing tests of controls
- The frequency with which tests are to be done (which often will mirror the operating frequency of the control, 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 should approve the plan. Once the plan is finalized and approved, it should be reviewed with the external auditor to obtain any input he or she may have and to reduce the risk of surprises arising from disagreement over testing approaches, scopes and sample sizes, as well as resolution of exceptions, 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
<b>Self-Assessment</b>	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 key documents
<b>Monitoring</b>	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
<b>Testing – Pervasive Process Controls</b>	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	
<b>Testing – Information Process Controls</b>	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 119 (i.e., self-assessment, monitoring and testing).

The steps in developing a testing plan are as follows:

- **Determine testing objectives** – Tests of controls provide evidence about whether controls over financial reporting are operating effectively. For example, to determine that disbursements have been properly authorized, tests of controls may be designed to enable the evaluator to examine a sample of payment vouchers to assess whether authorized company personnel signed the payment voucher before processing. Thus the objective of testing is to answer two questions:
  - Did the controls perform as designed?
  - Did authorized and competent people execute the controls?

The testing plan should take these objectives into account.

- **Consider the antifraud program and controls** – The testing plan should address testing of the company’s antifraud program and controls, as defined and documented. The plan should focus on fraud when validating the company-level controls, when testing controls over the financial reporting process and when testing controls mitigating assertion risks at the process level.
- **Define the failure conditions** – Defining what constitutes a “control failure” up front for each control tested before beginning testing is an effective way for management to direct the testing effort. A “failure condition” in testing is a departure from “acceptable” or “effective” performance of the prescribed control activity. For example, a failure condition may be defined as an error rate in the sample that management is unwilling to accept because it exceeds management’s maximum tolerable error rate (the upper error limit, or UEL). Said another way, a failure condition is an error rate that exceeds an acceptable level. The PCAOB recognizes this concept in Auditing Standard No. 2, which states, “... a control with an observed non-negligible deviation rate is a deficiency.” See Question 127 for further discussion.
- **Define the population** – In financial reporting, the “population” consists of all of the items constituting an account balance or a class of transactions subject to testing. It is important to articulate the characteristics of the population from which a sample is to be selected in a manner that can be related to specific control objectives. To accomplish this task, the testing plan developer should specify the target population as clearly and completely as possible. For example, if the evaluator tests a control designed to ensure all shipments are billed, the appropriate population is the shipped items, not the billed items. In controls testing, the population is also affected by the number of times a particular control is performed. For example, the population is defined by the frequency with which the control is executed – recurring, daily, weekly, monthly, quarterly and annually. The population is also defined by the number of individuals executing a control operation. Therefore, if the same control operation is executed by 10 people on a weekly basis, the testing plan developer must consider a population size of 520 operations when determining the required sample size.
- **Ascertain the test period** – In ascertaining the test period, the Section 404 compliance team must address the question of whether to apply tests of controls to (1) transactions executed throughout the period (e.g., the entire year), OR (2) during the period from the beginning of the year to an interim date, OR (3) primarily close to or at the end of the year. The answer to this question depends on management’s risk assessment, as risks relating to period-end transactions and journal entries are quite different from risks associated with routine transactions processed every day. The answer is also affected by the frequency of the control, i.e., whether the control is performed continuously (recurring), daily, weekly, monthly, quarterly or annually. See Question 128 for further discussion.
- **Define the sampling unit** – The *sampling unit* is the item to be tested. It constitutes one item in the population, such as a document, an entry or a line item. For example, if the testing objective is to determine whether disbursements have been authorized and the prescribed control activity requires a duly authorized voucher before processing, the sampling unit might be defined as the voucher. While the point about the sampling unit is somewhat elementary, it must be remembered when developing a testing plan that many types of controls do not involve selecting a sample from a population. For example, in some instances, the sampling plan must stipulate the domain where the controls can be observed, e.g., safeguard controls, segregation of duties, etc. The plan may set forth the frequency (daily, weekly, monthly, etc.) with which a particular control is executed, e.g., comparisons, reconciliations, etc. In such instances, the sampling unit may be a completed reconciliation meeting certain pre-defined criteria.
- **Select testing method(s)** – There are four basic testing methods – inquiry, observation, inspection and reperformance. Evidence is more reliable when *consistent evidence* is obtained from a *combination of procedures*. See Question 129 for further discussion.
- **Determine sampling method** – Sampling is divided into two categories – *judgmental* and *statistical*. When choosing the sampling methodology and determining sample size, the process owners and Section 404 compliance team leads should consider the following:

- The level of understanding that management and process owners have of the underlying process and the extent of errors in executing the specific control during the process
- The criticality of the business process(es) that feed the priority financial reporting elements
- The extent of reliance on self-assessment and company-level monitoring
- The nature of the control process and the underlying transaction data addressed within the control process

See Questions 130, 131 and 132 for further discussion.

- **Determine sample size** – Ultimately, the task falls to management to optimize selected sample sizes against the risk of missing a significant deficiency or material weakness that the external auditor might later detect. Management retains the ultimate responsibility to decide the sufficiency of testing for its purposes in supporting the assertions in the internal control report. When deciding sample sizes, there are certain factors management should consider. These are discussed in Question 133.
- **Finalize formal testing plan** – The testing plan articulates the rules of engagement before testing begins. Through the testing plan, management defines the nature of the internal controls that will be tested at the entity level and at the activity/process level, and where and how those controls are documented. The plan references the separate documentation of financial reporting elements, assertions and risks to provide the proper context. The test plan also addresses the testing approaches, scopes and sample sizes that are required to support the assertions in the internal control report, and sets forth the actions to take should a test indicate a control is not operating effectively.
- **Approve testing plan** – Management approves the testing plan.

Once the testing plan is completed, management should review it with the external auditor.

### 127. Why is it important to define the failure conditions before beginning testing?

As noted in Question 126, a “failure condition” in testing is a departure from “acceptable” or “effective” performance of the prescribed control activity. For example, a failure condition may be defined as an error rate in the sample that management is unwilling to accept because it exceeds management’s maximum tolerable error rate (UEL). In other words, a failure condition is an error rate that exceeds an acceptable level.

Defining what constitutes a “control failure” up front for each control tested before beginning testing is an effective way for management to direct the testing effort. A “failure condition” in testing is a departure from “acceptable” or “effective” performance of the prescribed control activity. For example, a failure condition may be defined as an error rate in the sample that management is unwilling to accept because it exceeds management’s maximum tolerable error rate (the upper error limit, or UEL). The PCAOB has recognized this concept in Auditing Standard No. 2, stating, “... a control with an observed non-negligible deviation rate is a deficiency.”

“Failure conditions” are NOT limited to the rate of error within a population. There are many other controls that must be tested that do not involve selecting a sample from a population, including segregation of duties, control environment attributes, physical safeguards, reconciliations, comparisons, and accounting for numerical sequence and completeness. These controls are often tested through inquiry and observation, and reconciliations can be reperformed. The failure condition relates to whether the controls actually exist as intended (e.g., physical safeguards) or are actually performed as intended (e.g., reconciliations and comparisons). Therefore, in addition to defining a failure condition using error rates, a failure condition may be defined qualitatively in terms of specific conditions. For example, management may designate certain conditions noted during testing that lead the evaluator to conclude that the “reasonable assurance” standard is not achieved. Examples of such “conditions” include:

- Failure to follow up on an exception noted during the company’s process
- The absence of critical matters (such as fraud) covered in audit committee meeting minutes

- The lack of evidence of effective communication and reinforcement of the company’s code of ethics
- The lack of expected physical safeguards
- Gratuitous comments from employees regarding pressure to change reported results or other evidence of management override

In summary, the test plan developer must make a precise statement of what constitutes a “failure condition” so the individuals performing the testing procedures have specific guidelines for identifying deviations from adequate or expected performance. If failure conditions are not pre-defined, the individuals performing the testing procedures will make up the rules as they go, leading to errors in judgment, decisions to retest when remediation is more appropriate, and constant second-guessing by the external auditors, all of which will lead to non-value-added activity. Defining the rules of engagement up front means, going forward, management, evaluators and auditors are all in agreement as to what will be done in specific situations. This is what an effective testing plan is about.

Another issue arising if the ground rules are not articulated up front is the risk evaluators will rationalize exceptions and conclude they do not represent deficiencies even though they really are deficiencies. In Auditing Standard No. 2, the PCAOB points out, “A conclusion that an identified exception does not represent a control deficiency is appropriate only if evidence beyond what the auditor had initially planned ... supports that conclusion.” Mere rationalization will not make exceptions go away.

To define failure conditions, take the following steps:

- (1) Start with the population characteristics or attributes that are to be tested.
- (2) Understand specifically “what can go wrong” with respect to the operation of the control.
- (3) Describe each specific example of “what can go wrong” in operation as an example of a “failure condition.”
- (4) Recognize in the test design that different failure conditions may require different tests, although use of the same sample may be appropriate.
- (5) Understand management’s acceptable error rate (the “planned” tolerable error) before beginning testing.
- (6) Include the planned tolerable error in management’s testing plan.
- (7) Include multiple conditions for “tests of one” when testing application controls.

For example, suppose a prescribed control requires every package supporting a disbursement to include the following: an invoice, a voucher, a receiving report and a purchase order, all stamped “paid.” If the existence of the invoice and receiving report stamped “paid” are necessary to indicate adequate performance of the control, then an exception may be defined as “a disbursement not supported by an invoice and a receiving report stamped ‘paid.’” Management must then define the tolerable error rate, which may be one error for every 200 disbursements. The test should be designed to compare the error rate noted in the sample to the tolerable error rate (.5 percent). If the tolerable error is exceeded, a “failure condition” results. If a small sample is selected, this could mean that one exception would cause the test to fail.

The absence of “failure conditions” noted during testing (i.e., in effect, an error rate below the tolerable error) supports a conclusion of “adequate performance.”

#### **128. How does the evaluation team ascertain the test period?**

As noted in Question 126, the Section 404 compliance team must address the question of whether to apply tests of controls to (1) transactions executed throughout the period (e.g., the entire year), OR (2) during the period from the beginning of the year to an interim date, OR (3) primarily close to or at the end of the year.

In theory, because Section 404 requires a point-in-time assessment as of year-end, some may ask whether management can wait until the end of the year to test. From a practical standpoint, it is recommended to differentiate controls over routine processes from controls over non-routine and estimation processes by testing the former over the course of the year and testing the latter closer to the end of the year. This strategy provides management the flexibility to remediate control deficiencies prior to year-end in sufficient time to retest the remediated controls to ensure they are operating effectively. It also reduces the risk of surprises. Further, the auditor needs sufficient time to perform the attest work.

There are other reasons to spread out the testing work. The Section 302 certification process is a quarterly reporting process. Internal control over financial reporting is a subset of the disclosure controls and procedures certified by the CEO and CFO every quarter. Testing on an interim basis may identify areas to remediate more timely than waiting until the last quarter to do the work. Spreading the testing out over time also is more efficient and avoids a year-end “spike.”

A choice to deploy interim testing requires consideration as to the nature, timing and extent of refresh testing necessary to update preliminary evaluations and determine operating effectiveness “as of” the end of the fiscal year. Testing performed earlier in the fiscal year will require more extensive updating closer to the end of the fiscal year. If testing covers an interim period, the evaluator must determine what additional evidence needs to be obtained for the remaining period. Factors to consider when determining the nature, timing and extent of refresh testing include:

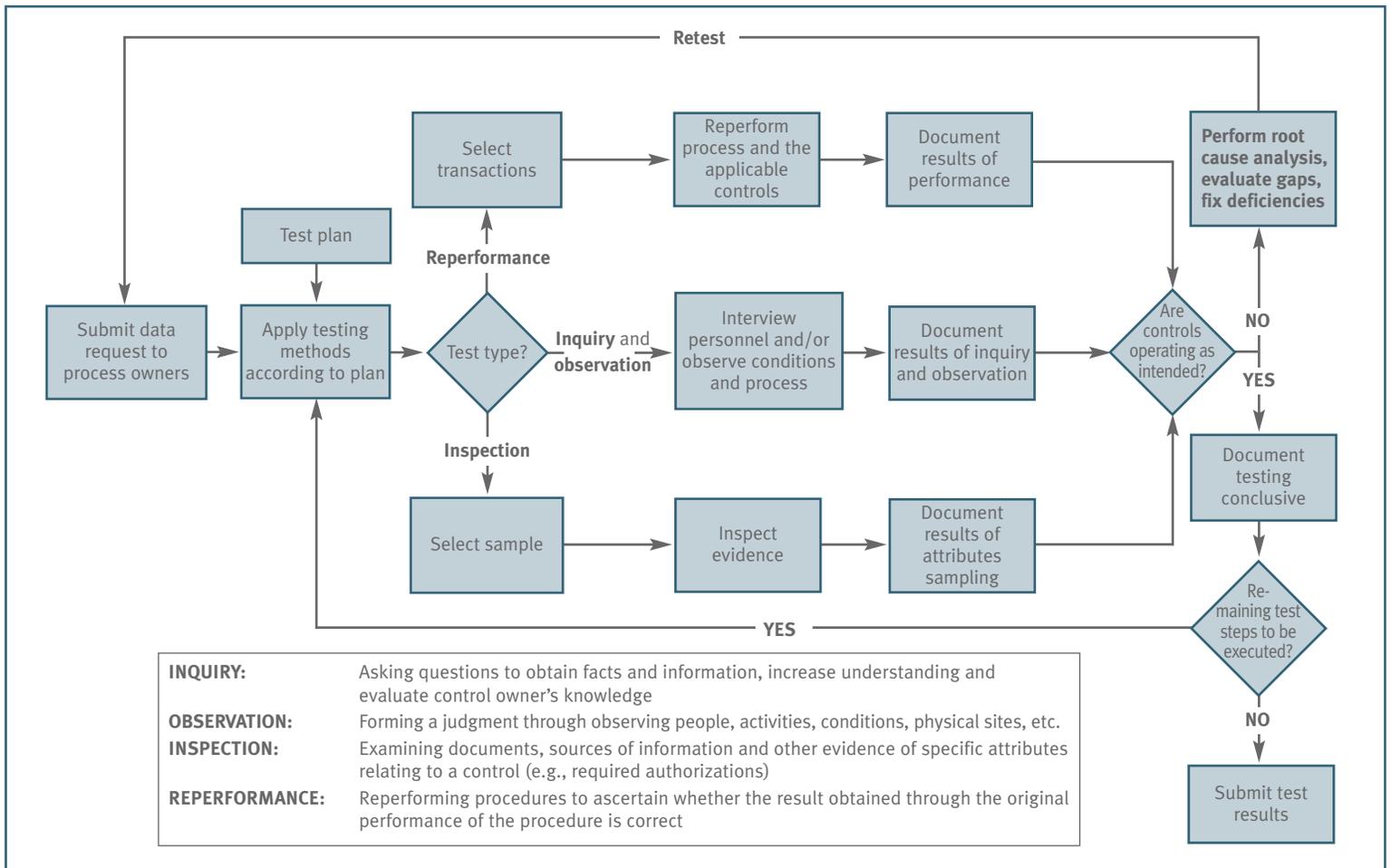
- The significance of the risk to the assertion involved
- The significance of the risk(s) mitigated by the specific controls tested prior to the “as of” date
- The results of the tests performed during the interim period
- The length of the remaining period between the interim period-end and the end of the year (generally should be no more than six months)
- Any changes in controls since the interim testing period

With respect to controls over pervasive, non-routine and estimation areas, because of the nature of these areas and the underlying risks, management should consider the need to perform tests of controls closer to the “as of” date. Examples include:

- Controls over significant non-routine transactions
- Controls over accounts or classes of transactions with a high degree of subjectivity or judgment in measurement
- Pervasive controls such as IT general controls or controls over the recording of period-end adjustments

#### **129. How does management select testing method(s) to apply in specific circumstances?**

There are four basic testing methods – inquiry, observation, inspection and reperformance. Following is an example as to how the four methods are applied.



*Inquiry* can be an effective way to corroborate or follow up on evidence gained through the other testing methods. When using inquiry, evaluators should ask open-ended questions, such as “can you tell me what you do?”, “how is this done?” and “can you walk me through it?” When using inquiry, evaluators should avoid leading questions that tip the answer, listen carefully, watch for non-verbal cues and apply professional skepticism. The PCAOB provides examples in Auditing Standard No. 2 of information that responses to inquiries might provide:

- The skill and competency of those individuals performing the control
- The relative sensitivity of the control to prevent or detect errors or fraud
- The frequency with which the control operates to prevent or detect errors or fraud
- Whether there have been instances of management override with respect to established controls

Effective inquiries lead to further inquiries and to subsequent inspection and observation techniques. Such combination of techniques facilitates testing of control over identifying, correcting and re-entering exceptions. Inquiries are also invaluable during a “talkthrough” with process owners, particularly when combined with effective listening and focus on non-verbal cues. That all said, inquiry, by itself, is inadequate to support management’s assessment. Used effectively, inquiry adds considerable insight as a testing technique.

*Reperformance* is a higher level of evidence than inquiry. It involves selecting transactions and reperforming the transaction, including reapplication of management’s authorization, recording, processing and reporting

criteria. The reperformed or recalculated transaction is compared to the reported result. If they agree, there is a presumption that the controls along the process operated effectively.

**Inspection** is another high level of evidence. For example, sampling for attributes can provide compelling evidence that controls over routine transactions are performing as intended. However, inspection must be used with care. A signature on a voucher is not, in and of itself, persuasive evidence of a careful review of a voucher package before signing. Therefore, inspection of the voucher might not be enough and reperformance of the control (checking prices, extensions and additions) may be necessary.

**Observation** is an effective technique for testing such controls as physical safeguards and segregation of duties as well as noting specific individuals in action as they execute documented control activities.

In summary, evidence is more reliable when *consistent evidence* is obtained from a *combination of procedures*. When developing a testing plan, the evaluation team needs to consider these points. For anyone who wishes to understand the interaction of the various testing techniques, the PCAOB examples in Appendix B of Auditing Standard No. 2 are required reading.

### 130. How does management determine the appropriate sampling method?

As defined by the AICPA Sampling Guide, sampling is “the application of a testing procedure to less than 100 percent of the items within a ... class of transactions for the purpose of evaluating some characteristic of ... the class.” Under Section 404, the context of this definition is reaching a conclusion with respect to the operating effectiveness of internal control over financial reporting. As further explained in Question 142, the key attributes of a control (e.g., manual versus system; frequency of operation; preventive versus detective; routine versus non-routine) have implications from a risk standpoint and assist the Section 404 compliance team in determining the nature, extent and timing of testing required to evaluate that control. For example, company-level controls generally require more emphasis on inquiry and observation. Controls that are manual in nature generally may require more extensive testing, i.e., higher sample sizes, than systems-based controls. The type of underlying transaction subject to a control (either a routine transaction or non-routine transaction) can also affect the nature, extent and timing of testing.

Sampling is an important aspect to tests of controls because it affects the number of items selected for testing as well as the selection process. It is not necessary to test every single instance in which a control is applied. It is only necessary to test the controls to such an extent that management is satisfied the results of the test provide conclusive evidence to support the assertion that the control is operating effectively. This conclusion need not be reached in isolation. The results of testing may be considered in light of other sources of evidence regarding operating effectiveness, including positive self-assessments received from process owners, the results of entity-level monitoring and the effectiveness of compensating controls (see Question 107).

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

Sampling is divided into two categories – judgmental and statistical. When choosing the sampling methodology and determining sample size, the process owners and Section 404 compliance team leads should consider the following:

- The level of understanding that management and process owners have of the underlying process and the extent of exceptions in the population when the specific control is executed (the greater this understanding, the smaller the sample)
- The criticality of the business process(es) that feed the priority financial reporting elements (the more critical the process, the more important the controls; the more important the controls, the more evidence is needed through testing to provide reasonable assurance they are operating effectively)
- The extent of reliance on self-assessment and company-level monitoring (the greater the reliance on these sources of evidence, the less evidence is needed through testing to provide reasonable assurance the controls are operating effectively)
- The nature of the control process and the underlying transaction data addressed within the control process (e.g., if the control is addressing a process involving unique pre-numbered documents or transaction identifiers, such as invoices or receiving reports, then statistically valid samples and conclusions can be effectively applied)

See Questions 131 and 132 for discussion of judgmental and statistical sampling.

### **131. How is judgmental sampling applied?**

As discussed in Question 130, *judgmental* sampling is one of the methods of sampling. This sampling approach involves the use of judgment by management in determining sample sizes based upon the nature and significance of the control. When determining sample sizes and the extent of controls testing on a judgmental basis, management must exercise care. Judgmental sampling introduces bias, which leads to sampling risk. In deciding how many items to test, management must consider the risk that the conclusion that a control is operating effectively based on limited testing *may differ* from the conclusion it would have reached if it had tested all operations of the control. Therefore, it is especially risky to select small judgmental samples when there is an inadequate understanding of the process and the expected error rate, i.e., management and process owners don't know what to expect. In fact, the PCAOB staff has stated that nonstatistical samples should be used based on the expectation of “no, or very few, control testing exceptions.”

One of the limitations of judgmental sampling is that it is inappropriate to infer testing results using judgmental samples to the population. If the controls are critical to the achievement of the company's stated financial reporting assertions (and to the mitigation of risks to achieving those assertions) and oversight is limited to manual supervision, management should consider more extensive sample sizes and even statistically valid samples for testing purposes in order to formulate more compelling evidence. If there is a critical control relied on versus several compensating controls, then management should expect to test more items for that particular control. As a general rule, the more complex a manual control, the greater the number of items to test. If the frequency of application of manual controls is high (e.g., daily rather than monthly or annually), then as a general rule the testing plan should provide for testing more items. However, this is not suggesting a proportionate increase in scope. In Auditing Standard No. 2, the PCAOB states, “When sampling is appropriate and the population of controls to be tested is large, increasing the population size does not proportionately increase the required sample size.”

When selecting judgmental samples, management will need to consider samples to be used by the external auditor. With rare exceptions, in the absence of an effectively functioning self-assessment program AND effective entity-level monitoring and analytics, companies will probably be expected to test at least as many items as the auditor. However many items are selected for testing, the Section 404 compliance team should make sure the underlying “thought process” supporting its conclusions is documented and approved by management. It is also desirable to obtain feedback and, if obtainable, agreement from the external auditor.

### 132. How is statistical sampling applied?

As discussed in Question 130, *statistical* sampling is another method of sampling. This sampling technique uses statistics to (1) reduce sampling risk, which is the risk that the sample results are inconsistent with the actual characteristics of the population, and (2) infer results of the sample to the population. If statistical sampling is used, there are several factors to consider:

- The **expected error** is the level of variability (or control exceptions) management anticipates finding in the population.
- The **margin of error** is a measure of sampling error, i.e., it is a measure of the difference between the estimate from the sample and the true population value.
- The **confidence level** is the likelihood that the results obtained from the sample lie within the margin of error.
- The **Upper Error Limit (UEL)** is the maximum error rate management is willing to accept (i.e., the tolerable error).

Ideally, the margin of error at the stated level of confidence plus the expected error should be less than or no greater than the tolerable error rate (UEL). However, this is not always the case as management seeks to balance the cost of testing with the evidence gained from sampling.

Without getting into a technical discussion, statistical sampling involves moving parts. Management should consider holding confidence level constant at a high level, such as 95 percent, to enable more forceful conclusions. High confidence levels are also more appropriate for a critical application or control, particularly when there is an absence of a strong control environment, effective monitoring and other compensating controls. A lower confidence level (such as 90 percent) is often useful only when seeking an indication of the likely population characteristics. Lower confidence levels may be appropriate when a particular control activity functions within a strong control environment, i.e., there is evidence of strong company-level or monitoring controls, strong pervasive controls (including general IT controls) along with a comprehensive self-assessment approach.

These considerations ultimately are subject to evaluation by the external auditor and the policies his or her firm chooses to adopt.

When using statistical sampling, following is an illustrative process for determining sample size:

- For each type of control, management and the process owner defines the presumed expected error rate. This rate is the level of variability (or rate of control exceptions) management and the process owners anticipate to find in the population. The expected error rate should be based on factual assessments by management and the process owners who are knowledgeable of the process and the related control objectives, design and performance. This means that management and the process owners need to apply their knowledge of the process.
- Management defines the tolerable error for all control frequencies. The tolerable error is not the same as the true error rate. The goal is to determine, given a 95 percent confidence interval, whether there is a 95 percent chance that the “true” population error rate will not exceed the tolerable error rate management selects. Management’s tolerable error is sometimes described as the UEL.
- When applying sampling tables, sample sizes may vary for controls depending on the extent of management reliance. For example, a lower maximum tolerable error might be expected for controls on which management is placing a high degree of reliance for purposes of achieving a given financial reporting assertion. To illustrate, a 3 percent maximum tolerable error rate may be selected for lower reliance controls and a 2 percent or 1.5 percent rate for higher reliance critical controls. These choices influence sample size.

When determining sample size using statistical sampling, the Section 404 project team should involve appropriate quantitative expertise. One of the primary issues management faces in sampling is the risk that the project team will conclude through testing that controls are operating effectively and the external auditors will then perform their review (using a different sample and/or sample size) and detect a problem not found by the project team. Involving appropriate skills in applying and interpreting the statistics as well as in executing the tests of the sample will reduce sampling risk.

### **133. How does management determine sample size?**

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 104 introduces the Internal Controls Capability Maturity Continuum. When a company’s internal controls are at the “initial” (ad hoc) stage for a critical process, the company will often take steps to improve these controls so they are more repeating and better defined. In these circumstances, it is difficult to know for sure that the processes are “in control” without the use of statistical techniques to infer test results to the population with a reasonable level of confidence. Because these environments lack process definition and are often in a state of change, self-assessment techniques are not as effective and entity-level monitoring often doesn’t exist. These environments are often characterized by manual and detective controls.

The following guidance should be considered when validating the operating effectiveness of manual “detect and correct” controls:

- If these controls are critical to the achievement of stated financial reporting assertions and oversight is limited to manual supervision, management should consider more extensive sample sizes for testing purposes.
- With respect to testing controls requiring manual oversight or involvement: the more frequently a manual control operates and/or the more important the control, the more extensive the testing.
- If the frequency of application of the manual controls is high (e.g., hourly rather than monthly or annually), then as a general rule the 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 104), we often see the emergence of more preventive and systems-based controls. At this level of capability, self-assessment techniques are more effective and monitoring procedures are more likely to be in place, particularly at the “managed” stage. At these higher levels of capability, management may conclude that less comprehensive judgmental sampling techniques, such as representative sampling, might be appropriate. Further, given the additional sources of evidence as to operational effectiveness that are often available at these higher levels of capability, management may choose to test fewer items. The following guidance should be considered:

- The compliance team should test more extensively the controls that support the effectiveness of other controls in these environments (i.e., controls on which other controls depend). This includes selected attributes of the control environment and specific IT general controls processes, such as security administration and change management. Tests of IT general controls ensure the continuous effective operation of automated and IT-dependent controls.
- Management should expect to test at least as many items as the external auditor typically would test. The SEC staff has commented at a conference: “It is hard to imagine that management could support its assertion with less testing than the auditor must undertake.”
- For an automated control, the number of items that should be tested is generally minimal (one to a few items) assuming IT general controls have been tested and found to be effective.

Thus management's testing plan is often influenced by the maturity of the company's controls, as illustrated using the Capability Maturity Continuum introduced in Question 104. Ultimately, management must balance the cost of higher sample sizes against the risk of missing a significant deficiency or material weakness that the external auditor later detects. As noted previously, management retains the ultimate responsibility to decide the sufficiency of testing. Because of the lack of clear criteria as to the number of items to test, input from the independent accountant should be obtained before commencing execution of the testing plan.

#### **134. How is the sample selected from the population?**

There are a variety of methods for selecting a sample. Regardless of the method used, it is important to select locations or business units in such a way that the sample is expected to be representative of the entire population. It is also important to select samples according to the testing plan. Sample biases can occur in many ways. For example, sample bias occurs when the number of items selected for the sample is too low, the time period for testing is insufficient in duration, the population targeted is biased in some way, or the items selected are chosen based on deliberate choice rather than through using a random process. Random selection guards against bias, so it should be used whenever possible. It is also important to check the quality of the information in the population from which the sample is drawn. If the quality is poor, sampling may not be justified.

Following are alternative selection methods:

***Unrestricted random numbers.*** This method, in which each item in the population has an equal chance of being selected, is very common. When it is used, the items in the population must be numbered or listed in a complete and accurate record.

***Intervals.*** In this method, there is a uniform interval between each item selected after a random start. It is applied when selecting items randomly is burdensome. It works fine when there isn't a pattern in the population that will bias the sample. If there are items missing in the population, they must be identified.

***Stratifications.*** The population is segregated into two or more classes, with each class sampled separately. This method is appropriate when there is considerable variation in the population and increased reliability in sampling results arises from breaking the population down into homogeneous groups of comparable items.

***Cluster and Multistage.*** When using the cluster method, the population is formed into groups and all items within selected groups are examined in their entirety. When using the multistage approach, sampling is applied to several levels, e.g., a sample is taken from several locations and another sample is taken from the sampled items. This approach is applied when random sampling is burdensome or not possible, because the population is dispersed geographically. Cluster sampling increases exposure to sampling error. Multistage sampling requires complex calculations.

#### **135. How does management finalize the formal testing plan?**

As we stated earlier, the testing plan articulates the rules of engagement before testing begins. There are several reasons why this is important:

- Management does not want evaluators "making it up as they go."
- Loosely defined testing plans open management up for "second guessing" by the external auditors when dealing with exceptions.
- Evaluators need to know when to (a) root cause exceptions, remediate processes and retest, versus (b) select an expanded sample size and retest.
- The issue of interim testing and year-end updates requires clarification.
- Process owners need guidance on supporting their self-assessments.

Through the testing plan, management defines the nature of the internal controls that will be tested at the entity level and at the activity/process level, and where and how those controls are documented. The plan should reference the separate documentation of financial reporting elements, assertions and risks to provide the proper context. The test plan addresses the testing approaches, scopes and sample sizes that are required to support the assertions in the internal control report. The plan also sets forth the actions to take should a test indicate a control is not operating effectively. Following is a summary of the key elements of a test plan:

**Validation approach** – Self-assessment, monitoring and/or testing

**Nature/Description of the test** – Describe nature of the control or transaction subject to validation and testing

**Applicable control significance** – Primary vs. secondary control

**Applicable control significance/type** – Manual control or system control; preventive control or detective control

**Frequency/Timing of the control/test** – Year-end; quarter-end; month-end; daily; or continuous

**Other elements of the testing plan** include:

- The person or persons responsible to perform tests of controls
- The frequency with which tests are to be performed (which often will mirror the operating frequency of the control, i.e., daily, weekly, monthly or annually)
- The parties to whom test results are reported
- The parties responsible for evaluating test results and reaching a conclusion as to operating effectiveness
- A description of the specific actions to take if a control fails
- The process for identifying gaps and undertaking remediation to close those gaps, including the individuals responsible
- The extent to which the plan addresses the components of COSO (assuming management uses the COSO framework)

### **136. How often must the testing plan be executed?**

Each year stands on its own. The PCAOB states that the evidence supporting the auditor's opinion must be supported each year and the auditor must test controls every year, regardless of whether the controls have changed. Thus *each* year the auditor must obtain evidence about the effectiveness of controls for *all* relevant assertions related to *all* significant accounts and disclosures in the financial statements. The Board summed up its view with the following statement:

Even if nothing else changed about the company – no changes in the business model, employees, organization, etc. – controls that were effective last year may not be effective this year due to error, complacency, distraction and other human conditions that result in the inherent limitations of internal control over financial reporting.

The same principle of providing sufficient evidence each year applies to management.

### **137. How are testing results documented?**

While there are no prescribed documentation requirements, the evaluator needs to know the nature of exceptions, their frequency and the way in which the process or control owner reconciles and documents their disposition. It

is also critical to establish the testing documentation protocols and obtain agreement with management and the external auditors. Simply covering format and columnar headings is not enough. Agreement is also necessary as to the level of detail when documenting the results of testing. One possible suggestion is to complete several tests as a “pilot” and invite the external auditor to critique the completed documentation as to sufficiency for his or her purposes during the attestation process. While there are no prescribed documentation requirements, the evaluator needs to document: the nature of testing procedures; the nature of exceptions, their frequency and the way in which the process or control owner reconciles and documents their disposition; and errors and deviations noted. Documentation must be sufficiently granular to facilitate “over-testing” by the external auditor.

Following are illustrative examples of documentation points to use when designing a form that facilitates the documentation process:

***Method of selecting the sample.*** Document the selection procedure used and how it was applied.

***Name and title of control owners interviewed.*** Document the results of inquiries of the “owner” of the control (the person who is accountable for its operation), including the questions asked (may be in the form of a template with questions and responses, including items inspected and observed as a result of the inquiry).

***Description of visual observations.*** Describe what was observed, e.g., “observed materials being counted in the receiving department, which was physically segregated from the remainder of the plant.”

***Identification of the control documents examined.*** Record sufficient information so the external accountant can retrieve the documents, if necessary, to reperform 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 either (a) the control owner doesn’t understand the control and is not performing it, or (b) the technique is merely a processing procedure and not really a control.

***Description of procedures for resolving exceptions.*** The evaluator should determine from the control owner how he or she corrects the errors and submits the corrected data back to processing.

***Document reperformance work.*** Describe the work performed in sufficient detail so that the external auditor can review and reperform the test.

***Summarize results of tests of judgmental samples.*** For judgmental samples, it is inappropriate to make an inference to the population as a whole. The evaluator may state: “We tested N items and noted Y exceptions.” Alternatively, the evaluator may state: “We tested N items and noted Y exceptions and that the error rate in the items selected is less than management’s stated tolerable error.”

***Summarize results of tests of statistical samples.*** For statistical samples, the evaluator should exercise care to prepare the summary of testing results consistent with the design of the sample and interpret the sample results consistent with the underlying statistics. It is often key to involve appropriate quantitative expertise to properly frame the summary of results in a statistically valid manner.

***An assessment of operating effectiveness.*** The evaluator must conclude as to whether the control is operating effectively.

### **138. How are testing results evaluated?**

The results of each test must be evaluated separately. If there are “failure conditions,” it is important to understand why these conditions exist. These conditions could require remediation and retesting. Alternatively, they could require expansion of sample size. However, sample size should be expanded only when the testing plan requires it and satisfactory results are expected; otherwise the retesting is a waste of time. When evaluating sample results, remember that exceptions taint the use of small judgmental samples.

When exceptions to or deviations from the control design occur, the evaluator should understand the reasons for the exception or deviation. The evaluator should collaborate with the process owner to consider whether:

- The error rate noted in the sample exceeds the predefined acceptable error rate planned for the test (i.e., management’s tolerable error).
- An exception noted for a small judgmental sample is potentially a problem.
- The identified error(s) is(are) inadvertent or intentional.
- The control is automated (in the presence of effective general IT controls, there is a presumption that an automated application control will always perform as designed).
- A failure of an automated control requires input from a technology expert to understand the implications.
- The degree of intervention by process personnel contributes to the exception or deviation.
- Management became aware of the exception or deviation on a timely basis.
- Management responds to the exception or deviation on a timely basis (if management was aware of it).
- The root cause of the exception or deviation is understood.
- Remediation is necessary.

When analyzing the test results, the evaluator must apply the definition of “failure conditions,” as set forth in the testing plan. It is important that the testing plan describe what evaluators are supposed to do when a “failure condition” is noted. For example, evaluators should understand the following:

- What constitutes effective and ineffective control operating performance, e.g., the evaluator should understand whether risks to achieving stated assertions are mitigated, whether stated assertions are achieved, the quantitative standard (tolerable error) and the qualitative standard (“reasonable assurance”).
- The sampling approach used and the nature of errors identified. Proper interpretation of testing results is key.
- Implications of control failures to the management assertion of “effective control operation,” the need for remediation and the need for additional testing.
- Approach to communicating and remediating control deficiencies.

A “failure condition” that cannot be remediated and tested in time prior to the “as of” date constitutes a control deficiency. Management should review control deficiencies and formulate a conclusion as to their severity. There will be times when the results of testing aren’t clear. In such situations, judgment is necessary.

All controls deemed compliant with the stated design should be assessed as “effective,” i.e., controls provide “reasonable assurance” that risks to achieving stated assertions are mitigated and stated assertions are achieved. For any controls deemed to not be in compliance with the stated design (i.e., a failure condition), the evaluator should consider:

- The nature of the failure, i.e., is it due to a poorly designed control (a design deficiency not detected during the earlier evaluation of design effectiveness)? Is it due to a properly designed control not operating as designed? Or is it due to the person performing the control not possessing the necessary authority or qualifications to perform the control effectively?
- The existence of compensating controls (and the need for additional testing of those controls). See Question 107.
- Qualitative factors, e.g., whether management override occurred.

When the evaluator observes a “non-negligible deviation” when testing control performance and there is not an adequate explanation, it should generally be concluded that the control is “ineffective.” The circumstances will be rare where a conclusion is reached that a control is operating effectively when there is a “greater than insignificant” error rate. Our expectation is that the external auditor is likely to concur rarely, if ever, with a conclusion on effectiveness in situations where there are a significant number of errors. For each ineffective control, an action plan should be developed to remediate the weakness as soon as practicable. The remediation plan should allow sufficient time for validation by management and the external auditor prior to year-end.

The overall responsibility for assessment of control effectiveness ultimately lies with management personnel, who must be satisfied that the testing approach, scope and sample size used in testing a control are sufficient to support a conclusion that the control is operating as intended. Management should evaluate the testing results evaluators report. Management is responsible for deciding what to do to correct control deficiencies.

### **139. 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.

Filtering is important because it narrows down the population of controls to the ones that matter, making the linkage of individual controls with the significant accounts and assertions to which they relate, as required by paragraph 84 of PCAOB Auditing Standard No. 2, a more manageable task. Filtering also increases the efficiency of testing, because without a systematic approach to filtering, companies will be testing more controls than necessary. In fact, the sheer volume of controls to test may influence management to select smaller sample sizes than may be appropriate in the circumstances. If more controls than necessary are being tested, significant non-value added activity may be driven off of the need to understand the reason for exceptions for controls that aren’t really important. If evaluation teams rationalize away testing results on the basis that the control wasn’t really important in the first place, there wasn’t adequate filtering.

As noted above, we are only concerned with the controls over significant processes affecting financial reporting. One way to filter controls is to classify the documented controls as primary, secondary and tertiary (see Question 142 for further discussion of these labels of control importance) and focus most of the testing on the primary controls, with some testing of the secondary controls.

Often, an overwhelming number of primary or “key” controls are identified during the documentation process. In such instances, the “primary” controls may be further segregated as “critical” or “significant.” The idea is to narrow down management’s detailed testing to all critical controls as well as selected significant controls. Sample sizes can be larger and test results more reliable when testing is focused. In this approach, “critical controls” are defined as follows:

The FIRST subset of primary controls, these controls have a pervasive impact on financial reporting (segregation of duties, system and data access, change controls, physical safeguards, authorizations, input controls, reconciliations, review process, etc.) and have the most direct impact on achieving financial statement assertions. Upon failure of a critical control, the risk of occurrence of an undesired activity would not be mitigated regardless of other controls identified within ANY process. Failure of critical controls would affect the ability of management to achieve not only process objectives, but also the company’s financial statement objectives.

“Significant controls” are defined as follows:

The SECOND subset of key controls, significant reliance is placed upon the effective design and operation of these controls. Upon failure of a significant control, the risk of occurrence of an undesired activity would not be mitigated regardless of other controls identified within the process; however, other “critical” controls may exist in other processes to mitigate the risk of occurrence of an undesired activity.

There may be primary controls that, by definition, are neither critical nor significant. These remaining primary controls provide assurance regarding the achievement of certain objectives as well as mitigate the risk of an unanticipated outcome within a process. However, failure of such controls does not preclude the process from achieving its financial statement objectives. These controls include supplementary financial controls and operational controls.

When identifying primary controls, it is vital to consider areas where financial reporting errors or fraud could occur. This is the crux of the matter, as everything else is secondary. Identification of secondary controls may be important if primary controls are not effective.

There may be more than one primary control per risk. One control might address several risks, which increases its importance. As the importance of a financial reporting element increases, the importance of testing compensating controls increases.

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 85 for a discussion of validating controls at the entity level, including the approach to deciding which controls to validate.

In summary, 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 primary or 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. Controls at the process level are dependent on the control environment and general IT controls. For example, the extent of reliance upon a key report used as part of an important reconciliation 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. For another example, when monitoring controls are relied upon, it is important to evaluate the IT processes generating the information that makes effective monitoring possible.
- Controls that address each component of internal control. If management decides to use the COSO Internal Control – Integrated Framework, testing must be directed to address adequately each of the five components of COSO – control environment, risk assessment, control activities, information/communication and monitoring.
- Controls that have the most direct impact on mitigating a risk and achieving an assertion that the company is controlling the flow of 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.

- Primary or 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 competence and performance of an individual may be more prone to breakdowns and error
  - Whether there have been changes in the volume or nature of transactions that might affect controls design or operating effectiveness
  - Whether there have been changes in processes, key personnel, systems or other factors that may affect the performance of internal control
  - Whether there have been changes to controls design
  - The degree to which the control relies on the effectiveness of other controls, e.g., the control environment
- 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.

Other factors to consider when identifying primary controls include:

- Proximity of controls to the points within processes at which errors or fraud could occur
- Significance of each control in achieving the relevant financial reporting assertions or control objectives (including whether more than one control achieves a particular assertion or objective or whether more than one control is necessary to achieve a particular assertion or objective)
- The reliability of the tests required to evaluate operating effectiveness
- The risk that the controls might not be operating effectively, as influenced by the complexity of the control and whether:
  - the control is automated or manual;
  - there have been changes in the volume or nature of transactions that might adversely affect control design or operating effectiveness;
  - there have been changes in the design of controls; or
  - there have been changes in key personnel who perform the control or monitor its performance.

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 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.

#### **140. How does management decide the extent of testing?**

When determining how many items to test for a particular control, the underlying thought process is risk-based. In Auditing Standard No. 2, the PCAOB provides three factors when assessing the extent of testing – the nature of the control, the frequency of the control and the importance of the control.

With respect to the *nature of the control*, the auditor should subject manual controls to more extensive testing than automated controls. Manual controls must be tested multiple times whereas automated controls need only be tested once or a few times, provided the general IT controls are operating effectively. Further, as the complexity of a control and the level of judgment required to operate it increase, the extent of testing must increase. As the competence of the person performing the control decreases, the extent of testing increases.

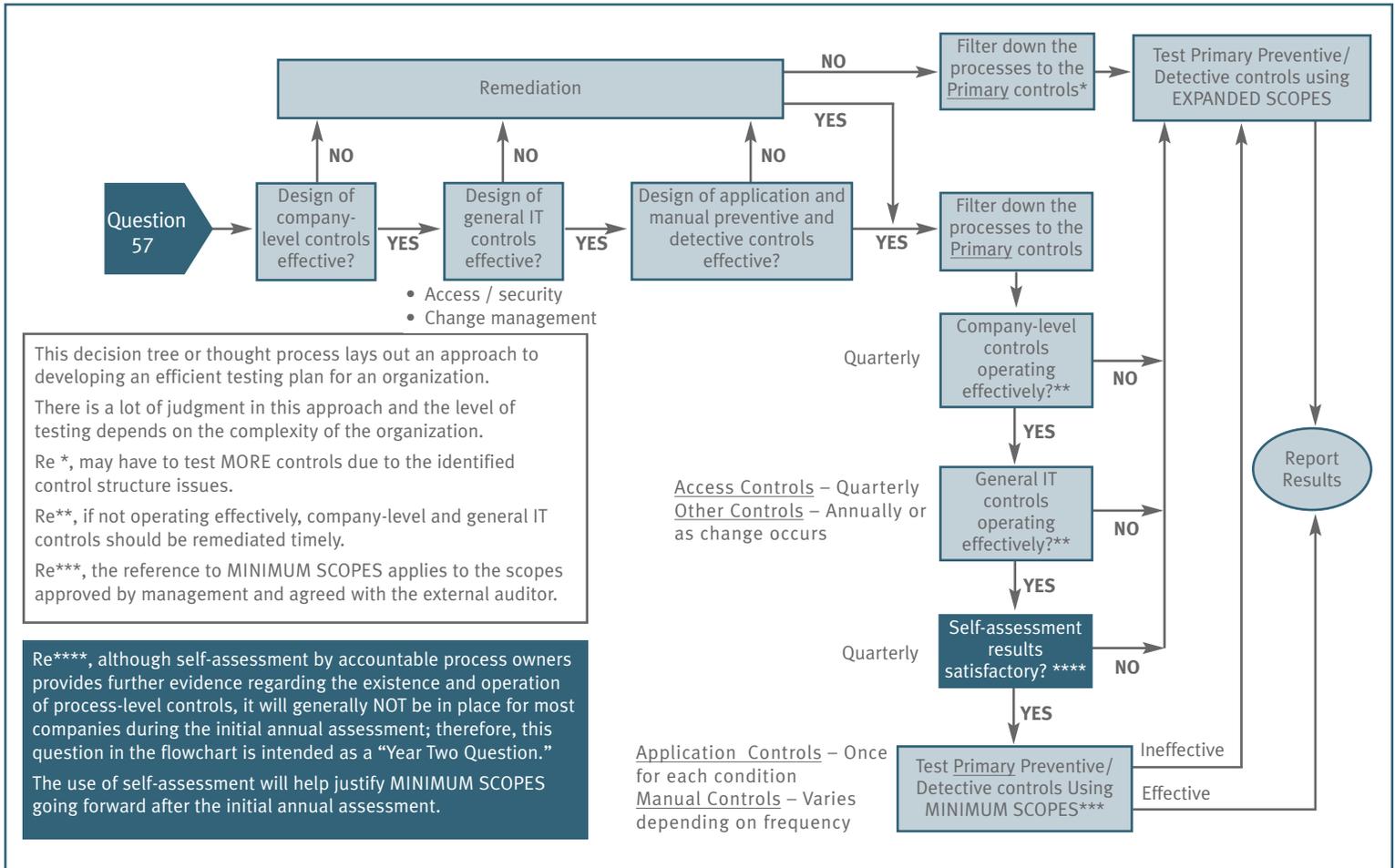
With respect to *frequency of operation*, the more frequently a manual control is performed, the more operations of that control the auditor should test. The Board points out that if a manual control is performed continuously (i.e., each time a transaction occurs), the auditor should test multiple operations of the control over a sufficient period of time to obtain “a high level of assurance” the control is operating effectively. As the frequency of operation declines, the auditor may test significantly fewer operations of the control. For example, this would be the case with monthly account reconciliations and controls over the period-end financial reporting process. However, in these instances the evaluation of each operation may be more extensive, as with the evaluation of the judgment applied in disposing of exceptions. The major audit firms have adopted minimum testing scopes based upon the frequency of operation, e.g., continuous, daily, weekly, monthly, quarterly and annually.

As the Board points out, increasing or decreasing the population size does not disproportionately increase or decrease the necessary sample size. This is a matter of statistics.

With respect to the *importance of the control*, controls that are relatively more important (i.e., the critical controls, as discussed in Question 139) should be tested more extensively. For example, controls addressing multiple financial statement assertions may be more important than controls addressing a single assertion. Certain period-end detective controls might be more important than related preventive controls. If a control is so critical it is the only control addressing a particular assertion, the scope of testing must be increased for that control.

The Board’s approach is risk-based and top-down. The company should generally FIRST assess entity-level controls, THEN assess IT general controls, and THEN assess the preventive/detective controls at the process level using the established testing guidelines set forth in the testing plan.

The following schematic completes the illustrative thought process begun in the response to Question 57 which identified the high- to medium-risk processes impacting the priority financial reporting elements. If entity-level controls (see Questions 85 and 86), including monitoring, are ineffective, it will result in a testing scope increase. If there is a weak company-level control environment that can’t be remediated timely, more testing will be needed at the process level and, depending on the facts and circumstances, at otherwise individually insignificant locations and units. If the company can remediate deficiencies in company-level controls timely, it may stick to the established testing guidelines, as set forth in the testing plan.



General IT controls are those underlying security administration and change management controls on which other process-level controls depend (see Question 87). If these IT controls are ineffective, there could be instances where management might be unable to go beyond this point and aggressive remediation might be required. Management should validate effective operation of these controls as soon as possible after concluding on design and be prepared for the question, “What is your evidence supporting your conclusion that the general IT controls are operating effectively?” If there are deficiencies in change controls and security that can’t be remediated, more testing will be needed at the process level. These deficiencies could also result in a “hard stop” if significant, e.g., the environment is highly automated and processes a significant volume of transactions.

At the process level, it is presumed testing would address a mix of preventive and detective controls. A control structure that is 100 percent detective is not an appropriate control structure and will raise issues from a sustainability standpoint when significant changes in the business occur. At the process level, the company must filter the controls by identifying those controls that are critical and significant, and determine how to test them in the most efficient manner (see Question 139 for a discussion of filtering).

If there are unacceptable testing exceptions, management must investigate the root causes and, in many cases, will need to redesign the control. The redesigned controls are then retested. An alternative is to not do a root cause analysis and test the control again using an expanded scope. If testing is expanded and more errors are found, the control clearly will require remediation. Management will need to find the cause of the error, fix it and retest the new control(s).

#### 141. 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 in a timely manner. To simply refer to a control without identifying the person or group responsible for the control or understanding how the control addresses errors 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: The marketing department reviews an IT-generated “was-is” list and changes are reconciled to the price change authorization signed by the VP of marketing. If a price change – either an increase or a decrease – was not input to the master price list on a timely basis, such changes are subsequently billed/credited to the customer.

#### 142. How should the Section 404 compliance team classify individual control techniques so that the team, as well as the independent auditor, can more effectively plan the required tests of controls?

There are several ways Section 404 compliance teams can classify individual control techniques to facilitate evaluation of controls design effectiveness and testing of controls operating effectiveness. These are identified below:

**Manual vs. System-based controls** – *Manual controls* predominantly depend upon the manual execution by one or more individuals, whereas *automated controls* predominantly rely upon programmed applications or IT systems to execute a step or perhaps prevent a transaction from occurring without human interaction. There are also *system-dependent manual controls*, e.g., controls that are manual (comparing one thing to another) but what is being compared is system-generated and not independently collaborated; therefore, the manual control is dependent on the reliability of system processing.

Why: Manual controls require more time and effort to test than automated controls. A control structure built on manual controls is not sustainable under stress and change conditions. As transaction volumes increase and with increasingly complex calculations, systems-based controls are often more reliable than people-based controls because they are less prone to mistakes than human beings, *if designed, operated, maintained and secured effectively.*

**Preventive vs. Detective controls** – *Preventive controls*, either people-based or systems-based, are designed to prevent errors or omissions from occurring and are generally positioned at the source of the risk within a business process. *Detective controls* are processes, either people-based or systems-based, that are designed to detect and correct an error (or fraud) or an omission within a timely manner to ensure achievement of a stated objective (e.g., begin the next transaction processing cycle, close the books, prepare final financial reports, etc.).

Why: An effective control structure is built on a mix of preventive and detective controls. A control structure built on detective controls is not sustainable under stress and change conditions. A shift toward an anticipatory, proactive approach to controlling risk requires greater use of preventive controls than the reactive “find and fix” approach embodied in a detective control.

**Relevant COSO element** – Controls can be classified according to the five COSO elements, as described in Question 42.

Why: It is desirable to address all five components of the COSO framework. Because most control techniques at the process level are classified as either “control activities” or “monitoring,” it is acceptable to address the other three components using an overall memorandum in lieu of a risk and control matrix.

**Control frequency** – Controls may be classified according to frequency of application, e.g., continuous, daily, weekly, monthly, quarterly, annually.

Why: Testing scopes vary according to the frequency by which the control technique is applied.

**Control importance** – Controls may be classified as primary, secondary and tertiary. These are defined below:

- *Primary controls* are activities or tasks performed by management or other personnel 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; these are the controls that managers and process owners primarily rely on. Primary controls provide reasonable assurance regarding the achievement of certain objectives, as well as reduce the risk of an unanticipated outcome to an acceptable level. Significant reliance is placed upon this control’s effective design and operation.
- *Secondary controls* are documented controls that contribute to the mitigation of risk and the ultimate achievement of one or more financial reporting assertions, but are not considered as important as primary controls by management and process owners; while these controls are significant, there are compensating controls that also assist in achieving the assertions.
- *Tertiary controls* are other documented controls that are neither primary nor secondary, i.e., they are not particularly important to the mitigation of risk and the achievement of financial reporting assertions. Therefore, management and process owners do not place reliance on them.

Application of the above definitions is illustrated in Question 139.

Why: Companies often test too many controls and, therefore, there is undue emphasis on selecting small sample sizes. There is not enough emphasis on filtering down the documented controls to the vital critical or significant controls that need to be tested to enable more thorough testing of fewer controls. Filtering the population of controls down to the vital few that matter is critical to evaluating controls design effectiveness and efficient testing of controls operating effectiveness. For example, the focus of testing should be directed to the primary controls, particularly if the primary controls are so critical there are no compensating controls should the primary control fail to operate as intended.

**Controls over routine processes vs. controls over non-routine processes** – Controls over routine processes are the manual and automated controls over day-to-day transaction flows. Controls over non-routine processes are the manual and automated controls over estimates and period-end adjustments; these controls often address the greatest risks in the financial reporting process and are most susceptible to management override.

Why: Controls over routine process may be tested throughout the year with some refresh testing toward the end of the year. Controls over non-routine processes are more appropriately tested closer to the end of the year.

## Controls addressing fraud vs. controls addressing unintentional errors

Why: The PCAOB made it clear in issuing Auditing Standard No. 2 that risks and controls must be addressed with respect to BOTH intentional and inadvertent errors. The intent was to make fraud risk explicit in the assessment. Classifying controls in this manner will ensure this has been accomplished. Fraud is unlike inadvertent errors. It is intentional, unrelated to actual transactions, not random, covered up and often facilitated through collusion with intent to deceive.

### 143. 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 121. 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 or other parties who are free of bias and are impartial. Note that the external auditors probably will not rely on process-owner testing.

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

Management should complete the preliminary evaluation on a timely basis so that the external auditor can evaluate the evidence supporting management's preliminary assertion on internal control. The purpose of the suggested approach outlined in our response to Question 60 is to support the development of the body of evidence in Year One for the external audit to begin while the necessary remediation and repair take place.

Thus the period between the date management completes its evaluation (say the end of the second or third quarter) and year-end (the date as of which management must assert the effectiveness of internal control) is an important issue to consider. Changes may have occurred and other issues may have arisen that might have affected the internal control structure since the date of management's preliminary evaluation. If self-assessment is used at year-end and monitoring controls are strong, the refresh testing required at year-end may be reduced to a minimum. However, for the critical controls over priority financial reporting elements, the evaluator may want to perform some refresh testing. Whether that testing takes place as of or after year-end or during a period before but close to year-end is largely dependent on management's confidence in the control structure and the effectiveness of monitoring.

Refresh testing updates interim tests of operating effectiveness to obtain additional evidence to support assertions as of the report date. On the other hand, the purpose of retesting remediated controls is to formulate a conclusion regarding the effective operation of those controls for a sufficient period of time prior to year-end. If the testing results are satisfactory, management should document the resolution of each exception and that the control has been improved. If the testing results are not satisfactory, the unresolved deficiencies along with other control deficiencies that have not been remediated must be evaluated in terms of whether there are other compensating controls in place and found to be operating effectively. If compensating controls do not exist, then management must evaluate the severity of the deficiencies.

At year-end, management must also assess whether there have been changes in internal controls, or in factors that affect the performance of internal controls, subsequent to the interim date. Such changes would invalidate or otherwise impact the results of tests of controls performed at an earlier point in time in the year. For example, the impact of significant changes in processes, personnel and application systems that occur subsequent to the interim date and affect the control environment needs to be evaluated and, as a result, additional tests of controls will be necessary. Such changes could affect the adequacy of controls design effectiveness. Another example would be changes to address control deficiencies identified as part of the

ongoing assessment process. A preventive control previously considered effective may prove to be ineffective if unexpected errors emerge and are detected downstream by compensating controls (see Question 107). In all of these circumstances, these changes require an update in testing. Further, some controls may function only at year-end, thus it may only be feasible to test them at or even after year-end.

An updated review is also an opportunity for management to begin putting in place its process for ongoing evaluations of changes in internal control that must be performed on a quarterly basis starting in Year Two.

The use of technology can provide a very elegant solution to refreshing the second- or 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 strengthening its entity-level monitoring and analytics with the objective of using them on an ongoing basis to support the quarterly evaluation process. The use of 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 One evaluation to year-end without having to perform extensive additional refresh testing and, second, provide a “dry run” of management’s approach for conducting the ongoing quarterly evaluation during Year Two and beyond.

In Year Two 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 and/or risk control specialists.

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 as well as to perform direct tests of controls. See Questions 178 through 189 for a discussion of Year Two and beyond.

#### **145. What should management do when exceptions are identified?**

When exceptions are identified, they must be evaluated carefully. When small minimum judgmental sample sizes are used, exceptions can taint the test results. Even one exception can be an issue depending on the facts and circumstances.

A control with an observed deviation rate that is clearly significant is not an effective control. The correct perspective is to look for controls for which the deviation rate, if any, is negligible. Management must be satisfied that the testing approach, scope and sample size used in testing a control are sufficient to support a conclusion that the control is operating as intended without a greater than insignificant error rate.

When testing operating effectiveness, exceptions or deviations to the control may occur. When evaluating the reasons for the exceptions or deviations, the project team should consider whether:

- The control is automated (in the presence of effective general controls, there is a presumption that an automated application control is expected to always perform as designed).
- The degree of intervention by entity personnel contributes to the exception or deviation.
- Management became aware of the exception or deviation on a timely basis.
- Management responds to the exception or deviation on a timely basis (if management was aware of it).

Regardless of the reasons for the exceptions or deviations, numerous or repeated instances may constitute a control deficiency that is 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.

#### **146. 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. This kind of discipline enables management to understand what is going on in the business and to initiate investigations when things don't look right.
- 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. These reports may utilize points of focus from the COSO Framework to evaluate the control environment and other internal control components.
- 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. In their role, process owners often use inquiry, observation and inspection techniques to satisfy themselves during the supervisory process that the controls are functioning properly. There may also be reports that enable them to evaluate the effectiveness of the process. For example, suspense reports and aging of items in suspense provide an indication as to the effectiveness of the process.

According to COSO, monitoring can be achieved either by obtaining direct evidence of the operation of specific controls or by testing results of control processes. An evaluation of monitoring effectiveness would include review of the integrity of the metrics, information and reports used during the monitoring process. The evaluation should consider the actions taken by management on exceptions, including assessment of the resolution of exceptions and determination of root causes and action taken to correct errors and improve processes. An evaluation of monitoring should be performed quarterly or monthly as determined by management's 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 encountered. These actions should include identifying the root cause(s) of the exceptions, correcting the exceptions and ensuring appropriate process improvements or other necessary actions are taken to avoid the occurrence of future exceptions.

#### 147. How are pervasive process controls tested?

Pervasive process controls can have an indirect impact on the operating effectiveness of information process controls. They include company- or entity-level controls such as establishing and communicating objectives and assigning key tasks to quality people. They also include company- or 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 control functions. 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.

#### 148. How are information process controls tested?

Information process controls are the manual and application controls that apply to any process generating financial and/or operating information, and provide assurance that information is reliable for use in decision-making. "Reliability" means relevant, complete, accurate and timely.

Process owners should self-assess their controls and report results to management. Self-assessment results should cascade upward to the disclosure committee and/or the certifying officers.

However, self-assessment is not enough. Management should also periodically test specific information process controls. Testing should be designed to provide assurances as to the quality of control self-assessments. Increased frequency of testing will allow earlier detection of any control deficiencies and implementation of process improvements to prevent future errors.

Management should design tests of controls to focus on a combination of tests, including inquiry, inspection, observation and reperformance. Examples of tests include the following activities:

- Obtain samples of processed transactions and evaluate attributes or amounts for purposes of inferring whether controls are operating effectively. More extensive samples are required for manual controls whereas a "test of one" (see Question 149) may be sufficient for application controls provided there are strong general IT controls in place.
- Perform reasonableness tests using either internal or external data.
- Compare accounting balances with budgets and prior periods and, if possible, with industry peers.

- Review reconciliations prepared by others and evaluate the appropriate disposition of reconciling items.
- Review the nature and magnitude of items on exception reports on a sample or comprehensive basis and evaluate whether the resolution/disposition of the individual exceptions by others was appropriate.
- Evaluate the differences that result from independent verification (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.

#### 149. How are IT controls tested?

See Question 87 for our approach to breaking down IT considerations during an assessment of internal control over financial reporting. We recommend considering IT controls together with the manual controls in an integrated fashion within a process, i.e., test the IT controls in a manner similar to the controls in other process areas. When controls are manual or automated, the relevant financial reporting assertions must be addressed and the appropriate combination of inquiry, inspection, observation, and reapplication and/or reperformance testing techniques must be applied to formulate a conclusion related to operating effectiveness. Adequate documentation of the testing should also be developed.

At the IT entity level (see Question 87), we expect most of the testing to be related to inquiries, inspection and observation techniques. Reperformance and reapplication techniques cannot typically be accomplished for many of these types of controls.

For the processes in the general IT controls area and for application and data owner controls (as discussed in Question 87), there is a need for all four types of testing, including reperformance and/or reapplication. These are processes in which key controls can and should be tested similar to other processes. Process flows and risk and control matrices should be referenced and considered when selecting the types of tests needed. With respect to timing, some external auditors may assert that pervasive controls such as IT general controls should be tested near the “as of” date. In the initial annual assessment, however, management should complete the testing of these controls as early as possible in the overall process because the results of these tests can drive potentially significant remediation efforts and could directly impact the nature and extent of testing of application controls. In such instances, some update testing near the “as of” date may be also be appropriate to support management’s assertion.

With respect to testing application-specific processes, if the general IT controls are designed adequately and are operating effectively, programmed controls consistently operate – either consistently correctly or consistently incorrectly. Therefore, there are two areas to consider:

- Embedded programmed controls: This program logic includes reasonableness checks, error checking, matching routines, error and exception reporting, complex calculations, critical management report integrity, etc. The evaluation team must test each condition. A “condition” relates to a step in the program logic, i.e., if a routine matches a vendor against the approved vendor list, there are at least two conditions (they match, they don’t match). These tests are dependent on the effectiveness of application change controls.
- Other programmed controls: These types of controls include interfaces, segregation of duties, access controls for critical transactions and data. They must be considered separately since they represent processes that are more dynamic in nature and depend on a proper functioning of the associated process activities.

When testing application-specific controls, there ordinarily is no need for a large sample if the general IT controls are designed and operating effectively. For example, evaluation teams may perform a “test of one” covering all conditions. However, in order to justify such a low scope it is possible the external auditor could require a detailed review of the application logic to form a baseline conclusion that the program logic is consistent with management’s assertion. In such instances, this is an initial year issue and management may choose to prioritize applications for this purpose and evaluate input and output controls for some

applications. Once the baseline is established in the initial annual assessment, the company can focus on change controls and the impact of changes in key application systems.

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

**150. How much testing should management perform relative to the testing the external auditor performs?**

In most areas, management should generally use *at least* the same sample size as the external auditor. The major audit firms have published minimum sample sizes they intend to use during the attestation process. However, the practice of using the minimum sample sizes should not occur in every case. Management needs to evaluate the sample sizes needed to provide a high level of assurance that the controls are operating effectively. See Question 133 for factors management should consider when evaluating sample sizes.

**151. What should the Section 404 compliance team do if a significant level of exceptions is encountered during testing?**

Exceptions should be expected in testing. The compliance team should evaluate each type of exception to understand the nature of exceptions encountered during testing. The number of exceptions should also be considered, as discussed in Question 152. If the nature of exceptions and number of exceptions is not an issue in terms of evaluating the effectiveness of the control in accordance with the parameters set forth in the testing plan (see Questions 126 and 127), the test is completed.

If the nature of exceptions and number of exceptions are an issue, there are several options:

- The compliance team can select a second sample that is expanded in size and retest the control. Retesting in this manner can be expensive because the second test can also generate an unacceptable level of exceptions.
- The compliance team can evaluate the root cause of the exceptions, define the necessary remediation in control design and/or operation, determine that the remediation takes place and then retest the remediated control.
- The compliance team can determine whether there are other controls that address the control objective and, if there are, test those controls to determine whether they are operating effectively. However, even if other controls are in place and operating effectively, the company must carefully consider whether follow-up is necessary with respect to the initial control tested because that control was selected as part of the controls design on which management is relying to satisfy the financial reporting assertion. The validation process cannot be trivialized by testing controls until the evaluator finds controls that work. Furthermore, the PCAOB has pointed out that compensating controls may not be considered when evaluating whether a control deficiency exists (see Question 107).

The above points support the assertion in Question 127 that the rules of engagement should be defined up front in the testing plan.

**152. How many exceptions are acceptable before a control deficiency is deemed to exist?**

The answer to this question ultimately depends on the answer to two different questions:

- What level of error do we expect in the population?
- What level of error are we willing to accept in the population?

This concept of tolerable error is embodied in Auditing Standard No. 2 in which the PCAOB states, "... a control with an observed non-negligible deviation rate is a deficiency." Clearly, the Board's view of "tolerable error" is an error rate that is "non-negligible." We can draw several observations from this point of view:

- A control operation that occurs with numerous or repeated exceptions is not an effectively operating control.
- When small minimum judgmental sample sizes are used, any number of exceptions can present an issue. In such instances, management needs to consider drawing another sample that is expanded in size to obtain more compelling evidence the control is operating effectively or take remedial action and retest the control again.
- “Non-negligible” suggests a high level of effectiveness. For example, what level of effectiveness would management normally expect in any significant business activity? Would management accept a two percent defect rate in its products shipped to customers? No competitive business would accept that level of defects. The same point holds true for any significant business activity representing a repeatable, defined process, particularly a process that significantly affects financial reporting.
- When sample results are on the margin, management should ask the two questions noted above. When considering these questions, it is important to recognize that a test of a sample of items is only an attempt to support an expectation about the level of error that actually exists in the population. When management and process owners select a control as part of the control design that achieves a financial reporting assertion, it is presumed the control is operating effectively. The objective of testing is to validate that presumption. If the sample includes errors, it will be difficult to prove to the external auditor that the control is effective. Therefore, if testing results are marginal, management should consider drawing an expanded sample to retest the control and obtain more conclusive evidence it is operating effectively.
- The PCAOB applies a “reasonable person” test to an entirely different matter in Auditing Standard No. 2. That same test can also be applied to the question of “how many exceptions are acceptable” before a control deficiency is deemed to exist? In other words, what would a reasonable person conclude after evaluating the number of exceptions arising from a given test? If the answer isn’t clear, another test or remediation may be warranted.
- Management should caution Section 404 compliance teams and process owners about “rationalizing away” exceptions. If that kind of bias takes place, the quality of testing results will be compromised, which increases the risk of significant deficiencies (or worse) arising from the attestation process. For example, when the auditor reviews the company’s testing working papers, he or she could reject the conclusions reached based on the company’s documented testing results. The auditor could also perform his or her own test and arrive at different results leading to a conclusion the control is not operating effectively.
- Finally, it is difficult for Section 404 compliance teams to conclusively state the “acceptable number” of exceptions because there may be compensating controls. If the documented controls design includes compensating controls, management may consider that fact when evaluating test results. On the other hand, if there is an absence of compensating controls, that raises the criticality of the control being tested. Section 404 compliance teams should avoid considering compensating controls when evaluating exceptions for an individual control. The PCAOB has cautioned against this practice. See Question 107.

The above points illustrate the considerable judgment coming into play when evaluating test results. They underscore the importance of defining the rules of engagement up front in the testing plan, including defining a “failure condition” as discussed in Question 127.

### **153. 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. This situation may cause management to reassess its testing approach in certain areas.

#### **154. Should the external auditor participate during management’s testing process?**

Not as a general rule. The external auditor may request an opportunity to observe the evaluation teams in action to obtain evidence of management’s assessment process and the degree of competence of the evaluation teams.

---

## **Remediation**

#### **155. If control deficiencies or gaps are identified, how should we remediate them?**

When the evaluation team faces control deficiencies or gaps, the team must evaluate the nature of the identified deficiencies and decide the deficiencies requiring correction. With respect to the deficiencies requiring correction, the evaluation team must design and implement a solution. When designing a solution, the team should address the nature of the deficiencies. For example, for design deficiencies the team should decide and document design improvements. For operating deficiencies, the team should make recommendations on providing the necessary authority or deploying the appropriate competencies to improve performance. When implementing solutions, the team should execute the following steps: Build and test design improvements, roll out design improvements, update policies and procedures, provide training, and measure performance.

#### **156. Assume a company identifies a material weakness in internal control and remedies that deficiency during the year it is required to comply with Section 404 under the SEC’s rules. How soon before the end of the fiscal year must the deficiency be corrected?**

This issue can be summed up with the following two questions:

- If a company has a material weakness, how long does the “fix” need to operate effectively to enable management to conclude that a material weakness doesn’t exist as of year-end?
- If management is able to conclude that a material weakness doesn’t exist as of year-end, what period of time does the auditor need to attest to management’s assertion?

As noted in Question 109, the determination of whether a deficiency is a material weakness rests with management and its auditors. The issue posed by this question adds yet another dimension by focusing on the time frame a “fix” must operate to overcome the “taint” of the control deficiency. It is an issue that will likely be a “facts and circumstances” call, where management will want to consult with the company’s independent accountant. Consultation is important because the audit firms have formulated policies as to the minimum time frame for a control to be in operation. In general, a shorter period might be required if the remediated control is performed more frequently, is nonjudgmental in nature, is automated or is an integral part of several compensating controls on which management is relying with respect to a material transaction. On the other hand, if the control is performed less frequently, is judgmental in nature, is manual or is the sole control on which management is relying with respect to a material transaction, a longer period would be required. See also our response to Question 157.

The real message is that if a company has a material weakness, management should get it fixed sooner rather than later to avoid a situation in which there is insufficient time to demonstrate effective operation of a remedy.

A certifying officer may be able to conclude, for purposes of the certification and the internal control report, that a material weakness has been sufficiently corrected “as of” the end of the relevant fiscal period to permit a conclusion that internal control is effective. However, the company should consider whether the prior existence of the material weakness generated material errors or omissions in previous reports. 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.

**157. Since this Section 404 project requires a point-in-time review, for how long do remediated controls need to be in place and in operation to be considered effective?**

Management should ensure the new controls are in place for a sufficient period of time to permit testing of operating effectiveness. The time period must be adequate to enable management and the auditor to obtain sufficient evidence of the controls' effective operation. For controls over routine processes that are applied continuously or daily, a period of four to six weeks should suffice. For controls operating on a weekly or monthly basis, a couple of months should be adequate. The goal is to assess the operating effectiveness of such remediated controls between the time they were implemented and year-end. The major audit firms have adopted policies on the minimum time frame within which to accomplish that goal, so consultation with the auditor is advised.

---

## Special Circumstances and Situations

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

Assume Company A, an issuer with listed stock, owns 25 percent of Company B, a private company, and accounts for its investment using the equity method. If Company B's statements are audited, the management of Company A should focus on ensuring the company's investments in this unconsolidated entity are properly accounted for in accordance with generally accepted accounting principles, based upon the available audited information and the timing of that information relative to year-end. This view from a consolidation perspective is a practical one as investors rarely have the level of influence to require transparency related to internal controls of investee companies.

The SEC staff has pointed out that investee companies accounted for under the equity method are not consolidated on a line-by-line basis in the investor's financial statements; therefore, the investee company's controls over the recording of transactions into the investee's accounts are not part of the issuer's internal control structure. In making this point, the staff makes no distinction between those equity method investments for which the registrant is required to file audited financial statements pursuant to Rule 3-09 of Regulation S-X and those where no such requirement is triggered.

If the investee's financial statements are audited, the investor should have processes and controls in place in the closing and consolidation process to obtain and use relevant information to account for the investment using the equity method. These processes and controls would focus on:

- Obtaining audited or unaudited financial information for use in recording the equity pick-up of the investor company's prorata share of income or loss.
- Consistent application of the estimation processes necessary to cover the gap between the investor company's reporting date and the date of the most recent set of financial information from the investee company. The financial reporting objective is to ensure that 12 months of equity pick-up is recorded during each annual period.
- Proper treatment of dividends, if any, as a reduction of the investment.
- Obtaining the necessary information to determine whether an impairment has occurred and to ensure the appropriate involvement of management in reaching a conclusion as to the need for an impairment write-down. These asset impairments are rare in practice.

**159. How are material acquisitions occurring during the fiscal year handled for purposes of determining the scope of the Section 404 assessment?**

The SEC provides relief on the issue of acquired entities of such size and/or complexity it is impossible for management to complete an assessment of their internal control over financial reporting during the period

between the consummation date and the acquiring company's fiscal year-end. While the SEC staff indicated it is expected that management would ordinarily include in its scope the controls at all consolidated entities, they acknowledged that it might not always be possible to conduct an assessment of an acquired entity's internal control over financial reporting in sufficient time to incorporate the results in the internal control report filed for the year during which the acquisition took place.

The effect of the SEC staff's position is as follows. If there is an acquisition during the year, management may evaluate the facts and circumstances to determine whether there is sufficient time to consummate the assessment of internal control over financial reporting for that entity in accordance with the appropriate assessment scope on a consolidated basis. If management decides to exclude the acquired business from its report on internal control over financial reporting, the staff would not object so long as there is adequate disclosure. With respect to adequacy of disclosure, the staff expects the following:

- (a) Management must refer in the internal control report to a discussion in the registrant's Form 10-K or 10-KSB regarding the scope of the assessment, noting that management excluded the acquired business from management's report on internal control over financial reporting.
- (b) If the reference in (a) is made, management must clearly identify the acquired business excluded and indicate the significance of the acquired business to the acquiring company's consolidated financial statements.
- (c) Notwithstanding management's exclusion of an acquired entity's internal controls from its annual assessment, the company must disclose any material change to its internal control over financial reporting due to the acquisition in accordance with Exchange Act Rule 13a-15(d) or 15d-15(d), whichever applies.

The staff places limits on the period of time during which management may exclude the acquisition from the assessment of internal control over financial reporting. The period in which management may omit an assessment on a consolidated basis of an acquired entity's internal control over financial reporting may not extend beyond one year from the date of acquisition. Furthermore, an assessment may not be omitted from more than one annual management report on internal control over financial reporting.

Based on discussions with the SEC staff, the overriding principle they are using in applying their guidance is that management can exclude a newly acquired business from only one internal control report. Rather than the timing (12 months), the key is the sufficiency of the time available for management to evaluate the internal controls of the newly acquired business after closing the transaction. Therefore, a practical approach for applying this guidance is to view the close of the fiscal year as the benchmark for looking back one year. Management should apply its "best efforts" to integrate the internal controls of the newly acquired business into the current year Section 404 assessment. If that is not possible based on the facts and circumstances, including the size and complexity of the acquisition and the available time, the internal control over financial reporting for the newly acquired division or unit can be excluded from the internal control assessment for that fiscal year, but not for the subsequent year.

#### **160. How are divestitures of significant entities (or net assets) and discontinued operations considered for purposes of evaluating internal control over financial reporting?**

In Auditing Standard No. 2, the PCAOB states, "The scope of the evaluation of ... internal control over financial reporting should include entities that were acquired on or before the date of management's assessment and operations that are accounted for as discontinued operations on the date of management's assessment." To illustrate, assume a company divests itself of a subsidiary or a major facility and the divestiture is consummated outright as of the date of sale without any pending contingencies, and a gain or loss on the sale and all related liabilities, if any, are recorded at that time. In that case, there are no controls to evaluate because the company has divested itself of the subsidiary or facility and there are no operations, work out activities or controls in existence as of the year-end assessment date. However, if the sale is not consummated by year-end and the company retains rights and title to specific assets and is obligated for related liabilities, the subsidiary or facility must be considered for purposes of inclusion within the scope of the Section 404 project.

Discontinued operations are different from an outright sale or divestiture of facilities, entities or net assets, however. The expected loss is recorded as of the date of management's decision to discontinue and any expected operating losses through the date of final disposition are accrued. Any expected income from discontinued operations through the date of disposition are recorded in the period in which they are realized. The net assets are consolidated on a one-line basis on the balance sheet and the related operations are one-lined on the income statement to exclude them from continuing operations. Thus discontinued operations accounting separates the operations of a discontinued location or unit from continuing operations so investors can evaluate separately the operations of continuing significance and understanding the magnitude and impact of discontinued operations. There is also a significant amount of information that is required to account for discontinued operations. For example, there are estimates to be made to properly reflect the economics as of the date of management's decision to discontinue. Actuals are compared to estimates every quarter, differences are recorded and prior estimates are updated.

Discontinued operations, therefore, must be considered for purposes of determining the Section 404 project scope if the sale is not consummated as of the year-end assessment date. In these situations, management should evaluate the discontinued operations as a separate unit like all other locations and units in terms of their significance to consolidated operations. If significant, management should document the processes and controls in place to ensure that the discontinued operations are properly accounted for. The key factors driving the nature and extent of work to be done on the processes and controls related to discontinued operations include (a) the length of time it will take to execute management's plan of discontinuance, (b) whether the assets continue to operate as of year-end, and (c) the timing of the ultimate consummation of sale. If the sale were to close before the date of management's assessment, the discontinued operations need not be included within the scope of the Section 404 assessment. If the sale were to close after the assessment date, the discontinued operations would fall within the scope of the Section 404 assessment.

As discontinued operations often function until a willing buyer is found, the unit continues to generate revenues, costs and expenses, just like any unit that is part of continuing operations. On the other hand, if facilities are shut down and there are no operations, the focus of the controls is limited to the development of information needed to account for the gain or loss as of the decision date plus the accrual of related liabilities (e.g., severance costs).

**161. How does a lag in reporting of the financial results by certain foreign subsidiaries for financial reporting purposes affect the assessment of internal control over financial reporting?**

Many companies with global operations have a lag in reporting the financial results of certain foreign subsidiaries for financial reporting purposes. For example, the SEC staff used an example of a 30-day lag to illustrate the circumstances, i.e., an entity with a December 31 year-end may consolidate the operations of certain foreign subsidiaries reporting annual results for the period ended November 30 on a consistent basis year-to-year. The staff is of the view that this difference in period ends is also acceptable in relation to the assessment of internal control over financial reporting. Reporting lags are also common for certain investments accounted for on the equity method.

**162. How are certain entities consolidated based on characteristics other than voting control, including certain variable interest entities and entities accounted for via proportionate consolidation, handled for purposes of determining the scope of the Section 404 assessment?**

The SEC typically expects management's report on internal control over financial reporting to address the controls at all consolidated entities, irrespective of the basis for consolidation. However, there may be situations where an entity was in existence prior to December 15, 2003 and is consolidated by virtue of FASB Interpretation No. 46 (revised December 2003), *Consolidation of Variable Interest Entities: An Interpretation of ARB No. 51*. That interpretation in the authoritative literature requires that companies apply that guidance and, if applicable, consolidate entities based on characteristics other than voting control no later than the period ending March 15, 2004 (or December 15, 2004 for small business issuers). In these instances where the company lacks the ability to dictate or modify the internal controls of an entity consolidated pursuant to

Interpretation No. 46, it may not have legal or contractual rights or authority to assess the internal controls of the consolidated entity even though that entity's financial information is included in the registrant's financial statements. Similarly, for entities accounted for via proportionate consolidation in accordance with Emerging Issues Task Force Issue No. 00-1 (EITF 00-1), management may not have the ability to assess the internal controls.

In these situations, the SEC staff is of the view that management should disclose the following, either in the internal control report or elsewhere in the body of the annual report:

- The company has not evaluated the internal controls of the entity (or entities) in question and the conclusion regarding the effectiveness of the registrant's internal control over financial reporting does not extend to the internal controls of the entity (or entities) in question.
- Total assets, net assets, revenues and net income that result from consolidation of the entity (or entities) whose internal controls have not been assessed.
- Management has been unable to assess the effectiveness of internal control at the entity (or entities) included in the consolidated financial statements due to the fact that the registrant does not have the ability to dictate or modify the controls of the entity (or entities) and does not have the ability, in practice, to assess those controls.

**163. If controls are replaced or eliminated during the period before the end of the year, must the evaluation team test them?**

No. If management implements changes prior to the end of the year to make controls more efficient and effective or to address control deficiencies, the superceded controls need not be tested. These superceded controls will not exist as of the end of the year and therefore are irrelevant. However, management should ensure the new controls are in place for a sufficient period of time to permit testing of operating effectiveness. See Questions 128 and 157 for discussion regarding a "sufficient period of time." In addition, the SEC requires public disclosure of any change in internal control over financial reporting that has materially affected, or is reasonably likely to materially affect, internal control over financial reporting.

---

## Reporting

**164. 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.

### **165. 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 196. 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.

### **166. 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.

In Auditing Standard No. 2, the PCAOB points out that management's conclusion about the effectiveness of internal control over financial reporting may take many forms. The Board reiterates the SEC's requirement that management state a direct conclusion about effectiveness. For example, the Board provided sample language: "...management's assessment that W Company maintained effective internal control over financial reporting as of [date]." The Board cautioned on several points:

- The use of subjective phrases like "very effective" should be avoided.
- Negative assurance statements are not acceptable, e.g., "nothing came to management's attention to suggest that the company's internal control over financial reporting is not effective."
- Management is not permitted to conclude internal control over financial reporting is effective if there are one or more material weaknesses.

Management may not qualify the internal control report. According to the SEC staff, management cannot make statements like "the company's controls and procedures are effective except to the extent that certain problems have been identified or express similar qualified conclusions." The staff points out that management must take those problems into account when concluding whether the company's internal control over financial reporting is effective.

**167. When management identifies a control deficiency that is deemed to be a material weakness in internal control over financial reporting, must the company disclose the weakness in its public reports even though the weakness may be corrected prior to the end of the year? If so, when is this requirement effective?**

Regulation S-K Item 308(c) requires companies to disclose any change (which, one could assume, would include a change to correct a material weakness) in the company's internal control over financial reporting that occurred during the company's last fiscal quarter that has materially affected (or is reasonably likely to materially affect) the company's internal control over financial reporting. Regulation S-K Item 308(c) is currently effective and required by Form 10-Q. In the context of disclosing any such changes, a company may conclude that it is prudent to describe any material weaknesses (or potential material weaknesses) that gave rise to the change.

The SEC staff has noted that they expect a registrant to make periodic improvements to internal controls and would welcome disclosure of all material changes to controls, whether or not made in advance of the compliance date of the rules under Section 404 of the Sarbanes-Oxley Act. However, the staff would not object if a registrant chose not to disclose changes made in preparation for the registrant's first management report on internal control over financial reporting. That said, consistent with the point of view we expressed above, the SEC staff reiterated that if a registrant has identified a material weakness, it should carefully consider whether that fact should be disclosed, including changes made in response to the material weakness.

After the issuance of the registrant's first management report on internal control over financial reporting, pursuant to Item 308 of Regulations S-K or S-B, the SEC staff points out that registrants are required to identify and disclose any material changes in its internal control over financial reporting in each quarterly and annual report. This would encompass disclosing a change (including an improvement) to internal control over financial reporting that was not necessarily in response to an identified significant deficiency or material weakness (i.e. the implementation of a new information system) if it materially affected the registrant's internal control over financial reporting.

**168. If the Section 404 compliance team determines at year-end that there are control deficiencies deemed to be significant deficiencies in internal control over financial reporting, are there circumstances requiring public disclosure of these deficiencies in connection with the filing of the internal control report?**

The SEC staff has pointed out that a registrant must identify and publicly disclose all material weaknesses. If management identifies a significant deficiency, it is not obligated to publicly disclose the existence or nature of the significant deficiency. However, the SEC staff has pointed out the following: If management identifies a significant deficiency that, when combined with other significant deficiencies, is determined to be a material weakness, management must disclose the material weakness and, to the extent material to an understanding of the disclosure, the nature of the significant deficiencies. Furthermore, if a material change is made to either disclosure controls and procedures or to internal control over financial reporting in response to a significant deficiency, the registrant is required to disclose such change and should consider whether it is necessary to discuss further the nature of the significant deficiency in order to render the disclosure not misleading.

**169. How is materiality considered for purposes of evaluating the effects of changes on internal control over financial reporting?**

In guidance published as a response to a frequently asked question, the SEC staff stated the following with respect to considering materiality:

Materiality, as with all materiality judgments in this area, would be determined upon the basis of the impact on internal control over financial reporting and the materiality standard articulated in *TSC Industries, Inc. v. Northway, Inc.* 426 U.S. 438 (1976) and *Basic Inc. v. Levinson*, 485 U.S. 224 (1988). This would also include disclosing a change to internal control over financial reporting related to a

business combination for which the acquired entity that has been or will be excluded from an annual management report on internal control over financial reporting ... As an alternative to ongoing disclosure for such changes in internal control over financial reporting, a registrant may choose to disclose all such changes to internal control over financial reporting in the annual report in which its assessment that encompasses the acquired business is included.

In summary, the key is that information is material if it would have affected the manner of an investor's decision-making when he/she made an investment decision, i.e., the decision-making process. However, it is not necessary that the information would have caused the investor to change his/her decision, i.e., the substantive outcome.

#### **170. Must management disclose improvements to internal controls?**

With respect to improvements in internal control over financial reporting, they must be disclosed if they have a material effect, or are reasonably likely to have a material effect, on internal control over financial reporting. The SEC staff indicated in the above frequently asked questions document the following:

- Generally they “expect a registrant to make periodic improvements to internal controls and would welcome disclosure of all material changes to controls, whether or not made in advance of the compliance date of the rules under Section 404 of the Sarbanes-Oxley Act.”
- The staff “would not object if a registrant did not disclose changes made in preparation for the registrant's first management report on internal control over financial reporting.”
- However, after the registrant's first management report on internal control over financial reporting, pursuant to Item 308 of Regulations S-K or S-B, the registrant is required to identify and disclose any material changes in the registrant's internal control over financial reporting in each quarterly and annual report. This disclosure “would encompass disclosing a change (including an improvement) to internal control over financial reporting that was not necessarily in response to an identified significant deficiency or material weakness (i.e., the implementation of a new information system) if it materially affected the registrant's internal control over financial reporting.”

#### **171. 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.

#### **172. 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.

#### **173. 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 to investors any change in the company's internal control over financial reporting that occurred during the issuer's most recent fiscal quarter that has materially affected, or is reasonably likely to materially affect, the company's internal control over financial reporting.

#### **174. 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. For example, for six months ended April 30, 2004, we looked at the companies that filed 133 reports with the SEC relating to internal control matters to obtain insights as to the potential market impact of reporting material weaknesses in internal control. We considered the following tests:

- The change in the reporting entity's stock versus the market as a whole from the closing price as of the day before disclosure to the closing price as of the day of disclosure (the day of disclosure is hereinafter referred to as the "disclosure date").
- The change in the reporting entity's stock versus the market as a whole during the trading day immediately before the disclosure date as compared to during the trading day immediately after the disclosure date.
- The change in the reporting entity's stock versus the market as a whole during the three trading days immediately before the disclosure date as compared to during the three trading days immediately after the disclosure date.

Applying the above tests, we found that the average stock price did indeed decline relative to the market in general. A range of two percent to four percent was a reasonable gauge as to the potential immediate market impact, which is not insignificant considering a company's market capitalization. While one may debate the cause of this impact, it appears that the market is reacting to the reports of material weaknesses in internal control.

It should be understood that the above impact is not necessarily indicative as to the potential impact of an adverse opinion (or a disclaimer of opinion, as discussed in Question 211) on internal control over financial reporting from the auditor. In a report issued earlier in 2004, Goldman Sachs reported, "We believe an unfavorable auditor opinion could have significant negative share price implications given investors' heightened interest in accounting transparency and corporate governance." It is possible the market recognizes management is currently working to prepare their company's internal controls for public reporting and will be less forgiving if management fails to pass the attestation test.

The damage to reputation could also be troublesome if the external auditor issued an adverse opinion. Just as an organization is known and respected for its products, services and brands, in the financial reporting fishbowl it sells something else – its reputation and integrity. This should be enough to get one's attention, because the stakes are high.

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.

#### **175. What happens if a company completes its Section 404 assessment and files an unqualified internal control report, and subsequently restates its financial statements for the applicable period?**

We will use the following scenario to address this question. Assume a calendar year reporting company and an accelerated filer, Company A, completes its Section 404 assessment for 2004 and files its first internal control report in its 2004 10-K filed in March 2005. The internal control report is clean, e.g., internal control over financial reporting is designed and operating effectively and there are no material weaknesses noted. The external auditor also issues in its attestation report included in the 2004 10-K an unqualified opinion that management's assessment is fairly stated AND that internal control over financial reporting is effective. Assume further that sometime during calendar 2006, Company A issues restated financial statements affecting the reported results for 2004. The restatement is attributable to a material weakness that existed during the 2004 reporting period but was not detected either by management or by the external auditor.

Several questions arise. For example:

- Will the SEC require management to reissue the 2004 internal control report?

While we do not note any provisions in the SEC's release on Section 404 that directly addresses this question, PCAOB Auditing Standard No. 2 states that a restatement of previously issued financial statements to reflect the correction of a misstatement is "at least a significant deficiency" and "a strong indicator that a material weakness in internal control over financial reporting exists." If the restatement is attributable to a control deficiency existing during 2004, Company A's management may have no choice but to reissue its assessment of internal control over financial reporting for that year because its original assessment may have been incorrect. Therefore, once management reports an error in previously reported financial statements, prior internal control reports indicating internal control over financial reporting as being effective during the reporting period may also require reissuance to explain that internal control over financial reporting was not effective during the applicable period and, if appropriate, the deficiencies have since been corrected. In addition, because a company is required to disclose any change in internal control over financial reporting that has materially affected, or is reasonably likely to materially affect, internal control over financial reporting, management likely would want to include disclosure regarding any changes made in response to the material weakness as part of its restatement.

- Will the external auditor reissue its 2004 attestation report on internal control over financial reporting?

At the time of this publication, we are not aware of any specific guidance that directly addresses this question. It is possible that the external auditor may apply a rebuttable presumption that a control deficiency or a combination of control deficiencies giving rise to a restatement of previously issued financial statements is a material weakness in internal control over financial reporting. If this presumption holds based on the analysis of the attending facts and circumstances, it is reasonable to expect the auditor to reissue the audit report on the effectiveness of internal control over financial reporting AND on management's assessment of internal control over financial reporting. Further, once management's assessment has been revised, assuming it is, the auditor's attestation will obviously no longer be applicable and would likewise require revision.

- What position will the SEC take with respect to the various 302 certifications filed during the period(s) the material weaknesses existed? Will they require them to be revisited or reissued?

To restate its financial statements, Company A would need to file a 10-K/A. Rule 12b-15 requires the company to include new 302 and 906 certifications with the 10-K/A.

- In civil and/or criminal proceedings, will prosecutorial authorities (SEC, Department of Justice, etc.) take advantage of management's issuance of (1) a "false" internal control report for 2004, and (2) 302 certifications during the year (and any other periods) a material weakness existed?

Obviously, this is a question for legal counsel. Whether criminal or civil liability will result from the false certifications depends on the circumstances under which the mistake arose, the extent of the mistake and various other factors. If, for example, a certifying officer willfully files a false 302 certification, it could subject the officer and/or the company to criminal liability. Willful violation of the Exchange Act is a felony that is punishable by fine and imprisonment. It could also be the subject of civil liability as the SEC could pursue a civil enforcement action against the officer, the company or both. A false 302 certification may also expose both the company and the certifying officer to criminal liability under a variety of other statutes.

In terms of civil liability, the act of filing new 302 and 906 certifications creates additional factual predicates on which governmental authorities and/or private plaintiffs may premise complaints for false and misleading information. For example, it is common to see class action suits alleging defendant companies "lacked adequate internal controls and as a result, issued misleading financial statements, causing the stock price to be artificially inflated."

## 176. What documentation does management need to support the assertions in the internal control report?

During the Section 404 compliance process, much documentation occurs. According to the PCAOB, the Section 404 compliance team must document management's approach and the basis for management's decisions, including the processes, procedures and due diligence management completed in executing its responsibilities and supporting its conclusions. There should be sufficient documentation of the rationale and framework for identifying significant accounts, location coverage, testing scopes and addressing exceptions. The compliance team's documentation should indicate who is involved in making decisions and should maintain minutes and memoranda to record key decisions made. All of this documentation evidences management's assessment process.

As an illustration, the project documentation might include, among other things:

- From Set the Foundation and Phase I (see Question 60)
  - Analysis of financial reporting elements to select the priority elements;
  - Decomposition of the reporting entity into locations and units and business processes, and supporting analysis selecting the control units and the significant processes feeding the priority financial reporting elements;
  - Support for the assessment of company-level controls;
  - Support for the assessment of general IT controls;
  - Support for the evaluation of the antifraud program and controls, including the specific controls designed to prevent or detect fraud, who performs them and the related segregation of duties; and
  - Process maps or equivalent documentation evidencing the period-end financial reporting process and identification of the points at which material misstatements due to error or fraud could occur.
- From Phase II (see Question 60)
  - Process maps or equivalent documentation evidencing how significant transactions are initiated, authorized, recorded, processed and reported, and identification of the points at which material misstatements due to error or fraud could occur;
  - Evidence of design of controls over all relevant assertions related to all significant accounts and disclosures;
  - Linkage of accounts to assertions to controls;
  - Evidence the five components of COSO (including the control environment and company-level controls) are addressed;
  - Controls in place that address the identified risks of material misstatements due to error or fraud that could occur;
  - Controls in place that safeguard assets;
  - The results of management's evaluation of controls design effectiveness;
  - Management's testing plan; and
  - The results of management's interim tests of controls operating effectiveness.
- From Phase III and IV (see Question 60)
  - The results of management's evaluation of control deficiencies and communications of findings to the auditor and audit committee; and
  - The results of management's retesting of remediated controls and refresh tests to update preliminary conclusions regarding controls operating effectiveness.

While not necessarily all-inclusive, the above list illustrates the substantial amount of documentation developed during the Section 404 compliance process.

The PCAOB also requires testing of the following controls:

- Controls over initiating, authorizing, recording, processing and reporting significant accounts and disclosures and related assertions inherent in financial reporting (these include application controls embedded within processes that are not explicitly mentioned in the above list, but are nonetheless important)
- Controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles
- Antifraud programs and controls (i.e., controls related to the prevention, identification and detection of fraud)
- Controls, including information technology general controls, on which other controls are dependent
- Controls over significant non-routine and non-systematic transactions (e.g., accounts involving judgments and estimates)
- Company-level controls, including the control environment and controls over the period-end financial reporting process

The compliance team's controls design and testing documentation must address these points.

We recommend that an overall high-level document be prepared to evidence management's assessment process. This memorandum should describe the steps of the process and refer to the project documents and work products. Examples of the project documents and work products may be attached to the overall memorandum as exhibits. The memorandum should describe the results of the design effectiveness work and the control testing work, including the identification and disposition of control deficiencies. The high-level memorandum should also be global in focus. For example, it might list by process the number of primary controls, the number of controls deemed "effective" and "ineffective" based on the initial testing, the number of "ineffective" controls remediated and retested, the number of controls for which a preliminary conclusion was reached requiring refresh testing, the controls for which refresh testing is completed, and the final conclusions.

The overall memorandum should accomplish four very important objectives:

- First, it should support the assertions to be included in the internal control report.
- Second, it should provide support that management has addressed all of the specific points provided by the PCAOB to the auditor as to what to look for with respect to evaluating management's assessment process and the comprehensiveness of management's controls documentation.
- Third, the certifying officers need some overall documentation to enable them to walkthrough the work done. Wading through the details is not the most effective way to help these senior executives gain confidence that the work done is complete and responsive to the requirements.
- Finally, the memorandum can serve as a tool for providing transparency to the auditors and the audit committee as to management's assessment process.

With respect to documentation, there is another important matter. Note that even if controls need not be tested at individually insignificant locations and units, controls documentation may be necessary at those locations and units, including when they are insignificant when aggregated. Some auditors are taking the position that management should have at least a minimum level of documentation of controls at locations and business units that are not considered significant, either individually or in the aggregate. This point of view is based on the SEC's requirement of public companies to "maintain adequate books and records."

Such documentation need not be as extensive, however, as the documentation at significant locations and units. Company policies, procedural manuals, job descriptions and completed standardized control checklists are examples of the kind of documentation which may be provided at these insignificant locations and units.

**177. How long must management retain the documentation supporting the assertions in the internal control report?**

Although the instructions to Regulation S-K, Item 308, require a company to “maintain evidential matter, including documentation, to provide reasonable support for management’s assessment of the effectiveness of the [company’s] internal control over financial reporting,” the instructions do not prescribe a minimum time period. The Sarbanes-Oxley Act and the rules issued by the SEC require auditors to maintain, for seven years after the conclusion of the audit, all “records relevant to the audit or review, including workpapers and other documents that form the basis of the audit or review, and memoranda, correspondence, communications, other documents, and records (including electronic records), which (1) are created, sent or received in connection with the audit or review and (2) contain conclusions, opinions, analyses, or financial data related to the audit or review.”

It would stand to reason that comparable documents prepared by the company could be deemed relevant to any future investigation into the company’s audit processes and, therefore, should be retained by the company for seven years as well. For example, company documentation might include, among other things: the selection of significant financial reporting elements and processes affecting those elements; the documentation of risks and controls supporting the assessment of controls design effectiveness; and the nature, timing and extent of tests of controls operation, as articulated in the testing plan, and management’s execution of the testing plan, as articulated in the “working papers” (e.g., the testing working papers, the technology tool documentation, etc.). In addition, pursuant to Rule 12b-11(d) under the Exchange Act, a company must keep all manually signed documents filed with or furnished to the SEC (including the certifications) for five years.

Needless to say, this question is one requiring input from legal counsel. Given the tenure of the times, no policy should be adopted and no steps should be taken without consulting counsel.

Another area related to the question of documentation retention deals specifically with the retention of documents and documentation by process owners to facilitate reperformance testing by auditors. We believe that the duration of retaining that type of documentation need not be as long as the working papers and related documentation described above once the auditor’s tests are completed. We are aware of one company adopting a sufficient period of time to cover the certification period and the outside auditor review period as well as provide a period of time as a sufficient “cushion.” The breadth of Section 404 (including the number of controls evaluated) and the number of systems involved make this kind of retention period for “second level” documentation a challenge. Because of the impact of auditor efficiency and sign-off and the fact that there may not be a compelling business need to retain this evidential matter for long periods of time, the external auditor’s expectations will probably be the driver of practice with respect to this level of documentation.

In some industries, there are laws and regulations that require retention of specific documents. These laws and regulations must also be considered when evaluating the company’s documentation retention policy. Again, legal counsel needs to weigh in on the document retention issue. The general counsel should also be involved in addressing these questions.

---

## **Moving Beyond the Initial Year One Assessment**

**178. Why should certifying officers care about the SOA Section 404 compliance structure going forward after the first internal control report is filed?**

CEOs and CFOs are required – on a quarterly basis – to attest that they are responsible for establishing and maintaining internal control over financial reporting, and that they have disclosed any change in internal

control over financial reporting that has materially affected, or is reasonably likely to materially affect, internal control over financial reporting. Thus they have two concerns with respect to Section 404. First, they want assurance that the controls over financial reporting are designed and operating effectively. Second, they don't want a material weakness to emerge. As a result, CEOs and CFOs should continue to closely monitor developments regarding internal control over financial reporting on a periodic basis.

### **179. What are the elements of an effective SOA Section 404 compliance structure after the initial annual assessment is completed?**

Certifying officers should take the following steps in preparing their organizations for moving beyond the initial year of Section 404 compliance:

- Pay attention to “tone at the top.” It starts with your personal involvement and commitment. Overtly support a strong control environment through, among other things, the code of conduct (see Issue 5 of Protiviti's *The Bulletin*, available at [www.protiviti.com](http://www.protiviti.com)), audit committee oversight (see Issue 9), an effective process for handling confidential and anonymous complaints (see Issue 11), clear policies for assigning authority and responsibility, effective human resource policies and practices, and an organization structure and management style that is conducive to an open and transparent internal control environment. Speak out about ethics, internal control and personal integrity in company meetings. Let the organization know ethical violations will not be tolerated.
- Reinforce responsibility and accountability through establishment of a self-assessment process. If you already have a self-assessment process, make sure it is effective and is linked to specific business processes and critical controls. If you don't have a self-assessment process, conduct one periodically. Provide guidance to your process owners as to what is expected of them in supporting the assessments they submit. Let them know internal audit will periodically review the basis for their assessments. Engage your operating unit managers by making them privy to self-assessment results and request their participation when following up on matters requiring remediation.
- Implement a change-recognition process. When certifying officers have confidence that disclosure controls and internal control over financial reporting are functioning as intended, and processes are improved as necessary when changes occur in the business, they will be able to focus on the disclosure implications of change. This is where their focus should be. A formal change-recognition process is needed to identify emerging risks, issues and developments in a timely manner for action and disclosure on a quarterly basis.
- Consider establishing a risk control specialists group to support your process owners with remediation, design changes and documentation updates during times of change and to perform testing of operating effectiveness. Decide whether to (1) embed the risk control specialists within operations, or (2) establish an independent risk control function either reporting to a C-suite executive or housed within the internal audit department.
- Define the SOA year two role of the internal audit department. Focus internal audit's role on evaluating management's assessment process, performing testing in selected areas and reporting results. Define the function's role consistent with its other responsibilities (e.g., to conduct operational and compliance audits in critical risk areas), its capabilities and its available capacity.
- Formalize a reporting and escalation process that will support management's continuing responsibilities under Section 302 and initiate timely remediation of significant deficiencies. Management must disclose significant deficiencies and material weaknesses to the audit committee and external auditors on a timely basis. Management must also make sure a process is in place to report and escalate significant deficiencies and potentially significant deficiencies to the disclosure committee and to other designated management as soon as practicable.
- Understand who is taking charge of identifying and controlling the unique risks introduced by IT. Don't underestimate the importance of managing IT-related risks. The complexity of technology makes these risks more critical. Confirm that the chief information officer is engaged continuously in the process of

evaluating internal control over financial reporting. Also, be sure your software solution for managing compliance satisfies your needs going forward.

- Insist on getting value for your first-year investment. Once the first internal control report is filed, ask your people to mine the value of the increased transparency into your business processes that the Section 404 compliance documentation provides. If you don't get results, your people aren't looking hard enough.

“Life after year one” cannot begin until the above steps are taken to lay a strong foundation for ongoing compliance. Because they necessitate advance preparation THIS year, some companies have already begun to focus on these steps to ensure that the investments they are currently making will payoff in the future.

### **180. How are process owners engaged going forward?**

Process owners should be held accountable for the effective functioning of internal controls for which they are responsible. Through an effective self-assessment process, accountability is reinforced by requiring process owners to respond to questions regarding specific controls for which they are responsible, creating a transparent “chain of accountability” for internal control over financial reporting. The Section 404 compliance process lays the foundation for an effective self-assessment process by providing insights as to the key controls and the owners of those controls.

The PCAOB has taken the position that company-level controls include “controls to monitor other controls, including ... self-assessment programs.” Because “process owners” are the men and women closest to the critical control points within the organization, they are best positioned to know what's working and what isn't, when changes are occurring in the process, and what's the impact of systems and other pervasive changes on the controls within the process. Process owners both execute controls and supervise and monitor the owners of controls, and ultimately are responsible for assessing the design and the performance of controls.

What does this mean to certifying officers? If you don't have a self-assessment process, implement one. If you have a self-assessment process already in place, improve it. Make it more robust by linking it to the critical controls identified by the Section 404 compliance process and including it as an integral part of the disclosure process and continuous monitoring required by Section 302 reporting. Look at self-assessment as a management tool that drives the “tone at the top” down to the process owners.

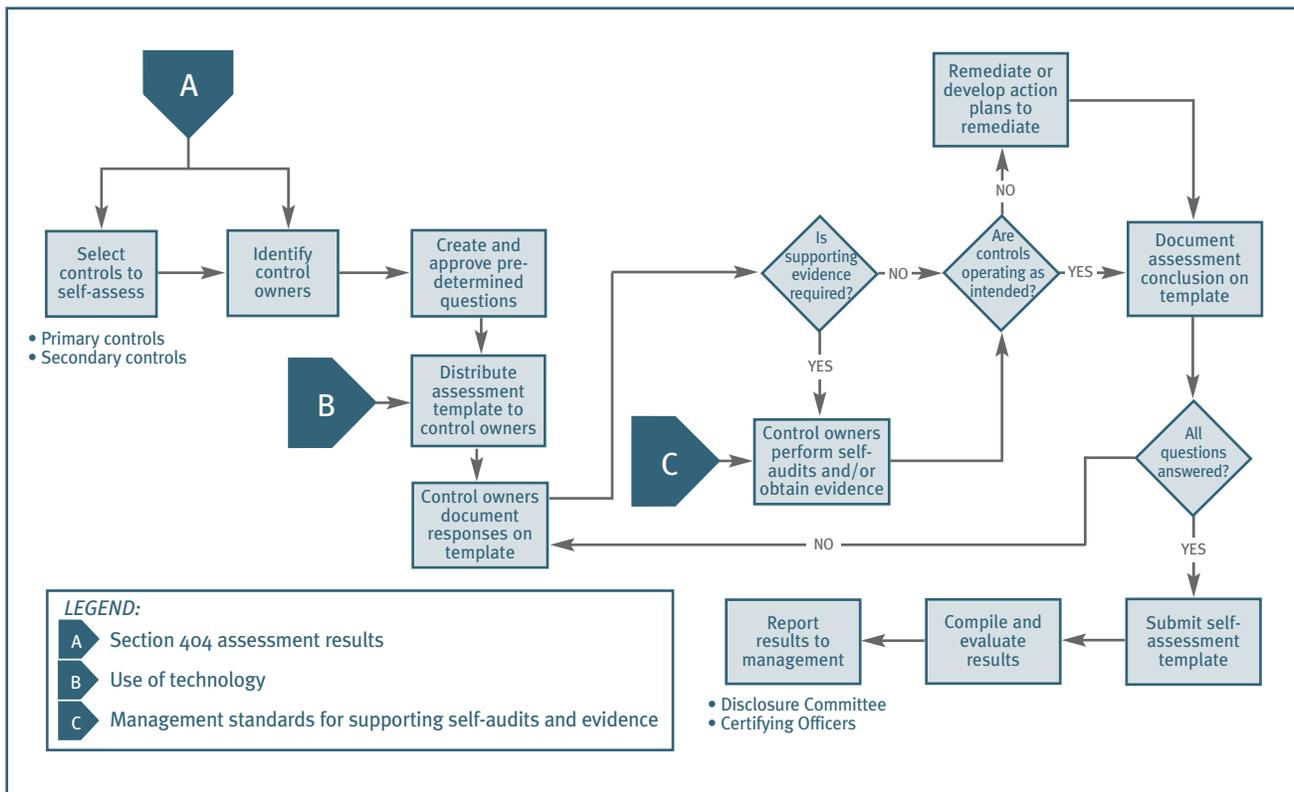
### **181. How does self-assessment work going forward?**

The self-assessment process involves several key components:

- The key controls have been identified.
- The owners of those controls are known.
- Predetermined questions are approved by management.
- The process involves rigorous deployment of questions and follow up with owners.
- The process may be applied at the entity and process levels.
- Self-assessment results are communicated to management.
- Exceptions and open matters are resolved on a timely basis.

Process and control owners often use inquiry, observation and inspection techniques as they supervise and monitor the activities for which they are responsible to assess whether the controls are functioning properly. They may also use reports to evaluate the effectiveness of the process, e.g., accounts receivable in suspense reports and aging of items in suspense provide an indication as to the effectiveness of the accounts receivable process. These activities provide the basis for periodic self-assessments. These activities may be augmented by additional self-audits by the process owners as prescribed by the self-assessment process.

Self-assessment involves the following steps:



The effectiveness of self-assessment is evaluated in terms of the quality and reliability of the assurances the process provides to certifying officers. Internal audit can test selected controls to evaluate the self-assessment program.

While self-assessments can be performed for the primary and critical controls, they cannot be relied upon as the sole evidence supporting management's conclusions regarding internal control over financial reporting. For primary controls, other evidence is needed through tests of controls to support the annual assertion. Therefore, self-assessment may complement other testing approaches to provide certifying officers assurance that the primary controls are operating as of a point in time, e.g., at year-end or quarter-end.

## 182. Why do process owners need support going forward?

Companies are investing thousands of hours of effort in year one and in some cases spending millions of dollars. Going forward, it is unrealistic to expect the process owners to shoulder the burden of Section 404 compliance by themselves. If there are significant changes, it is inconceivable how they will get the job done without support. It is imperative, therefore, that companies protect their initial-year investment by supporting process owners and ensuring ongoing compliance.

The PCAOB requires management to maintain up-to-date compliance documentation. The good news is that the documentation arising from Year One compliance may be rolled forward if there are no changes in policies, processes, people and systems. That said, who will keep this documentation up-to-date going forward? Who will assess the impact of changes in processes and systems, redesign controls in response to change and update the related controls documentation for changes made? Who will remediate deficiencies when necessary? Do process owners know how to do these things? Who will coach, assist and evaluate them? An appropriate organizational structure that facilitates compliance must provide answers to these questions, because process owners are neither auditors nor experts in documentation and remediation. They need help and support going forward after year one.

### 183. What are alternative structures for supporting process owners in complying with SOA Section 404 after the initial annual assessment?

The matter of organizational structure is very important. For purposes of ongoing compliance with Section 404, there are at least two important aspects affecting structure. The first is the issue of managing gaps and overlaps. The second is establishing the appropriate transitional organizational structure.

#### *Managing Gaps and Overlaps*

An organizational structure that drives effective internal control over financial reporting is predicated on a sharp delineation of roles and responsibilities. The question of “ownership” is oftentimes obscured by the “command and control” structure of most organizations because that structure has always placed strong emphasis on managing silos. For example, the “procure to pay” process is executed by the purchasing, receiving, accounts payable and treasury (cash disbursements) functions. Not only do these functions operate at different levels of the organization, there are critical interfaces or “touch points” among these functions that make the “procure to pay” process work. There must be effective controls over these interfaces, as well as owners of these controls who are accountable for their effective operation.

Certifying officers can benefit from clarifying accountability at all levels and for all key financial reporting processes within the organization. While Section 404 compliance should drive this definition, the ultimate litmus test occurs when management deploys a self-assessment process. To make self-assessment happen, every key control must have a name by it. Gaps (such as when there is no one responsible for executing a control) should be eliminated and overlaps (such as when there are multiple owners of a control) minimized. While easy to say, this kind of clarity is not easy to achieve. Therefore, many companies face situations in which process ownership must be clarified, particularly at the interface points within processes.

Because Section 404 compliance demands attention to execution, it is important to understand that the process ownership aspects of identifying processes and the controls within processes is a significant change management issue. The mere exercise of assigning responsibility can result in redrawing the scope of control responsibilities that previously existed for specific individuals. Thus it is critical that companies consider carefully the transitional organizational structure over the next couple of years to facilitate process owner understanding and acceptance of the scope of their respective responsibilities. Such responsibilities include appropriately testing and self-assessing internal controls to provide assurance that they are operating effectively as designed.

#### *Establish the Appropriate Transitional Organizational Structure*

Certifying officers need an organizational structure that facilitates ongoing compliance with SOA Sections 302 and 404. The structure should emphasize the internal audit function, a group of risk control specialists or both. For example, assume an organization contemplates a lot of changes, or the skill sets, capacity and charter of the internal audit function are not conducive to providing the assistance that process owners need with respect to documenting controls, evaluating change, assessing controls design, testing controls operation and remediation. In such instances, certifying officers should consider creating a risk control function or engaging *risk control specialists*. A risk control group does not execute processes and controls. It may report to and be embedded within the entity’s operations. Alternatively, it may be independent of operations, reporting to the chief financial officer, the chief compliance officer or the chief risk officer. In fact, the change management aspects of eliminating gaps and minimizing overlaps suggest a need for risk control specialists to support process owners over a 12- to 24-month period as they assume responsibility for the ongoing operation of specific controls after the first internal control report is filed. Another factor management may choose to consider is the impact on desired objectivity of the internal audit function.

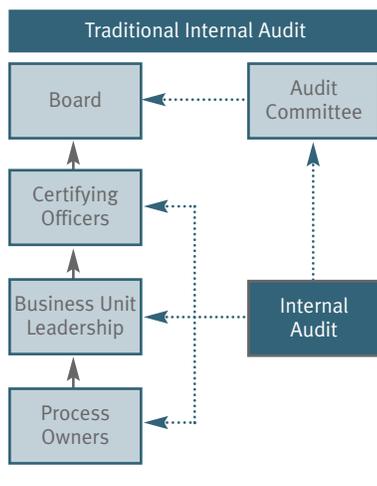
If not much change is contemplated or *internal audit* has strong requisite process, risk and control skill sets, and available capacity, the department may be expanded and deployed and its charter aligned to provide process owners the assistance they need in lieu of a separate risk control group. If it is desired to deploy risk control specialists, such specialists may be organized as a separate division within the internal audit function,

reporting to the chief audit executive, or integrated across the organization. In any event, the internal audit function should align its audit plan with whatever SOA compliance-related monitoring role management has designated for it to fulfill.

Whether embedded or independent, whether reporting to a C-level executive or whether housed within internal audit, risk control specialists play a vital role. Through their knowledge of risk, SOA requirements and business process, they ensure consistent compliance enterprisewide and effectively evaluate the risk at critical interface points between business functions. They infuse process innovations on a periodic basis. They facilitate the identification of metrics that will drive efficiency and effectiveness. In specialty areas like technology, supply chain, commodity trading and treasury, they have access to organizations with which they may co-source personnel with expertise that is not deployed daily in most organizations. Most importantly, they give the process owners assistance from someone they respect, which is vital in the early transitional stage as process owners assume new and expanded responsibilities for controls.

In summary, we suggest three organizational structures that facilitate ongoing compliance with Sections 404 and 302:

### Alternative SOA Compliance Structures



What happens:

- Internal audit tests
- Internal audit consults on control environment whenever possible

Advantages:

- Internal audit focused on financial reporting controls
- Least amount of internal change from an historical perspective (assuming a competent IA function)



What happens:

- Risk control group:
  - Coaches process owners
  - Assists with remediation
  - Tests controls
  - May exist with or without an IA function
- IA independently assesses management’s compliance process

Advantages:

- Consolidated team of risk specialists promotes consistency of control structure
- Maximize appearance of IA objectivity to increase external auditor reliance



What happens:

- Risk control specialists:
  - Are embedded within business units
  - Work directly with process owners on control environment
  - Perform testing
- IA independently assesses management’s compliance process

Advantages:

- Process owners supported close to the source
- Maximize appearance of IA objectivity

There are several factors certifying officers should consider as they evaluate the appropriate transitional organizational structure going forward. Following are five:

- (1) The need to clarify roles and responsibilities of, among others, process owners, operating unit managers and, depending on the selected structure, internal auditors and risk control specialists. As noted earlier, clarity of roles and responsibilities is essential to achieve accountability.
- (2) As the underlying business processes are simplified, focused and automated, there will be greater emphasis on preventive controls (versus detective controls), systems-based controls (versus manual controls) and monitoring. The state of maturity of the company's processes (meaning the extent to which they are defined and managed) will drive the nature of the skills needed. For example, business processes that rely heavily on automated controls will require less testing. However, testing in these environments demand more emphasis on technology-related skills that are not required with respect to processes that rely on manual controls. What's the point? The more efficient and effective the organization's processes, the more they will depend on preventive and automated controls. Consequently, less testing will be necessary and compliance costs will decline over time.
- (3) The extent of change expected within the industry should be considered, e.g., regulatory, consolidation and other developments. The more change, the more help process owners will need.
- (4) A highly competent and objective risk control function (either within internal audit or separate) and a strong internal audit department are management tools recognized by the PCAOB as units whose work the external auditor can rely on to a greater extent than on work performed by others within the company. Going forward, this may be an important factor as companies look for ways to mitigate net audit costs while maintaining audit effectiveness.
- (5) The choice of using internal audit and risk control specialist(s) to advise and coach process owners and perform testing is based upon:
  - the assigned role and responsibilities of process owners; the capabilities;
  - the capacity and cost of deploying process owners; and
  - the capabilities, capacity and cost of deploying internal audit.

If the needs of the organization require expansion of these skill sets, hiring all of the necessary skills may be expensive, particularly in areas of specialized skills such as IT. Therefore, co-sourcing may provide an attractive option to management.

Following is an illustrative summary of the components of infrastructure for ongoing compliance along with examples of illustrative questions when defining the components of infrastructure needed:

### Examples of Components of Infrastructure for Ongoing Compliance



### Examples of illustrative questions when defining the components of infrastructure needed (not intended to be all-inclusive):

Is there a self-assessment process and is it effective?	<ul style="list-style-type: none"> <li>• How do you know?</li> <li>• How far down the organization?</li> <li>• Is it continuous, quarterly or ad hoc?</li> <li>• To whom are results reported?</li> </ul>
Are process owners required to support their assessments?	<ul style="list-style-type: none"> <li>• If so, what guidance is provided?</li> </ul>
Are there constraints in deploying process owners/internal audit?	<ul style="list-style-type: none"> <li>• What are their capabilities?</li> <li>• What is their capacity?</li> <li>• What infrastructure needs to be in place to support the effort?</li> <li>• What is the cost?</li> </ul>
What is internal audit's role with respect to SOA compliance?	<ul style="list-style-type: none"> <li>• What is the organization's view with respect to preserving objectivity?</li> <li>• If separate risk control specialists group, what is role of internal audit?</li> </ul>
Are risk control specialists needed to assist process owners with testing and other activities?	<ul style="list-style-type: none"> <li>• If so, where should they be positioned within the organization?</li> <li>• How do you staff and measure performance?</li> </ul>

In summary, after the first year Section 404 assessment is completed, certifying officers face three realities. First, if there is a significant breakdown in internal control over financial reporting, the company could receive an adverse opinion from the auditor on its internal control. Second, the entity's process owners have a business to run and, due to the day-to-day demands of executing the processes of the business, will be unable to carry the entire compliance load during periods of significant change. Third, there are change management issues that reinforce the need to support process owners, at least on a transitional basis over the next couple of years. Certifying officers need an effective organizational structure that provides them confidence that what is supposed to be done with respect to ongoing 302 and 404 compliance is, in fact, being done and reduces the risk of personal exposure going forward.

#### 184. How does the maturity of a company's business processes affect the sustainability of its internal control structure?

Many companies have work to do with respect to improving their underlying business and accounting processes so they are sound and sustainable. External auditors are likely to press hard for process improvements that will lead to a more sustainable internal control structure during times of change. Continued reliance by management on ad hoc, manual processes will be challenged.

The stakes are high in ensuring there are no material weaknesses because if there is just one, management must assert that internal control over financial reporting is ineffective and the external auditor must issue an adverse opinion. Unfortunately, many material weaknesses do not get reported to management until it is too late to fix them. In many instances management didn't know they existed. This is often due to the lack of maturity of the company's processes. See Question 104 for discussion of the capability maturity model.

Control deficiencies arising from ad hoc processes are often rooted in an overemphasis on manual and detective controls. This captures the essence of what we see in the control deficiencies noted in SEC filings. Companies are reporting material weaknesses (and even significant deficiencies) in internal control over financial reporting, are providing updates on the status of their control-improvement efforts and are disclosing risk factors related to uncertainties in the internal control structure. Over the eight-month period through June 2004, there were over 220 filings regarding control deficiencies and other related issues. Most of these filings were material weaknesses covering a broad range of control deficiencies, with the most common being inadequate financial personnel, revenue recognition, account reconciliations, and ineffective monitoring, review and analysis. Other areas of control deficiencies noted multiple times in the filings included inadequacies in the period-end financial close process. Business processes that are ad hoc or merely repeating are often at the root of these deficiencies. See Question 232 for further discussion.

These dynamics suggest a need for companies to evaluate their key business processes not only to assess control design effectiveness but also to assess process maturity as a measure of sustainability. Companies should not stand pat with their existing processes just because they may be repeatable and passed the assessment test in year one. If processes are heavily dependent on manual and detective controls and on human intervention, the company's internal control structure may not be sustainable during periods of change. Management should target such processes strategically for improvement and for increased scrutiny by internal audit or risk control specialists. While we see many companies remediating their control deficiencies with short-term solutions, we also see them planning for longer-term improvement in key processes that support financial reporting.

#### **185. How do companies “find the value” from Section 404 going forward?**

With respect to Section 404 compliance, certifying officers should ask for value returned just like they do for any other investment or expenditure. Section 302 and 404 provide the “launching pad” to improve processes and the control structure and enhance entity-level monitoring of the financial reporting process. SOA compels public companies to assess weaknesses in their business processes, including their controls over processing information. Because the financial reporting processes for many companies are dependent on people and detective controls and are sometimes inadequately defined, there are potentially strong sources of value extending beyond compliance. For example, there is a significant opportunity to “build in” (versus “inspect in”) quality, optimize costs and compress time within the organization's processes while simultaneously reducing its financial reporting risks.

With improved financial reporting, companies also can augment the governance process by managing reputation and other business risks to protect and enhance enterprise value. Companies with documented processes can compare and benchmark their processes to improve efficiency, articulate clearer job descriptions, better train their people, design improved metrics, eliminate nonessentials, and simplify, focus and automate manual activities.

#### **186. After the initial annual assessment, how does management conduct the quarterly evaluations of those elements of internal control over financial reporting that are a subset of disclosure controls and procedures?**

The SEC's final Section 404 rules state that a quarterly evaluation of internal control over financial reporting is not required. However, the rules in place starting in August 2002 requiring quarterly evaluations of disclosure controls and procedures and disclosure of the 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 39 and 40.
- Management must evaluate changes in the internal control over financial reporting on a quarterly basis in the years following the initial annual assessment, including those controls that are an integral part of disclosure controls and procedures.
- Technology provides the foundation for ongoing process-owner self-assessments of control operational effectiveness at any point in time. Customized questions are developed for use in the self-assessment process based upon input of the key controls identified during the initial annual assessment. See Question 181.
- With process-owner feedback every quarter, management, i.e., the certifying officers, will be positioned to focus on the need for disclosure as a result of change, e.g., changes in processes, systems, operations and other factors, and their impact upon the effectiveness of internal control.

Because the initial annual assessment is process-based, the upward reporting by process owners will truly be a “chain of accountability,” that will contrast with the “chain of certifications” created by many companies requiring their direct reports to individually certify results. In practice, those direct reports have, in turn, often required the same of their direct reports, and so on. The chain of certifications approach, often referred to as “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.

**187. After the initial annual review of control effectiveness is completed, should management assess changes to the company’s risk profile on a quarterly basis?**

Yes. An enterprisewide risk assessment process will help keep the disclosure process fresh. It will identify changes in factors affecting internal controls as well as new and emerging risks for timely action and disclosure. The company also must disclose any change in its internal control over financial reporting that occurred during its most recent fiscal quarter that has materially affected, or is reasonably likely to materially affect, the effectiveness of the company’s internal control over financial reporting.

Because of the impact on financial reporting risk, every company needs a process for identifying environment, operating and other changes that impact the financial statements, other disclosures in public reports and the effectiveness of internal control over financial reporting. Examples of changes requiring evaluation include mergers and acquisitions, divestitures, new innovative business practices, new systems, changes in personnel (including significant early retirement or personnel reduction programs), significant market declines and changes in laws and regulations. The disclosure committee, or an equivalent group of executives, should be charged with the responsibility of monitoring change for purposes of identifying

material information requiring consideration and possible disclosure. Operational risks, new related party transactions, new litigation and other contingencies, emerging strategic risks, new regulatory developments, changing credit and market risks, and risks to reputation and brand image may require disclosure. In addition to considering the implications of change on disclosures required by Section 302, companies also need to look at the implications to the Section 404 assessment and consider the need to re-examine control design and operating effectiveness.

**188. 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 easier and less stressful than the initial annual assessment. All of the required documentation will already exist and the emphasis will be on the effects of change. Most importantly, the independent public accountant’s requirements will be understood. The quarterly evaluations of internal control over financial reporting should also result in issues surfacing with the auditors and the audit committee on a timely basis and serve as a catalyst for timely remediation efforts.

**189. Going forward, what will happen to Section 404 compliance costs?**

As companies transition from the intense project mode of the first year to an ongoing process in year two, they seek to implement a compliance process at costs that are reasonable and sustainable on an ongoing basis. Following is a summary of the cost drivers over the first three years of Section 404 compliance:



**Notes**

(1) Testing scopes must be at least comparable to scopes of independent auditor

(2) A process created in Year Two

(3) Improving quality, reducing costs and compressing time while simultaneously reducing risk through simplifying, focusing and automating manual processes and improving the mix of preventive and detective controls can result in improvements in efficiency and effectiveness that will reduce testing scopes over time

**Role of Management**

**190. 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 be knowledgeable of the public reporting preparation process and the critical “feeds” to that process. 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.

A word of caution: If a company has a disclosure committee, management should ensure that the committee conforms to its charter. Organizing a disclosure committee with a specific charter and then failing to operate that committee in accordance with its charter exposes management to criticism.

### **191. 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.

### **192. What is the role of the Section 404 compliance project steering committee?**

A Section 404 compliance steering committee serves three primary functions:

- First, the committee evaluates and approves the project plan, approves major scoping decisions, reviews major project findings and approves the internal control report.
- Second, it provides overall project oversight and serves as a sounding board for the project team to discuss and, if necessary, resolve major issues when they arise.
- Third, it assists the project team in gaining access to the internal resources needed to successfully complete the project.

The steering committee consists of the certifying officers, operating unit heads or representatives, and leaders of appropriate functions, including the general counsel, human resources, information technology and internal audit. The project sponsor, who may be one of the certifying officers, chairs the committee. The project leader reports to this committee.

The steering committee's sole purpose is to position the project team to succeed. It may meet periodically as scheduled to provide a checkpoint for key decisions and, when necessary, may meet to address significant issues.

### **193. 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.

#### **194. 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.

#### **195. 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 same 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.

#### **196. What communications, if any, are required of management beyond the quarterly executive certifications and annual internal control report?**

Section 302 requires the CEO and CFO to report to the independent accountant (and to the audit committee) the following:

- All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting that are reasonably likely to adversely affect the company's ability to record, process, summarize and report financial information
- Any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal control over financial reporting

#### **197. 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.

**198. 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.

**199. Can management rely on the work of the internal auditors?**

Yes, but not exclusively. We believe results of internal audit testing provide one source of evidence of the effectiveness of internal control over financial reporting. There are, however, other sources that management should also draw from, e.g., process owner self-assessment and entity-level monitoring.

**200. 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 212, 213, 214 and 215.) Although the SEC is very clear on this point in its auditor independence rules, the SEC does permit the auditors to provide recommendations for improvement in internal controls. Ultimately, the responsibility rests with management to make decisions regarding any recommendations, including decisions to implement.

---

## **Role of Internal Audit**

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

The NYSE listing standards provide that "each listed company must have an internal audit function." In its commentary to that requirement, the NYSE states that the internal audit function must provide management and the audit committee with ongoing assessments of the company's risk management processes and system of internal control. A company may choose to outsource this function to a third-party service provider other than its independent auditor.

With certain exceptions, NYSE-listed companies will generally have until the earlier of (a) the company's first annual meeting occurring after January 15, 2004, or (b) October 31, 2004, to comply with the new rules.

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

NASDAQ and AMEX have not addressed the internal audit function in their listing requirements. The revised NASDAQ rules approved by the SEC were silent with respect to an internal audit function. However, the PCAOB points out in Auditing Standard No. 2 that a nonexistent or ineffective internal audit function at a company needing such a function to have effective monitoring and risk assessment is a de facto significant deficiency as well as a possible material weakness. In today's world, companies without an internal audit function will be the exception, regardless of the legal requirements.

In January 2003, The Conference Board Blue Ribbon Commission on Public Trust and Private Enterprise issued its findings and recommendations with respect to auditing and accounting. Under Principle III: Improving Internal Controls and Internal Auditing, one of the “Suggested Best Practices” states:

All companies should have an internal audit function, regardless of whether it is an “in-house” function or one performed by an outside accounting firm that is not the firm that acts as the company’s regular outside auditors.

We believe that all firms should evaluate the need for an internal audit function if they do not have one. We have confirmed with a member of the Blue Ribbon Commission that the term “accounting firm” was not intended to preclude outsourcing to a qualified internal audit services provider.

**203. How should internal audit avoid any conflict-of-interest issues as it plays a value-added role with respect to the Section 404 certification process?**

There are a number of ways. First, internal audit should not have primary ownership over the Section 404 certification process. Second, a trend is emerging where internal audit is reporting directly to the audit committee. For example, in its findings issued in January 2003, The Conference Board Blue Ribbon Commission on Public Trust and Private Enterprise recommended, as a “best practice,” that the chief audit executive or internal audit director 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.

**204. 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.

**205. What changes in internal audit can be expected as a result of Section 404?**

The PCAOB requires the independent auditor to review and assess the impact of the internal auditor’s work and reports. This requirement puts more pressure on the internal auditors to fully execute their audit plans. Internal audit functions not using COSO as a framework for conducting and reporting on audits will have to align with the COSO framework to facilitate integration with Section 404 compliance. The PCAOB emphasis on further developing highly competent internal audit departments will likely bring upon a renewed interest and emphasis in conducting quality assurance reviews to help companies and their audit committees assess the existing internal audit function, what needs to be improved and how to get it done.

The PCAOB also requires the independent auditor to evaluate whether the company’s internal process of reporting deficiencies is timely enough. If not, the auditor must evaluate the deficiencies in the reporting process as to severity. This level of attention on timeliness of reporting can have a significant impact on escalation policy for internal auditors and others in organizations that have not thought about the issue. Timely escalation of significant deficiencies or near significant deficiencies is consistent with and supportive of management’s reporting responsibilities under Section 302.

---

## Role of the Independent Public Accountant

### 206. 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.

### 207. 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 176 for a discussion of the documentation management needs to support the assertions in the internal control report.

### 208. 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.

**209. What does the PCAOB require with respect to the attestation report?**

The PCAOB requires a “single auditor/multiple report” model whereby the external auditor expresses an opinion on management’s assessment of internal control over financial reporting AND on the company’s internal control over financial reporting. An auditor cannot issue Section 404 attestation reports unless it is also auditing the company’s financial statements.

The rationale for this requirement is that it will help the reader understand the delineation between management and the auditor if a material weakness is reported. In this circumstance, the auditor’s opinion on internal control over financial reporting will be an adverse opinion. The auditor’s opinion on management’s assertion will be unqualified (provided management has issued a conclusion in its internal control report that internal control over financial reporting is ineffective).

**210. How will the auditor evaluate management’s assessment of internal control over financial reporting?**

The PCAOB requires the auditor to evaluate the following:

- (a) Whether management properly stated its responsibility for establishing and maintaining adequate internal control over financial reporting
- (b) Whether management used a suitable framework as criteria for evaluating internal control over financial reporting
- (c) Whether management’s assessment, as articulated in the internal control report, is free of material misstatement
- (d) Whether management has expressed its assessment in an acceptable form (See Question 166)
- (e) Whether material weaknesses in the company’s internal control over financial reporting have been properly disclosed, including material weaknesses corrected during the period (See Question 15)

**211. What happens if management decides to forego the documentation and testing necessary to support a conclusion on internal control over financial reporting?**

The PCAOB staff has stated that in these circumstances Auditing Standard No. 2 requires the auditor to communicate in writing to management and the audit committee that the audit of internal control over financial reporting cannot be satisfactorily completed and that he or she is required to disclaim an opinion. The auditor cannot issue an adverse or a qualified opinion because in these circumstances the auditor is precluded from expressing any opinion.

**212. 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.

**213. Can the independent public accountant perform any testing on behalf of the audit client?**

While the work of the independent public accountant does in fact provide yet another checkpoint for management, it should not be the basis for management’s evaluation. The independent public accountant’s responsibility is limited to reviewing the basis for management’s assertions regarding the company’s internal control over financial reporting. Under Section 404 of Sarbanes-Oxley, the independent auditor will be required to issue an opinion that attests to and reports on management’s assertion in the annual internal control report that

the internal control over financial reporting is designed and operating effectively. This assertion is one that management must support with appropriate documentation. Because the independent public accountant will rely on management's supporting documentation, it would be circuitous logic for the independent public accountant's work to be the basis for management's assertions. Further, in Auditing Standard No. 2, the PCAOB adds a new written representation for management to provide to the auditor stating that management did not use the auditor's procedures performed during the audits of internal control over financial reporting or the financial statements as part of the basis for management's assessment of the effectiveness of internal control over financial reporting.

#### **214. 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 215, 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?

Other factors relating to tools and technologies for implementing controls repositories, documenting process maps, facilitating the assessment process and managing overall Section 404 compliance are discussed in Question 63.

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.

**215. 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 are 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/or testing of internal controls, management cannot simply accept responsibility for that work. This would be tantamount to management accepting responsibility for the results of bookkeeping or other services provided by the auditor related to the company's significant accounting records or financial reporting areas. Management must be actively involved in the documentation process.
- Third, the auditor must exercise care to ensure that he or she does not end up auditing his or her own work or provide a service acting in a management capacity.
- Finally, while there is some ambiguity in the final rules that didn't exist during the SEC's open meeting in May 2003, it appears the overriding message is for management and the audit committee to proceed with care when engaging independent accountants to document internal control over financial reporting.

One practical approach to addressing the ambiguity of this issue is to focus on the magnitude of the documentation required to bring a company into compliance. This approach, 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.

## **216. 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. The response to Question 176 provides a high-level checklist of things management must document when supporting the assertions in the internal control report and preparing for the attestation process.

## **217. Can management share interim drafts of the financial statements with the auditor?**

Interim drafts of the financial statements may be shared with the auditor; however, to minimize the risk of the auditor determining that his or her involvement in the process might represent a significant deficiency or material weakness, the PCAOB staff notes that management should clearly communicate three things to the auditor:

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

Due to the changed dynamics in the auditor-client relationship, management should be careful when submitting financial statement drafts to the auditor. If the drafts are incomplete, the auditor may conclude there is a significant deficiency or worse. If specific footnotes are not included in the draft, management should point out the omission as well as the expected timing for completing those footnotes.

Management should also discuss the ground rules with the auditor in advance of submitting financial statement drafts. If there is any uncertainty with respect to the protocol for sharing drafts and management wants advice on financial statement presentation during the report preparation process, they should consider seeking the input of a qualified third party.

## **218. Can management discuss accounting issues with the auditor?**

Yes. The PCAOB staff points out that "a discussion with management about an emerging accounting issue" or "the application of a complex and highly technical accounting pronouncement in the company's circumstances," are examples of "timely auditor involvement" that should not necessarily be an indication of a deficiency in the company's internal control over financial reporting. In these instances, management should proceed with caution until they clearly understand the auditor's ground rules for evaluating the company's internal control over financial reporting in view of these types of discussions. When in doubt, management should consult with third party advisors.

**219. Can management rely on the statutory audit work performed by the external auditor for significant subsidiaries or joint ventures?**

Some argue that the regulatory or contractual environment for statutory audits at specific subsidiaries or joint ventures helps to decrease the inherent risk in their respective financial statements. Therefore, the argument continues, management need not test the controls as much as they would otherwise. These companies appear to have difficulty divorcing themselves from the standalone “full and separate” audits performed by the external auditor because they have relied upon them in the past. The rationale is that the company isn’t really “relying” on the external auditor, but is only considering the audit in evaluating inherent risk.

We recommend that management exercise caution with respect to taking this position for the following reasons:

- As explained in our response to Question 215, the auditor cannot audit his or her own work. Neither can the auditor provide services acting in a management capacity. Evaluating company inherent risk and internal controls, whether at a subsidiary or elsewhere, is a management responsibility.
- As explained in our response to Question 213, the PCAOB requires the auditor to obtain a written representation from management that management did not rely on the external auditor’s audit work.

**220. Can the external auditor use the work of the internal audit function and others for purposes of performing an audit of internal control over financial reporting?**

Yes. The PCAOB provides that the auditor may evaluate the use of the work of others based on three principles – (1) the nature of the controls being tested, (2) the competency and objectivity of the individuals performing the work, and (3) testing the work of others. This approach provides the auditor considerable flexibility by allowing the exercise of professional judgment in deciding the use of the work of highly competent and effective internal auditors (as well as others meeting the Board’s criteria). In fact, the Board refers to “the special status that a highly competent and objective internal auditor has in the [external] auditor’s work,” meaning the auditor will be able to rely to a greater extent on the work of a “highly competent and objective internal auditor” than on work performed by others within the company.

The three principles are discussed further below:

- ***The nature of the controls being tested.*** There are several factors the auditor should consider, as outlined by the Board. For example, the auditor should consider the materiality of the financial reporting elements the control addresses, the degree of judgment required to evaluate operating effectiveness, the pervasiveness of the control, the level of judgment or estimation required in the account or disclosure, and the potential for management override of the control. As these factors increase in significance, the need for the auditor to perform his or her own work increases. As these factors decrease in significance, the auditor may rely more on the work of others. In any event, the auditor is required by the PCAOB to perform the necessary work with respect to the control environment.
- ***The competency and objectivity of the individuals performing the work.*** The auditor will often make this evaluation by obtaining or updating information from prior years. Factors relating to competence include, among other things, education, certifications and performance evaluation. Factors relating to objectivity include (in addition to other matters) organizational status, reporting lines, nature of audit committee access and internal policies with respect to assigning individuals to test areas to which they were recently assigned. With respect to “objectivity,” the intent is to ensure the individuals performing the work can make evaluations with impartiality and that are free of bias.
- ***Testing the work of others.*** This principle is an important part of an ongoing assessment of the competence and objectivity of individuals performing the work. Auditing Standard No. 2 provides for flexibility to the auditor when he or she tests the work of others. For example, testing the work of others in every significant account in which the auditor plans to use their work is not required. When testing the work of others, the Board suggests that the external auditor consider such factors as the sufficiency of

the scope of work to meet the objectives, adequacy of work programs, adequacy of documentation of work performed (including evidence of supervision and review), propriety of conclusions in the circumstances and consistency of conclusions with the results of the work performed.

Section 404 compliance teams will want to make sure they are managing their work appropriately, consistent with the above criteria.

In addition to the above criteria, the PCAOB's standard addresses the sufficiency of the external auditor's own testing. The standard requires that, on an overall basis, the auditor's own work must provide the principal evidence for the auditor's opinion on the company's internal control over financial reporting. The PCAOB's intent is to provide flexibility in using the work of others while also preventing over-reliance on the work of others. The PCAOB staff has indicated that the auditor's testing of the work of others does not "count" toward the auditor's obtaining the principal evidence supporting his or her opinion. However, the auditor's independent testing in areas in which the auditor is using the work of others does "count" for this purpose.

This question is further discussed in Protiviti's *Guide to Internal Audit: Frequently Asked Questions About the NYSE Requirements and Developing an Effective Internal Audit Function*.

**221. Can the independent auditor issue a report to management or the audit committee indicating that no significant deficiencies were noted during an audit of internal control over financial reporting?**

No. The PCAOB precludes the auditor from issuing such representations or reports. Under the standards set forth in Auditing Standard No. 2, an audit of internal control over financial reporting is not designed to detect significant deficiencies. These reports may not be issued because of the potential for misinterpretation.

**222. Will the SEC accept an adverse opinion on internal control over financial reporting?**

Yes. While the SEC will not accept an adverse opinion on the financial statements, the Commission will accept an adverse opinion on internal control over financial reporting. Both the SEC and the PCAOB require the auditor to issue an adverse opinion on the effectiveness of internal control over financial reporting if one or more material weaknesses exists. If management issues an internal control report in the Form 10-K asserting that internal control over financial reporting is ineffective due to the existence of a material weakness, the auditor's issuance of an adverse opinion is, in effect, symmetrical with the conclusion in management's report. However, if the auditor concludes a material weakness exists, but management does not and therefore concludes in its internal control report that internal control over financial reporting is effective, then the auditor would render an adverse opinion on management's assessment. If the auditor issues an adverse opinion on internal control over financial reporting due to a material weakness, the auditor must make mention that the weakness was considered in determining the nature, timing and extent of auditing procedures in connection with the audit of the financial statements and that the report on internal control over financial reporting does not affect the report on the financial statements.

**223. What is required of the independent auditors each quarter?**

In Auditing Standard No. 2, the PCAOB requires the auditor to perform certain procedures on a quarterly basis. These procedures include making inquiries about significant changes in the design and operation of internal control over financial reporting that have occurred subsequent to the preceding annual audit or prior review of interim financial information. The auditor must evaluate the implications of any changes noted and determine whether such changes materially affect, or are reasonably likely to materially affect, internal control over financial reporting. The auditor is not required to render a report on a quarterly basis.

This is the same type of involvement the auditor has with respect to the quarterly 10-Qs. Note also that the definition of a control deficiency incorporates the potential for misstatements in interim financial statements.

**224. Can the same audit firm issue an opinion on internal control over financial reporting of a user organization and also issue the SAS 70 letter pertaining to a service organization to which the user organization has outsourced a significant process?**

In situations where management has outsourced certain functions to third-party service provider(s), management retains responsibility for assessing the controls over the outsourced operations (see Question 88). However, the SEC staff has noted that management would be able to rely on a Type 2 SAS 70 report even if the auditors for both companies were the same. In this situation, the management of the service provider engaged the audit firm and that management is independent of the user organization's management. On the other hand, the staff also noted that if the management of the user organization were to engage its audit firm to also prepare the Type 2 SAS 70 report on the service organization, management would not be able to rely on that report for purposes of assessing internal control over financial reporting. In any event, management is still responsible for maintaining and evaluating, as appropriate, controls over the flow of information to and from the service organization.

---

## **Role of the Audit Committee**

**225. With respect to the financial reporting process and internal control over financial reporting, what is expected of the audit committee?**

The audit committee oversees the financial reporting process and internal control over financial reporting. This is an important role. The PCAOB has stated that ineffective audit committee oversight is at least a significant deficiency and a strong indicator of a material weakness.

Because board and audit committee oversight is an element of the control environment, according to COSO, the independent auditor is required to evaluate audit committee oversight effectiveness as an integral part of his or her assessment of the control environment and monitoring controls. This requirement of the auditor does not supplant the overall responsibility of the board of directors to evaluate audit committee effectiveness. According to the PCAOB, the external auditor's evaluation must consider:

- Independence of audit committee members
- Clarity of committee responsibilities, as articulated in the committee charter, and the extent to which the audit committee and management understand those responsibilities
- Extent of involvement with the external auditor
- Extent of involvement with the internal auditor
- Extent of direct and independent interaction with key members of financial management, including the chief financial officer and chief accounting officer
- Degree to which difficult questions are raised and pursued with management and the auditor, including questions that indicate an understanding of the critical accounting policies and judgmental accounting estimates
- Time devoted to control issues
- Level of responsiveness to issues raised by the auditor, including those required to be communicated by the auditor to the audit committee (for example, significant deficiencies)

Other examples of factors the board, audit committee and management – but not the outside auditor – should consider when evaluating committee effectiveness include:

- Committee compliance with SOA Section 301

- Presence of one or more financial experts on the committee
- The nomination process (i.e., are committee members selected using an outside search firm or equivalent process based upon desired skill sets?)
- Committee compliance with other provisions set forth in the applicable listing requirements

Although the external auditor may not consider the above factors in his or her evaluation, the board should.

**226. 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 deficiencies. 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.

**227. What questions are audit committees asking with respect to Section 404 compliance?**

With respect to Section 404, the line of questioning has increased substantially as audit committee members get more involved in the process. Some of the questions audit committee members have told us they asked at the inception of the project 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 prepare for the Section 404 requirement? Is it being planned in an orderly manner 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 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 audit of internal control over financial reporting 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 30 percent of the annual audit fee, does that mean it will take 30 percent of the time the annual audit takes? If not, how much of this fee is a premium for assumption of risk?
- 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 last year's 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?

As the Section 404 compliance project progresses, the additional questions audit committee members are asking include:

- a) How will the auditor evaluate the effectiveness of the audit committee's oversight with respect to the financial reporting process and internal control over financial reporting, and what is the current status of these new requirements? Is there anything the committee should be doing that historically it has not?
- b) Are there any disagreements between management and the auditor with respect to management's approach to assessing internal control over financial reporting?
- c) Is management satisfied that the company's internal reporting policies are sufficient to timely surface control deficiencies that could potentially be significant deficiencies?
- d) Has management decided on the company's testing standards? If so, how do they compare with the testing planned by the external auditor and is the external auditor satisfied that management's testing plan is sufficient for purposes of making an assessment of internal control over financial reporting?
- e) What is management doing to prepare for ongoing compliance with Sections 302 and 404 after the initial internal control report is filed?
- f) As a practical matter, when does the controls testing work for most companies have to be completed in order to have adequate time to do remediation work to cure potential defects?
- g) If the auditor issues an adverse opinion on internal control over financial reporting, how will that report affect the auditor's opinion on the financial statements? What are the ramifications under the SEC's rules? Will this result in a company not being able to sell securities in an SEC registered offering?
- h) Is there any chance the SEC will delay the deadline on Section 404? Is it possible the SEC may delay the auditor attestation, while requiring management to issue an internal control report?

---

## Impact on Sections 302 and 906

### 228. What is the impact of the Section 404 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.

#### **229. 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 228. 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.

#### **230. 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.”

#### **231. Why are companies reporting control deficiencies that are not material weaknesses?**

During the eight months ended June 30, 2004, approximately one percent of U.S. public companies filing reports with the SEC have reported disclosures regarding internal control matters. Approximately 75 percent of these filings involve reporting and/or remediation of material weaknesses in internal control over

financial reporting. The remaining filings report control deficiencies and other matters not involving material weaknesses. This is due to companies being required to disclose change that has materially affected, or is reasonably likely to materially affect, internal control over financial reporting. To illustrate, some companies have reported changes in their business, such as: rapid growth through acquisitions and market conditions; increased complexity of transactions; large and complex acquisitions; integration of legacy accounting and information systems, and other major developments. Human resources matters have also been a point of focus for disclosure of change. For example, some companies have disclosed significant reductions in the workforce. Others have disclosed the turnover of key finance personnel, such as turnover at the chief financial officer position and layoffs of accounting personnel, which significantly reduced the number and experience level of accounting staff. One company disclosed the transition of a large number of general and administrative personnel from one facility to another facility. Still other companies have reported on their remediation of significant deficiencies or provided an update on the resolution of previously disclosed deficiencies, while others have disclosed uncertainties with respect to the internal control environment as a “risk factor.”

### **232. What are the common types of control deficiencies being reported by public companies?**

For the eight months ended June 30, 2004, *Compliance Week* reported 225 filings related to matters pertaining to internal control over financial reporting. After eliminating redundancies for the same company filing multiple times, we have noted the following:

- The four most common deficiencies cited were (1) adequacy of financial personnel, (2) revenue recognition, (3) account reconciliations, and (4) adequacy of monitoring, review and analysis. These areas have dominated the reporting from the very beginning. Reporting of segregation of duties and inventory accounting (e.g., costing, relief, valuation and other matters) were tied for the fifth most common deficiency cited.
- Other frequent control deficiencies include “unsupported or unauthorized disbursements and transactions” (including unsupported journal entries), deficiencies in the control environment and inadequacies in the period-end financial close process. In addition to these common areas of deficiencies, there were numerous control deficiencies cited relative to assertions inherent in specific financial reporting accounts and disclosures.
- Other areas of control deficiencies noted multiple times in the filings for the eight month period ended June 30, 2004 included (1) reliance on ad hoc, manual processes, (2) deficiencies in the general IT control environment (security administration, change management, disaster recovery, application and data controls and other areas), (3) noncompliance with or undocumented accounting policies, (4) control issues resulting from mergers and acquisitions, and (5) control issues relating to income tax accounting.

Since June 2004, subsequent SEC filings related to internal control matters through the date this publication went to print, did not provide a significantly different picture.

### **233. What are the demographics of companies reporting control deficiencies?**

During the eight months ended June 30, 2004:

- The five industries reporting the most control deficiencies were (in descending order from most frequent to least frequent) technology, manufacturing, services, energy and utilities, and telecommunications. These five sectors comprise three-fourths of the filings related to internal control matters during the eight-month period ended June 30, 2004.
- Companies with revenues of less than \$100 million submitted almost 60 percent of the filings.
- Companies falling into the category of revenues of over \$100 million but less than \$1 billion submitted almost 25 percent of the reports.

- Companies that had restated previously issued quarterly and/or annual financial statements submitted about 10 percent of the filings.

---

## Accelerated Filing Requirements

### 234. 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 were originally scheduled to be phased in over three years. Through the phase-in period, the annual report deadline will be reduced from 90 days to 60 days, 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.

Prior to this publication going to print, the SEC proposed to postpone the final year of the accelerated filing requirements phase-in period to enable accelerated filers to maintain their focus on complying with Section 404. The following table illustrates the extended phase-in period, taking into account the SEC's proposed one-year delay:

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	75 days after fiscal year-end	40 days after fiscal quarter-end
December 15, 2005	60 days after fiscal year-end	40 days after fiscal quarter-end
December 15, 2006	60 days after fiscal year-end	35 days after fiscal quarter-end

The purpose of the phase-in period was to allow a transition for companies to adjust their reporting schedules and to develop efficiencies to ensure that the quality and accuracy of reported information would not be compromised. The Section 404 compliance process has complicated this transition. Companies and individuals have communicated this concern to the SEC and to Congressional Committees. Accordingly, the Commission proposes to delay the third and final phase of the transition so that the deadline for accelerated filers for the next annual report would remain at 75 days for an additional year and, for the three subsequently filed quarterly reports, would remain at 40 days after fiscal quarter-end. In effect, the second-year deadlines of the phase-in period would remain in place for an additional year. The proposal further provides that the accelerated filing phase-in period would resume for reports filed for fiscal years ending on or after December 15, 2005, when an accelerated filer would have to file its annual report within 60 days after year-end. Thereafter, the company would then have to file its next three quarterly reports within 35 days after fiscal quarter-end (during 2006 for calendar year reporting companies, for example). At the end of Year Four of the extended transition period, the accelerated filing phase-in will be complete, with the 60-day and 35-day deadlines remaining in place for accelerated filers for all subsequent periods.

### 235. 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

November 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?”

The purpose of the public float test, according to the SEC, is to provide a reasonable measure of company size and market interest. This definition of accelerated filers excludes nearly half of all publicly traded companies.

**236. 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.

**237. If a calendar year reporting company meets the requirements as an accelerated filer for SEC reporting purposes as of December 31, 2003, what is its Section 404 compliance status if its market cap subsequently falls below \$75 million as of June 30, 2004?**

The company must comply beginning with the filing of its first 10-K for a fiscal year ending on or after November 15, 2004. Assume a calendar year reporting company files its 10-K for 2003 as an accelerated filer. Assume further its market cap is below the \$75 million benchmark as of the end of its second quarter ended June 30, 2004. Rule 12b-2 of the Exchange Act defines the term “accelerated filer” to mean an issuer after it first meets the four conditions listed in Question 236 as of the end of its fiscal year. Once the company became an accelerated filer as of December 31, 2003, it will remain an accelerated filer, unless it becomes eligible to use Forms 10-KSB and 10-QSB for its annual and quarterly reports. In other words, assuming that the company does not become a small-business issuer, even if its market cap as of June 30, 2004, were to drop below \$75 million, it remains an accelerated filer. The SEC staff reinforces this point by observing that

Exchange Act Rule 12b-2 provides that “a registrant that is not already subject to accelerated filing should determine whether it is an accelerated filer at the end of its fiscal year, based on the market value of its public float of its common equity as of the last business day of its most recently completed second fiscal quarter.”

---

## Private Companies and Initial Public Offerings

**238. 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.

**239. 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 a 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 July 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 July 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 236 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. If the same company were to go public during 2005, 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. Finally, under the current SEC rules, a calendar year reporting small-business issuer going public during 2005 must comply with the annual internal control reporting requirements when it files the Form 10-K for the year ended December 31, 2005.

**240. When must a calendar year reporting company comply with Section 404 when it goes public and has an initial capitalization below the accelerated filing floor?**

As noted in Question 26, if the company goes public during 2004, it will not be an “accelerated filer;” therefore, it will not be required to comply with Section 404 until the filing of its first 10-K for a fiscal year ending on or after July 15, 2005. If the company goes public during 2005, it must comply with Section 404 in 2005 whether it is an accelerated filer or not. In other words, size does not matter once the transition period is over (as discussed in Question 239).

**241. 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.

**242. 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.

**243. Assuming a June 30 year-end company goes public on September 30, 2004, is the first Section 302 certification required to be included in the first 10-Q for the quarter ended December 31, 2004, or will the company be required to certify as of September 30?**

Section 302 applies to periodic reports under the Exchange Act of 1934 and is not applicable to registration statements filed under the 1933 Act. Therefore, the first 10-Q (or the 10-K, if it is the first report filed after going public) is when the executive certification requirement kicks in. In this case, the certification would first be filed in the 10-Q filed for the quarter ended December 31, 2004. With respect to these and other similar reporting matters, we advise companies to consult with counsel.

---

## U.S. Nonaccelerated Filers

### 244. Is Section 404 applied differently to smaller companies?

Many smaller companies generally have less complex processes and therefore less complex and formalized controls. Small and medium-sized companies often do not have the formal control structure found in larger companies. However, the lack of the formality found in larger, more complex companies does not provide relief for weak controls. The concept of control activities in a small company is the same as in a larger one, although the formality of the controls may be different and management (including the CFO) may be more personally involved in the company's processes.

The PCAOB reported that it attempted to evaluate the potential for reducing compliance costs for smaller companies. The Board concluded that Section 404 is intended to improve reliability of financial reporting for ALL public companies, and there should be no exceptions made for small and medium-sized companies. Therefore, the Board decided to remove an appendix previously included in the proposed standard and to refer to the COSO framework, which includes specific reference to the application of internal control over financial reporting to smaller entities. One of the issues the Board faced was that some commenters expressed the views that the appendix included in the proposing release was too accommodating to smaller and medium-sized companies and could in fact provide incentives to have less effective internal control and potentially increase fraud risk at those entities. For this reason, the Board found that striking an appropriate balance was "particularly challenging."

In essence, the Board decided it was not its job to develop internal control criteria for small and medium-sized companies, leaving the task to COSO or some other appropriate body. Therefore, it currently is up to the auditor to exercise judgment as to the nature of the internal control over financial reporting that must be in place at small to medium-sized companies in order to express an opinion that internal control over financial reporting is effective. During the open meeting, the Board stated it would be following up on Section 404 implementation at small to medium-sized companies in order to assess progress and the associated costs.

### 245. Can public companies rely on their external auditor to compute the tax provision and reserves included in their financial statements?

No. Public companies need to have someone in-house who at least understands the basic financial reporting principles relating to the tax area in order to ensure proper reporting, including the related risks and controls over the completeness and accuracy of the data used in the calculation and the reasonableness of the computed tax provisions and reserves. If companies have historically used their auditors to determine their quarterly and/or annual tax provisions, they should reevaluate this practice given the SEC's independence rules. As discussed in Question 215, the Commission has made it clear the auditor cannot audit his or her own work.

---

## Foreign Filers and Locations

### 246. Are foreign filers subject to the Section 302 executive certification requirements?

Foreign private issuers filing Forms 20-F and 40-F are not subject to quarterly reporting requirements.

### 247. Based on experiences to date by U.S. accelerated filers, what are the lessons for foreign filers who have just begun their compliance efforts?

Some of the key lessons relating to planning, organizing and managing the project are as follows:

- For most accelerated filers, the Section 404 compliance effort is a major project effort requiring a PMO. See Question 49.

- Top management support is vital. It is difficult to succeed without it.
- Engage unit managers and process owners (both in-house and outsourced) by getting them involved and holding them accountable.
- Take charge of the project. Avoid such pitfalls as managing the project at too low a level within the organization, letting the project team get lost in irrelevant details and allowing key scoping decisions to remain unaddressed too long.
- Don't ignore the clock. This is a huge effort. A study by Financial Executives International reports an average of 14,000 internal hours for companies with annual revenues of \$1 to \$5 billion. So start early if you can.
- Communicate up, down and across the organization.
- Involve the external auditor at appropriate points during the process. Work with them, understand their expectations and timing requirements, conduct periodic checkpoints and plan to give the auditors sufficient time. Recognize management must represent they did not use the auditor's procedures performed during the audit process.

Some of the key lessons relating to executing the project are as follows:

- Answer key scoping questions early – which financial reporting elements, which locations and units, which processes and which systems?
- As early as possible in the process, assess your entity-level controls, evaluate your general IT controls and plan on making fraud explicit in the assessment.
- Focus on the priority financial reporting elements, assertions and risks. Link the priority elements, processes, key assertions, risks and controls. Integrate IT risks and controls with the Section 404 assessment.
- Inventory the company's existing controls documentation and use process maps to provide the most effective "walkthrough." Make sure your process owners are prepared for the auditor walkthroughs.
- Pay attention to details. Read the PCAOB standard and document your roadmap for complying with the standard. Apply the COSO framework (or some other suitable framework) as it is designed. Expect the initial annual assessment to be a learning experience. Expect to encounter "bumps" along the road; the first year is proving to be a challenge – for everyone.
- Define the testing plan and "rules of engagement" up front. Filter the controls to test, define the "failure conditions," articulate testing documentation protocols and decide what to do when failure conditions are encountered. Vary testing scopes according to frequency of the control, test at least to the same degree that the auditor would, use appropriate sample sizes to obtain a high level of assurance, use competent and objective evaluators, and don't forget refresh testing updates close to year-end.
- Consider the nature and extent of remediation timely. Begin the evaluation process and tackle significant design deficiencies as soon as practicable. Thoughtfully remediate operating deficiencies. Be sure to retest remediated controls.
- When documenting the assessment, address the points outlined in the response to Question 176.

**248. Must the Section 404 documentation prepared in countries outside the United States be presented in English?**

There is no SEC or other requirement to prepare all internal control documentation in English. For most companies, such a requirement would be an unnecessary burden. Typically audit firms are able to refer work to their offices with the language skills necessary to do the required work. The capability of local

management to effectively assess and conclude on the effectiveness of the processes and controls is a factor when determining whether translation is necessary. The rigor and consistency of the company's assessment approach and the tools and training supporting it are also a consideration.

If translation is deemed necessary, then perhaps only certain aspects of the documentation would need to be translated based upon importance. For example, depending on significance, an overall memorandum and selected summary schedules could be prepared in English to address matters of importance to registrant management. In addition, matters requiring consolidation often require translation to the language of the reporting entity.

Foreign locations must be put in perspective as to size and risk when deciding how much of the documentation, if any, must be in English. The key is to make sure an emphasis on translation does not undermine the quality of the assessment or the implementation of controls. Indiscriminate emphasis on translation could present increased risk. For example, in countries like Japan, where the language does not translate well into English, translation would complicate the process and make it more difficult to ensure that the right risks are identified and the right controls are in place. It would also potentially limit the number of people who could be involved, as in some countries, few of the nationals may speak English or, at a minimum, be able to speak and write the language fluently, especially in a business context. This issue applies to other countries as well due to the complexities of evaluating internal control, which is difficult enough in English. Therefore, it may make more sense for multinational companies to use the language of the local country for documentation purposes, unless English is usually spoken in the business environment, e.g., Singapore.

As with so many of these types of issues, early consultation with a company's external auditor is strongly advised. This issue also underscores the value of a company's internal audit function having the appropriate language skills or being able to access a co-sourcing provider who can deliver qualified internal audit or risk and control specialists fluent in selected local languages.

---

## Other Specific Matters Relating to PCAOB Auditing Standard No. 2

### 249. 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 reported it planned to spend \$36.6 million, with a \$50 million annual budget once it reaches full staffing. The PCAOB has offices in Washington, D.C. and New York, and expects to have approximately 300 employees eventually. 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.

On March 9, 2004, the Board issued Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*. The Board's assessment process, as outlined in the standard, is based on the COSO framework, is based on "reasonable assurance", is risk-based and is focused on financial reporting assertions.

### 250. What is the impact of the PCAOB's conclusion that business continuity and contingency planning are not part of the audit of internal control over financial reporting?

In Auditing Standard No. 2, the PCAOB asserts that business continuity and contingency planning do not affect a company's current abilities to initiate, authorize, record, process or report financial data. Therefore, the auditor need not consider this area in the audit of internal control over financial reporting.

We do not believe the Board intended to cast judgment on management's business case for exercising its prerogative to protect the organization's information assets. If management has decided to implement a business-continuity plan and business-impact analysis because of a conclusion that it is the prudent thing to do based upon the criticality of IT assets to the business, they should proceed as planned. In light of the events of September 11, 2001, business interruption is clearly an important business risk to be managed.

More importantly, if a significant, priority system goes down and a company loses large amounts of data critical to financial reporting because of the absence of effective disaster and backup recovery capabilities, there will be a lot of explaining to do if the lost data results in missed reporting deadlines or causes the certifying officers to refuse to sign certifications because critical information isn't available. Systems that are vital to the sustainability of the business may also have significant financial reporting implications. 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 also 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.

**251. What is the PCAOB's view on the applicability of safeguarding of assets to an assessment of internal control over financial reporting?**

In Auditing Standard No. 2, the Board clarified that the focus of safeguarding of assets was on "those policies and procedures providing reasonable assurance regarding the prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements." The Board stated that if a preventive control is not in place to safeguard assets, but a detective control is in place to prevent a misstatement of the financial statements, there is not a material weakness or significant deficiency, as those terms are defined. The Board also developed an appendix on safeguarding of assets in the final standard that was based on the COSO addendum dealing with the subject.

**252. Will the PCAOB issue further guidance regarding the independent public accountant's attestation requirements and standards? If so, when?**

It is reasonable to expect the PCAOB to issue further guidance in the future. In fact, the Board issued its *Staff Questions and Answers* on June 23, 2004, which Protiviti considered when updating this publication. At the time this publication went to print, there were other implementation issues requiring significant judgment. It is possible the PCAOB may provide further guidance to address one or more of them. Some of these issues are as following:

- The depth and breadth of management's documentation of controls;
- The extent of management's tests of controls operating effectiveness;
- Applying the guidance on multiple locations or business units to achieve "a large portion" coverage;
- Applying the guidance on multiple locations or business units to address circumstances when there are a large number of locations of similar size or risk; and
- Addressing conversions to new systems and major modifications and upgrades of systems close to year-end.

In addition, notwithstanding the PCAOB's efforts to clarify the subjective distinction between insignificant control deficiencies and significant deficiencies and between significant deficiencies and material weaknesses, it is possible the Board will issue further clarification as experience is gained applying the criteria set forth in Auditing Standard No. 2.

(For reports on recent PCAOB announcements, guidelines and activities, please visit [www.pcaobus.org](http://www.pcaobus.org).)

---

## 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](http://www.protiviti.com).)

**COSO** – The Committee of Sponsoring Organizations of the Treadway Commission. See Question 41 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 249 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 18 for more information.

**Section 404** – Refers to Section 404 of the Sarbanes-Oxley Act, which addresses internal control over financial reporting.

**Section 906** – Refers to Section 906 of the Sarbanes-Oxley Act, which requires an executive certification stating that a company’s periodic report containing its financial statements fully complies with the requirements of Section 13(a) or 15(d) of the Exchange Act, and that the information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer. See Question 19 for more information.

**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 a leading provider of independent internal audit and risk consulting services. We help clients identify, assess and manage operational and technology-related risks encountered in their industries, and assist in the implementation of the processes and controls to enable their continued monitoring. We also offer a full spectrum of internal audit services focused on bringing the deep skills and technological expertise to enable business risk management and the continual transformation of internal audit functions.