1-1-2004

PCAOB auditing standard no. 2 : a guide for financial managers

Michael Ramos

Lori West

Public Company Accounting Oversight Board

AICPA Audit and Accounting Practice Aid Series

PCAOB Auditing Standard No. 2: A Guide for Financial Managers

American Institute of Certified Public Accountants

AICPA

PCAOB Auditing Standard No. 2: A Guide for Financial Managers

AICPA

AICPA Audit and Accounting Practice Aid Series

PCAOB Auditing Standard No. 2: A Guide for Financial Managers

Written by
Michael Ramos

Edited by
Lori West
Technical Manager
Accounting and Auditing Publications

American Institute of Certified Public Accountants

AICPA

Notice to Readers

This publication, *PCAOB Auditing Standard No. 2: A Guide for Financial Managers*, was developed by an independent consultant and the staff of the AICPA. Its contents represent the opinions of the author. It is written for financial managers charged with evaluating their company's internal control as required by Section 404 of the Sarbanes-Oxley Act of 2002 and for the CPAs in public practice who provide them with consulting services. This publication has not been approved, disapproved, or otherwise acted upon by any senior technical committee of the AICPA and therefore its contents have no official or authoritative status

1 2 3 4 5 6 7 8 9 0 AAP 0 9 8 7 6 5 4

Table of Contents

Acknowledgments

The creation of this Practice Aid was truly a team effort, and I would like to thank all those involved. Linda Cohen and Bob Durak recognized the need for the publication and supported me throughout my efforts. Lori A. West diligently edited these materials and made them suitable for print. Judith Sherinsky provided invaluable feedback on the technical content. This Practice Aid originally was part of a CPE video course, and I am indebted to the Professional Development—Vision & Video Products Team at the AICPA for their contributions to the book: Alan Reich, Vince Sarno, and Joanne Flood.

About the Author

Michael Ramos is the author of numerous accounting and auditing technical publications and training courses. His most recent Practice Aid is *How to Comply with Sarbanes-Oxley Section 404: Assessing the Effectiveness of Internal Control.*

Introduction

The series of business failures that began with Enron in late 2001 exposed serious weaknesses in the system of checks and balances that were intended to protect the interests of shareholders, pension beneficiaries and employees of public companies—and to protect the confidence of the American public in the stability and fairness of U.S. capital markets. . . .

Congress responded to the corporate failures with the Sarbanes-Oxley Act of 2002, creating a broad, new oversight regime for auditors of public companies while prescribing specific steps to address specific failures and codifying the responsibilities of corporate executives, corporate directors, lawyers and accountants. . . .

Failures in internal control, particularly over financial reporting, were among the specific concerns addressed by Congress in the Sarbanes-Oxley Act. . . .

The bottom line for Congress, and for the PCAOB, is the reliability of the company's financial statements—statements relied on by shareholders, management, directors, regulators, lenders, investors and the market at large. . . .

In the simplest terms, investors can have much more confidence in the reliability of a corporate financial statement if corporate management demonstrates that it exercises adequate internal control.

The Public Company Accounting Oversight Board
Introduction to Auditing Standard No. 2

Management's Requirement to Report on Internal Control

In July of 2003, as directed by Section 404 of the Sarbanes-Oxley Act of 2002, the Securities and Exchange Commission (SEC) adopted rules requiring registrants to include in their annual reports a report of management on the company's internal control over financial reporting. The SEC final rule, *Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports*, states that the internal control report must include:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company
- Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year
- A statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting
- A statement that the registered public accounting firm that audited the company's financial statements included in the annual report has issued an audit report on management's assessment of the company's internal control over financial reporting

The SEC's rules included guidance on the form and content of management's report, but provided only the following general guidance on the procedures that management should follow to assess internal control:

- A company must maintain evidential matter, including documentation, to provide reasonable support for management's reporting.
- Management must perform procedures sufficient both to evaluate the design and to test the operating effectiveness of internal control over financial reporting.
- Controls subject to management's assessment of internal control include but are not limited to:
  - — Controls over initiating, recording, processing, and reconciling account balances, classes of transactions and disclosure and related assertions included in the financial statements.
  - — Controls related to the initiation and processing of nonroutine and nonsystematic transactions.
  - — Controls related to the selection and application of appropriate accounting policies.
  - — Controls related to the prevention, identification, and detection of fraud.
- Inquiry alone generally will not provide an adequate basis for management's assessment.
- Management should document its assessment of internal control effectiveness to 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.
  - — The results of the tests were appropriately considered.

Although this guidance was helpful, the SEC specifically refrained from specifying the method or procedures to be performed by management in its evaluation of internal control. More detailed guidance became available when the Public Company Accounting Oversight Board (PCAOB) issued its standard relating to the auditor's requirements for auditing management's report on internal control.

Introduction to PCAOB Auditing Standard No. 2

In June 2004, the SEC approved PCAOB Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, PC sec. 140). This standard requires auditors for the first time to conduct two audits of their publicly traded clients: the traditional audit of financial

statements and a new audit of internal control. The standard provides definitive guidance for independent auditors on the performance of their audit of internal control.

Auditing Standard No. 2: Not Just for Auditors

The Auditing Standard also will have a significant effect on the way in which company management conducts its own required assessment in internal control effectiveness. For example, the standard:

- Requires auditors to assess the quality of the company's self-assessment of internal control. In providing this guidance, the standard describes certain required elements of management's process that must be present for the auditor to conclude that the process was adequate.
- Requires auditors to assess the adequacy of the company's documentation of internal control. The standard goes on to provide definitive guidance on what management's documentation should contain for the auditor to conclude that it is adequate. Lack of adequate documentation is considered a control deficiency that may preclude an unqualified opinion on internal control or may result in a scope limitation on the auditor's engagement.
- Allows the auditor to rely on the work performed by the company in its self-assessment process to support his or her conclusion on internal control effectiveness. However, to rely on this work to the maximum extent, certain conditions regarding the nature of the work and the people who performed it must be met.
- Establishes the definition of a *material weakness* in internal control. To conclude that internal control is effective, management should have reasonable assurance that there were no material weaknesses in internal control as of the reporting date.

Subsequent to the approval of the Auditing Standard, both the PCAOB and the SEC released documents of answers to frequently asked questions. These documents set forth the PCAOB and SEC staff's opinions and views on certain matters. Although both the PCAOB and the SEC point out that these opinions and views do not represent official "rules," you should be prepared to justify any departure from the answers to questions discussed in these documents. Pertinent guidance from both of these documents has been included in this Practice Aid.

This Practice Aid is designed for company management and those under their supervision who are involved in the company's self-evaluation of internal control effectiveness. This Practice Aid will walk you through all of the key requirements of the standard that have a bearing on how you should conduct your evaluation. It will provide you with insight and analysis on what these requirements mean. This Practice Aid covers:

- Management's responsibilities relating to the company's self-assessment of internal control and the related audit

- How the company may and may not work with its auditors to carry out its responsibilities
- The performance requirements for each major phase of the assessment of internal control, including:
  - — Planning the scope of the work
  - — Documenting internal control
  - — Evaluating the design effectiveness of internal control
  - — Testing the operating effectiveness of internal control
  - — Assessing internal control deficiencies

Relationship to the Authoritative Standard

This Practice Aid contains many excerpts taken directly from the Auditing Standard and the answers to frequently asked questions documents prepared by the staffs of the SEC and PCAOB. However, the Practice Aid does not include the complete standard or the answers to frequently asked questions. This Practice Aid is *not* a substitute for reading the actual standard or frequently asked questions. Before completing your self-assessment, and possibly in conjunction with reading this Practice Aid, you should obtain and read the actual, authoritative text and related implementation guidance.

PCAOB Auditing Standard No. 2 is quite lengthy. It includes several appendixes, including a background and basis for conclusions in Appendix E. When reading the standard, you should note that all appendixes are an integral part of the standard and carry the same authoritative weight as the actual standard itself.

You can download the Auditing Standard directly from the PCAOB Web site at http://www.pcaobus.org/pcaob_standards.asp (Release 2004-1).

The answers to frequently asked questions can be found at:

- SEC staff *Management's Report on Internal Control Over Financial Reporting and Disclosure in Exchange Act Periodic Reports: Frequently Asked Questions;* http://www.sec.gov/info/accountants/controlfaq0604.htm
- PCAOB *Staff Questions and Answers: Auditing Internal Control Over Financial Reporting;* http://www.pcaobus.org/documents/Staff_Q_and_A/Staff_Internal_Control.pdf.

When reading this Practice Aid, please note the following.

- References to paragraphs in PCAOB Auditing Standard No. 2 that are in **boldface type** indicate that the information that follows was taken directly from the standard. If paragraph references are in regular text, the information that follows was paraphrased.
- PCAOB Auditing Standard No. 2 includes guidance labeled "Note" within the body of the text. These notes and the footnotes to the standard are considered to be an integral part of the standard and carry the same authoritative weight as any other information in the standard. In this Practice Aid, we have retained the PCAOB's label, "Notes," clearly distinguishing them from this Practice Aid author's observations.
- This Practice Aid uses the phrase "Auditing Standard" to refer to PCAOB Auditing Standard No. 2. When we make references to other auditing standards, those references are clearly labeled.
- At the end of the Practice Aid are appendixes. Most of the materials are reproduced from the Auditing Standard and are included here for your convenience.

CHAPTER 1: ROLES AND RESPONSIBILITIES OF MANAGEMENT AND THE EXTERNAL AUDITOR

BACKGROUND OF AUDITING STANDARD NO. 2

Overview of Sarbanes-Oxley Section 404

The Sarbanes-Oxley Act of 2002 was created in response to a series of business failures, beginning with Enron in 2001. Failures in internal control, particularly over financial reporting, were among the specific concerns addressed by Sarbanes-Oxley, and Section 404 of the law, which requires:

- *Company management* to issue a report on internal control that—
  1. States its responsibility for establishing and maintaining adequate internal control over financial reporting; and
  2. Contains an assessment, as of year-end, of the effectiveness of the company's internal control structure over financial reporting.
- The company's *external auditors* to audit and report on management's internal control assessment and on the effectiveness of the company's internal control.

Observations About the Requirements

- The law requires two separate evaluations of your company's internal control: yours and the external auditors'. In some cases, there will be a duplication of effort. Certain aspects of internal control will be tested twice. In other areas, the external auditors will be able to rely on your work to support their own conclusion on internal control. Determining the extent to which your work can directly benefit the audit and, on a broader level, the extent of cooperation that is possible between you and your external auditors will be significant considerations as you undertake your assessment.

- Note that your assessment of internal control effectiveness is "as of" year end, which is different from an assessment of effectiveness throughout the period. The as-of reporting requirements have significant affect on how your audit of internal control is performed. For example, you will probably perform some of your tests in advance of year end. But to report on the effectiveness of internal control as of year end, you will be required to perform procedures to obtain evidence that the conclusions you reached at an interim date remain valid at the reporting date. The issues that result from the as-of reporting requirements will be highlighted in subsequent chapters of this Practice Aid.

- It is common for companies with international operations to have a lag in reporting the financial results of certain foreign subsidiaries for financial reporting purposes. For example, a company may consolidate the operations of a foreign subsidiary with a November 30 year end, rather than the December 31 year end of the parent company. This difference in period ends under these circumstances is considered acceptable for the evaluation of internal control. (See Securities and Exchange (SEC) *Management's Report on Internal Control Over Financial Reporting and Disclosure in Exchange Act Periodic Reports: Frequently Asked Questions* (http://www.sec.gov/info/accountants/controlfaq0604.htm), question 12.)

Management's Internal Control Report

Management's report on internal control effectiveness is contained in the company's Form 10-K or 10-KSB, which is filed annually with the SEC. Under the SEC rules, the company's internal control report must include:[1]

(a) *Management's Annual Report on Internal Control Over Financial Reporting.* Provide a report on the company's internal control over financial reporting that contains:

(1) A statement of management's responsibilities for establishing and maintaining adequate internal control over financial reporting,

(2) A statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting

(3) Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the most recent fiscal year, including a statement as to whether or not internal control over financial reporting is effective. This discussion must include disclosure of any material weakness in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the registrant's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting, and

(4) A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the registrant's internal control over financial reporting

(b) *Audit Report of the Registered Public Accounting Firm.* Provide the registered public accounting firm's audit report on management's assessment of the company's internal control over financial reporting

(c) *Changes in Internal Control Over Financial Reporting.* Disclose any change in the company's internal control over financial reporting that has materially affected, or is reasonably likely to materially affect the company's internal control over financial reporting.

Observations About the Rule

The SEC staff's answers to frequently asked questions (FAQ) provide guidance on the following matters related to management's internal control report:

- Management may *not* "qualify" its conclusions by saying that the company's internal control is effective "subject to" certain qualifications or exceptions. That is, the report should state that controls either are or are not effective. If management concludes that internal control is not effective, it may report that controls are ineffective for specific reasons. (Question 5)

- Generally, the SEC staff would expect a company to disclose *all material* changes in internal control that occur in a fiscal quarter. However, if the company makes changes or improvements to controls as a result of preparing for the company's *first* report on internal control, the staff will not object if these changes are not disclosed. However, if (in preparing for its first internal control report) the company discovers a material weakness and makes changes to internal control in response, the SEC staff

[1] See Regulation S-K, Item 308 (17 CFR § 229.308), or Regulation S-B, Item 308 (17 CFR § 228.308).

states that management should "carefully consider" whether the material weakness and related corrective action should be disclosed. (Question 9)

- The company must disclose material weaknesses in internal control. However, it is *not* obligated to disclose the existence or nature of a significant deficiency, unless a combination of significant deficiencies is deemed to be a material weakness. (Question 11)

Effective Dates

The requirement to disclose material changes in the entity's internal control (17 CFR § 229.308(c)) became effective on August 14, 2003. The effective date for the other provisions of the rules described above, that is, management's report on the effectiveness of internal control and the related external auditor attestation, become effective at different times, depending on the filing status of the company.

- *Accelerated filer.* A company that is an accelerated filer as of the end of its first fiscal year ending on or after November 15, 2004, must begin to comply with the internal control reporting and attestation requirements in its annual report for that fiscal year.[2]
- *Non-accelerated filers.* Smaller companies, foreign private issuers, and other non-accelerated filers are required to comply with the full requirements of the new rules for their first fiscal year ending on or after July 15, 2005.

Definition of Internal Control and the COSO Framework

SEC Definition of Internal Control

For the purposes of complying with the internal control reporting requirements of the Sarbanes-Oxley Act, the SEC rules provide the working definition of the term *internal control over financial reporting*. Rule 13a-15(f) defines *internal control over financial reporting* as follows:

> The term internal control over financial reporting is defined as 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:
>
> (1) Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;
>
> (2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and

[2] *Accelerated filer* is defined in the Securities Exchange Act of 1934, Rule 12b-2. Generally, companies with a market capitalization of $75 million or more are considered accelerated filers.

(3) 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.

Observations About the Rule

- The term *internal control* is a broad concept that extends to all areas of the management of an enterprise. The SEC definition narrows the scope of your consideration of internal control to the preparation of the financial statements, hence the use of the term *internal control over financial reporting.*
- The SEC intends its definition to be consistent with the definition of internal control that pertains to financial reporting objectives included in the Treadway Commission's Committee of Sponsoring Organizations' (COSO) report, *Internal Control—Integrated Framework.*
- The rule makes explicit reference to the use or disposition of the entity's assets, that is, the safeguarding of assets.
- Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, PC sec. 140), provides some guidance on controls relating to the safeguarding of assets. See Appendix B in this Practice Aid.

Note: This Practice Aid, unless otherwise indicated, uses the term *internal control* synonymously with *internal control over financial reporting*, as defined by the SEC rules.

PCAOB Auditing Standard No. 2 frequently refers to "financial statements and related disclosures." The term *disclosures* refers to the notes to the financial statements and does not include the preparation of Management's Discussion and Analysis (MD&A) or other similar information presented outside the financial statements. In this Practice Aid, unless otherwise indicated, we use the term *financial statements* interchangeably with *financial statements and related disclosures.*

The COSO Framework

To gauge the company's internal control effectiveness, you must be able to compare it to an established standard for effectiveness. Choosing an appropriate control criterion is a precondition to performing an assessment of the effectiveness of your company's internal control.

As indicated in the previous section, your company's internal control report must identify the framework used to assess internal control effectiveness. The rules do *not require* or otherwise endorse any of the several frameworks that are available for such purposes. The COSO internal control framework is one widely accepted framework for internal control.[3]

[3] The *Guidance on Assessing Control*, published by the Canadian Institute of Chartered Accountants, and *The Turnbull Report*, published by the Institute of Chartered Accountants in England & Wales, are examples of other suitable frameworks.

The roots of the COSO framework date back to 1985, when COSO was formed to sponsor the National Commission on Fraudulent Financial Reporting. The charge of that group was to study and report on the factors that can lead to fraudulent financial reporting. Since this initial undertaking, COSO has expanded its mission to include improving the quality of financial reporting. A significant part of this mission is aimed at developing guidance on internal control. In 1992, COSO published *Internal Control—Integrated Framework*, which established a framework for internal control and provided evaluation tools that businesses and other entities could use to evaluate their control systems.[4]

The COSO framework describes five interrelated components of internal control:

- *Control environment.* Senior management must set an appropriate "tone at the top" that positively influences the control consciousness of entity personnel. The control environment is the foundation for all other components of internal controls and provides discipline and structure.
- *Risk assessment.* The entity must be aware of and deal with the risks it faces. It must set objectives, integrated throughout all value chain activities, so the organization's units operate in concert. Once these objectives are set, the entity must then identify and analyze the risks to achieving those objectives and develop ways to manage them.
- *Control activities.* Control policies and procedures must be established and executed to help ensure the actions identified by management as necessary to address risks are effectively carried out.
- *Information and communications.* Surrounding the control activities are information and communication systems, including the accounting system. These systems enable the entity's people to capture and exchange the information needed to conduct, manage, and control entity operations.
- *Monitoring.* The entire control process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.

Observations

- Even though the SEC does not require companies to use the COSO framework, the performance and reporting requirements of PCAOB Auditing Standard No. 2 are based on the COSO internal control

[4] In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published a document entitled *Enterprise Risk Management Framework*, whose purpose was to provide guidance on the process used by management to identify and manage risk across the enterprise. This new framework does not supersede or otherwise amend its earlier internal control framework. Internal control is encompassed by and is an integral part of enterprise risk management. Enterprise risk management is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk. *Internal Control—Integrated Framework* remains in place for entities and others looking at internal control by itself.

framework. That the PCAOB has used the COSO framework to structure its guidance does not preclude you from using other, suitable frameworks. **Paragraph 14** of the standard states:

> [suitable frameworks other than COSO] have been published in other countries and may be developed in the future. Such other suitable frameworks may be used in an audit of internal control over financial reporting. Although different frameworks may not contain exactly the same elements as COSO, they should have elements that encompass, in general, all the themes in COSO. Therefore, the [external] auditor should be able to apply the concepts and guidance in this standard in a reasonable manner.

MANAGEMENT'S RESPONSIBILITIES IN AN AUDIT OF INTERNAL CONTROL

As indicated in the Introduction to this Practice Aid, SEC Release No. 33-8238 (which describes the requirements related to management's report on internal control) provides general direction to management on the methods that should be used to evaluate internal control effectiveness. (See Section B.3.d.)

The Auditing Standard incorporates the SEC guidance on management's methods and procedures. **Paragraph 20** of the Auditing Standard *requires management* to do the following.

a. Accept responsibility for the effectiveness of the company's internal control over financial reporting;

b. Evaluate the effectiveness of the company's internal control over financial reporting using suitable control criteria;

c. Support its evaluation with sufficient evidence, including documentation; and

d. Present a written assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year.

If management has not fulfilled these responsibilities, the external auditors are required to disclaim an opinion. When auditors disclaim an opinion, they will state that the scope of their work was not sufficient for them to express—and they do not express—an opinion on internal control effectiveness. The whole point of engaging an auditor to audit internal control is to have them express an opinion on its effectiveness, so it is clearly in your best interests to ensure that company management fulfills its responsibilities.

Management's Assessment Process

The Auditing Standard provides substantial guidance on what management should do to effectively comply with the requirements described in paragraph 20b and 20c. These requirements describe the required elements of the company's assessment process and its documentation. This guidance is discussed in detail in Chapter 2 of this Practice Aid.

Management's Representations

As they are required to do in a traditional financial statement audit, company management are required to make certain written representations to the external auditors at the conclusion of the internal control audit, in order for the auditors to render an unqualified opinion. **Paragraph 142** of the Auditing Standard requires management to provide to the external auditors written representations:

a. Acknowledging management's responsibility for establishing and maintaining effective internal control over financial reporting;

b. Stating that management has performed an assessment of the effectiveness of the company's internal control over financial reporting and specifying the control criteria;

c. Stating that management did not use the [external] 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;

d. Stating management's conclusion about the effectiveness of the company's internal control over financial reporting based on the control criteria as of a specified date;

e. Stating that management has disclosed to the [external] auditor all deficiencies in the design or operation of internal control over financial reporting identified as part of management's assessment, including separately disclosing to the [external] auditor all such deficiencies that it believes to be significant deficiencies or material weaknesses in internal control over financial reporting;

f. Describing any material fraud and any other fraud that, although not material, involves senior management or management or other employees who have a significant role in the company's internal control over financial reporting;

g. Stating whether control deficiencies identified and communicated to the audit committee during previous engagements pursuant to paragraph 207 have been resolved, and specifically identifying any that have not; and

h. Stating whether there were, subsequent to the date being reported on, any changes in internal control over financial reporting or other factors that might significantly affect internal control over financial reporting, including any corrective actions taken by management with regard to significant deficiencies and material weaknesses.

If management fails to provide these written representations, the scope of the internal control audit has been limited, and the external auditors are precluded from issuing an unqualified opinion. In some cases, the external auditors may conclude that the scope limitation is so severe that they have no choice but to withdraw from the engagement. See Chapter 2 of this Practice Aid for an additional discussion of how an external auditor's scope limitation will adversely affect the company.

Additionally, **paragraph 143** of the Auditing Standard requires the external auditors to "evaluate the effects of management's refusal on [their] ability to rely on other representations, including, if applicable, representations obtained in an audit of the company's financial statements."

Practice Pointer. Because of the severe consequences of *not* providing the written representations described in the Auditing Standard, providing these representations is not considered optional. Even though you will not be signing a representation letter until the end of the audit, you should be familiar with what will be required of you from the beginning of the process. Some of the representations will require you to take certain action throughout the performance of the self-assessment process, and so you should plan and perform the process to take these requirements into account.

Observations About the Requirement

The written representations requirement highlights certain other requirements of management's process that were not previously mentioned in paragraph 20. From reading management's required representations, it is apparent that management's responsibilities also include:

- Assessing internal control effectiveness in a way that does *not* rely on the work performed by the company's auditors during either the audit of internal control or the financial statements.
- Disclosing to the external auditors all control deficiencies discovered during the company's self-assessment process.
- Disclosing to the external auditors any material fraud and any fraud involving senior management or others with significant internal control responsibilities.
- Describing how internal control deficiencies identified by the external auditors in the past have, or have not, been resolved.
- Describing significant control changes that occurred after year end.

The external auditor requires that the engagement letter be signed by "those members of management with overall responsibility for financial and operating matters whom the auditor believes are responsible for and knowledgeable about, directly or through others in the organization, the matters covered by the representations." Normally, these management group members include the chief executive officer and chief financial officer. In some cases, either the external auditors or company management may ask those individuals who are directly supervised by management to provide certain specific representations.

THE EXTERNAL AUDITOR'S RESPONSIBILITIES IN AN AUDIT OF INTERNAL CONTROL

The Objective of an Audit of Internal Control

As indicated previously, company management and the external auditors share some common goals related to internal control—both are charged with evaluating the effectiveness of the company's internal control as of year end. For this reason, a reading of how the Auditing Standard describes the external auditor's objectives may help you articulate your own.

Paragraph 4 of the Auditing Standard states in part.

> The [external] auditor's objective in an audit of internal control over financial reporting is to express an opinion on management's assessment of the effectiveness of the company's internal control over financial reporting . . . . Maintaining effective internal control over financial reporting means that no material weaknesses exist; therefore, the objective of the audit of internal control over financial reporting is to obtain reasonable assurance that no material weaknesses exist as of the date specified in management's assessment.

Observations

- Note the standard's reference to "reasonable assurance" as a threshold for determining whether internal control is effective. Reasonable assurance is a very high threshold, but it stops short of *absolute* assurance. When drawing your conclusions about internal control effectiveness, you should consider using this same "reasonable assurance" threshold.

- The last sentence of paragraph 4 rephrases the objective of an audit of internal control as a process to obtain reasonable assurance that no material weaknesses exist as of the reporting date. For this reason, the definition of the term *material weakness* will be a driving force in the planning and performance of company management's self-assessment process. To effectively plan and perform this assessment, the project team should have a good working knowledge of the term.

- Chapter 5 of this Practice Aid defines and discusses the term *material weakness* and the related terms *significant deficiency* and *control deficiency*.

To anticipate and respond effectively to the external auditor's requirements during an internal control audit, it helps if you have a working understanding of how they approach their work.

Paragraph 5 of the Auditing Standard lays out a broad framework for how external auditors will conduct an audit of internal control.

> To obtain reasonable assurance, the [external] auditor evaluates the assessment performed by management and obtains and evaluates evidence about whether the internal control over financial reporting was designed and operated effectively. The [external] auditor obtains this evidence from a number of sources, including using the work performed by others and performing auditing procedures himself or herself.

Observations About the Requirements

- The external auditor's audit of internal control involves two main evaluations:

  — An evaluation of management's assessment of internal control effectiveness.

  — An evaluation of whether internal control was designed and operating effectively.

- Evidence relating to the design and operation of internal control comes from two sources:

  — The work performed by the company in its self-assessment process.

  — The work the external auditor performs himself or herself.

- Early in the planning stages of your self-assessment project, you should consider how to maximize the extent to which the external auditors can use the company's work.

The External Auditor's Other Responsibilities

Management's Quarterly Reports and Certifications on Internal Control Over Financial Reporting

Section 302 of the Sarbanes-Oxley Act requires company management to report quarterly on, among other things, the effectiveness of the company's internal control and all material changes in the entity's internal control over financial reporting.

With its rules implementing this requirement, the SEC introduces a new term, *disclosure controls and procedures*, which is different from *internal controls over financial reporting* defined earlier. SEC Rule 13a-15(e) defines disclosure controls and procedures as essentially encompassing the controls over all material financial and *nonfinancial* information in the Securities Exchange Act of 1934 reports. The internal control over financial reporting is just one element of a company's disclosure controls and procedures.

In addition to providing a report on the effectiveness of its disclosure controls and internal control over financial reporting, the company's principal executive officer and principal financial officer are required to sign a certification, which is included as exhibits to the entity's 10-Q and 10-K or 10-KSB. The text of this certification is reproduced in Exhibit 1-1.

Exhibit 1-1 Section 302 Certification

SEC Rule 13a-14(a)/15d-14(a)

I, [*identify the certifying individual*], certify that:

1. I have reviewed this [*specify report*] of [*identify registrant*];
2. Based on my knowledge, this 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 such statements were made, not misleading with respect to the period covered by this report;
3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;
4. The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:
   (a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;
   (b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial

reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

(c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

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

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

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

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

Observations About the Certification

- To help public companies implement the SEC's requirement to report on and certify disclosure controls and procedures, the SEC also advised all public companies to create a disclosure committee to oversee the process by which disclosures are created and reviewed. The effective functioning of this committee and its work product may be helpful to you as you plan and perform your annual assessment of internal control effectiveness.

- The quarterly certification includes statements about *both* disclosure controls and procedures and internal control over financial reporting.

- An external auditor's responsibility as it relates to the quarterly certifications in internal control is different from his or her responsibility relating to the annual audit of internal control. For the quarterly reporting, the external auditor will perform limited procedures to:

  — Inquire of management about significant changes in the design or operation of internal control that could have occurred subsequent to the preceding annual audit or prior review of interim financial information.

- Management should be prepared to respond thoroughly to these inquiries.

Differences Between the Audit of Internal Control and the Financial Statement Audit

You are probably accustomed to responding to external auditor inquiries and requests for information related to a traditional financial statement audit. As indicated earlier, the Sarbanes-Oxley Act adds a second audit, the audit of internal control, to the traditional financial statement audit. Moreover, the same audit firm must perform *both* audits.

PCAOB Auditing Standard No. 2 describes how the audit of the financial statements and the internal control audit should be integrated. Essentially, the external auditor will use the information obtained in one audit to inform his or her judgments and procedures made in the other.

You also should be aware that the external auditor's tests of internal control effectiveness performed during an audit of internal control will be much more extensive than the internal control tests typically performed as part of the financial statement audit.

Finally, you should be aware of how an external auditor's adverse opinion on internal control affects his or her opinion on the financial statements. The identification of a material weakness in internal control (and the resulting adverse opinion on internal control effectiveness) does not preclude the external auditor from issuing a "clean" opinion on the financial statements, if certain additional procedures can be performed successfully.

KEY CONSIDERATIONS IN THE AUDITOR-MANAGEMENT RELATIONSHIP

Both Sarbanes-Oxley and the PCAOB Auditing Standard describe a two-pronged approach for providing financial statement users with useful information about the reliability of a company's internal control:

- First, management assesses and reports on the effectiveness of the entity's internal control.
- Second, the company's external auditors audit management's report and issue a separate, independent opinion on the effectiveness of the company's internal control.

In this scheme, it is vital that the two perform their duties independently of each other.

By the same token, the practical aspects of implementing the requirements of Sarbanes-Oxley Section 404 suggest that external auditors should be able to use, to some degree, the work performed by management in its self-assessment of internal control in their audit. To do otherwise, to completely prohibit external auditors from using some of management's work, would make the cost of compliance quite steep.

Thus, the Auditing Standard balances two competing goals: objectivity and independence of the parties involved versus the use of management's work by the external auditor as a means of limiting the overall cost of compliance.

Note: As discussed in subsequent chapters, the company is *prohibited* in its self-assessment of internal control from relying on the work performed by the external auditors in their audit.

The External Auditor's Use of the Company's Internal Control Work

The company is required to perform a thorough, detailed assessment of its internal control. As much as possible, management will want to provide the results of its work to the external auditors, so the auditors will not have to duplicate the company's efforts.

Paragraphs 108 through 126 of the Auditing Standard provide extensive guidance on the degree to which the company's work on internal control can be used by the external auditors. The relevant section is titled "Using the Work of Others." The standard indicates that the work of "others" includes the relevant work performed by:

- Internal auditors.
- Other company personnel.
- Third parties working under the direction of management or the audit committee.

The external auditor's ability to rely on the work of others has its limits. **Paragraph 108** of the standard describes the fundamental principle in the external auditor's using the work of others. The external auditor must "perform enough of the testing himself or herself so that the external auditor's own work provides the principal evidence for the [external] auditor's opinion." The standard goes on to describe a framework for ensuring that the [external] auditors comply with this principle. Essentially:

- The external auditor is prohibited from using the company's work in certain areas of the audit.
- For all other areas, the external auditor may use the company's work, if certain conditions are met.

Work That Must Be Performed by the External Auditors

There are two areas where the external auditors are prohibited from using the company's work in their audit.

- *Control environment.* The external auditors are prohibited from using the work of company management and others to reduce the amount of work they perform on controls in the control environment. This does not mean that they can *ignore* your work in this area. To the contrary, **paragraph 113** of the standard requires the external auditor to "consider the results of work performed in this area by others because it might indicate the need for the [external] auditor to increase his or her own work."
- *Walkthroughs.* External auditors are required to perform at least one walkthrough for each major class of transactions. A walkthrough involves tracing a transaction from origination through the company's information systems until it is reflected in the company's financial reports. Chapter 3 of this Practice Aid discusses the requirements for walkthroughs in more detail.

Included in Appendix F of this Practice Aid are several examples, taken from the Auditing Standard, of how this framework (described in the following pages) would be applied in practice.

Observations About the Requirements

- **Paragraph 115** of the standard states that "controls specifically established to prevent and detect fraud" are part of the control environment. Thus, the external auditors will be testing antifraud programs and controls themselves.
- The answer to question 23 in the PCAOB's *Staff Questions and Answers: Auditing Internal Control Over Financial Reporting* (http://www.pcaobus.org/documents/Staff_Q_and_A/Staff_Interal_Control.pdf) discusses the interaction between the requirement that external auditors test antifraud programs and controls themselves and other requirements relating to procedures to detect material misstatements due to fraud that are performed in the financial statement audit. The PCAOB staff clarifies that certain procedures that the external auditors will perform in a financial statement audit to assess the risk of material misstatement due to fraud, should be performed by the external auditors (and not others) in their audit of internal control.
- **Paragraph 110** of the standard provides the general guidance that "[j]udgments about the sufficiency of evidence obtained and . . . the significance of identified control deficiencies, should be those of the [external] auditor."

Using the Work of Others

For all areas other than the control environment and the walkthroughs, the external auditors may use the company's tests on internal control during their audit.

Paragraph 109 of the standard summarizes the steps that the external auditor must follow to use the work of others to support his or her conclusions reached in the audit of internal control. To determine the extent to which the external auditor may use the company's work, the external auditor is required to:

a. Evaluate the nature of the controls subjected to the work of others (See paragraphs 112 through 116);

b. Evaluate the competence and objectivity of the individuals who performed the work (See paragraphs 117 through 122); and

c. Test some of the work performed by others to evaluate the quality and effectiveness of their work (See paragraphs 123 through 125).

Evaluating the Nature of the Controls **Paragraph 112** of the standard provides relatively straightforward guidance on determining whether the nature of the controls subjected to the work of others would make those controls good candidates for the external auditors to rely on in their audit.

> 112. *Evaluating the Nature of the Controls Subjected to the Work of Others.* The auditor should evaluate the following factors when evaluating the nature of the controls subjected to the work of others. As these factors increase in significance, the need for the auditor to perform his or her own work on those controls increases. As these factors decrease in significance, the need for the auditor to perform his or her own work on those controls decreases.

- The materiality of the accounts and disclosures that the control addresses and the risk of material misstatement.
- The degree of judgment required to evaluate the operating effectiveness of the control (that is, the degree to which the evaluation of the effectiveness of the control requires evaluation of subjective factors rather than objective testing).
- The pervasiveness of the control.
- The level of judgment or estimation required in the account or disclosure.
- The potential for management override of the control.

Exhibit 1-2 summarizes the guidance provided in paragraph 112 of the Auditing Standard.

Exhibit 1-2 Evaluating the Nature of the Controls

Factor	*External Auditor More Likely to Do His or Her Own Work*	*External Auditor More Likely to Rely on the Company's Work*
Materiality of account related to the control	Account is material	Account is not material
Risk of material misstatement of account related to the control	High risk of material misstatement	Low risk of material misstatement
Judgment required to evaluate operating effectiveness of control	Highly subjective	Highly objective
Pervasiveness of control	Pervasive	Restricted to specific account, transaction, or assertion
Judgment or estimation required in the account	Highly subjective/extensive use of estimates	Highly objective
Potential for management override	High potential	Low potential

Competence and Objectivity of Individuals Who Performed the Work The extent to which the external auditors can use the company's work depends on the degree of competence and objectivity of the individuals performing the work. The more objective and competent the individuals are who performed the work, the more use the external auditors can make of it in their audit.

Competence and objectivity must be *considered together*. That is, the work of an individual who has one trait but not the other should not be relied on in the audit.

Paragraphs 119 and 120 provide guidance on the factors external auditors must consider to evaluate competence and objectivity.

> 119. Factors concerning the competence of the individuals performing the tests of controls include:
>
> - Their educational level and professional experience.
> - Their professional certification and continuing education.
> - Practices regarding the assignment of individuals to work areas.
> - Supervision and review of their activities.

- Quality of the documentation of their work, including any reports or recommendations issued.
- Evaluation of their performance.

120. Factors concerning the objectivity of the individuals performing the tests of controls include:

- The organizational status of the individuals responsible for the work of others ("testing authority") in testing controls, including—
  a. Whether the testing authority reports to an officer of sufficient status to ensure sufficient testing coverage and adequate consideration of, and action on, the findings and recommendations of the individuals performing the testing.
  b. Whether the testing authority has direct access and reports regularly to the board of directors or the audit committee.
  c. Whether the board of directors or the audit committee oversees employment decisions related to the testing authority.
- Policies to maintain the individuals' objectivity about the areas being tested, including—
  a. Policies prohibiting individuals from testing controls in areas in which relatives are employed in important or internal control sensitive positions.
  b. Policies prohibiting individuals from testing controls in areas to which they were recently assigned or are scheduled to be assigned upon completion of their controls testing responsibilities.

Use of the Work of Internal Auditors The Auditing Standard makes special note of the work of internal auditors, noting that their work may be used "to a greater extent than the work of other company personnel." **Paragraph 121** provides guidance to the external auditors regarding the conditions that should exist if they are to use the company's internal auditors to the maximum possible extent.

121. Internal auditors normally are expected to have greater competence with regard to internal control over financial reporting and objectivity than other company personnel. Therefore, the auditor may be able to use their work to a greater extent than the work of other company personnel. This is particularly true in the case of internal auditors who follow the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors. If internal auditors have performed an extensive amount of relevant work and the auditor determines they possess a high degree of competence and objectivity, the auditor could use their work to the greatest extent an auditor could use the work of others. On the other hand, if the internal audit function reports solely to management, which would reduce internal auditors' objectivity, or if limited resources allocated to the internal audit function result in very limited testing procedures on its part or reduced competency of the internal auditors, the auditor should use their work to a much lesser extent and perform more of the testing himself or herself.

Testing the Work of Others In order to evaluate the overall quality and effectiveness of the work of others, the external auditors are required to test some of their work, either by:

- Testing some of the controls that they tested; or
- Testing similar controls not actually tested by them.

Paragraph 125 provides the following broad guidance on what the external auditors will look for when evaluating the quality and effectiveness of the company's work.

- Scope of work is appropriate to meet the objectives.
- Work programs are adequate.
- Work performed is adequately documented, including evidence of supervision and review.
- Conclusions are appropriate in the circumstances.
- Reports are consistent with the results of the work performed.

External auditors are *not* required to test the work of others in every significant account in which they plan to use the company's work.

Practice Pointers. To allow the company's external auditors to make as much use as possible of the company's own assessment of internal control, you should have a clear understanding of the conditions that must be met for the external auditors to use the work. To help the external auditors determine that those criteria have been met, you may wish to *document your compliance with the key requirements* described previously and make this documentation available to the external auditors early on in their audit planning process. For example, you should consider:

- Obtaining the bios or resumes of project team members showing their education level, experience, professional certification, and continuing education.
- Documenting the company's policies regarding the assignment of individuals to work areas.
- Documenting the "organizational status" of the project team and how they have been provided access to the board of directors and audit committee.
- Determining that the internal auditors follow the relevant internal auditing standards.
- Establishing policies that ensure that the *documentation* of the work performed includes:
  - — A description of the scope of the work
  - — Work programs
  - — Evidence of supervision and review
  - — Conclusions about the work performed

Seeking Help and Advice From External Auditors

During the course of its assessment of internal control, the company is likely to encounter many issues for which management needs advice. The company may find itself short on resources and needing to engage third parties to help in the process. In these situations, it is natural for management to turn to its external auditors for advice and other assistance.

You should be cautious in seeking the assistance of the company's external auditors to help with the company's internal control assessment. **Paragraph A7** of the PCAOB staff's FAQs provides some general guidance to both management and external auditors on how to seek and provide advice. The guidance from the staff was in answer to a question directed specifically to an external auditor's review of a company's draft financial statements or their providing advice on the adoption of a new accounting principle or emerging issue—services that historically have been considered a routine part of a high quality audit. The PCAOB staff had the following observation.

> **A7.** The inclusion of this circumstance in Auditing Standard No. 2 as a significant deficiency and a strong indicator of a material weakness emphasizes that a company must have effective internal control over financial reporting on its own. More specifically, the results of auditing procedures cannot be considered when evaluating whether the company's internal control provides reasonable assurance that the company's financial statements will be presented fairly in accordance with generally accepted accounting principles. There are a variety of ways that a company can emphasize that it, rather than the auditor, is responsible for the financial statements and that the company has effective controls surrounding the preparation of financial statements.
>
> Modifying the traditional audit process such that the company provides the auditor with only a single draft of the financial statements to audit when the company believes that all its controls over the preparation of the financial statements have fully operated is one way to demonstrate management's responsibility and to be clear that all the company's controls have operated. However, this process is not necessarily what was expected to result from the implementation of Auditing Standard No. 2. Such a process might make it difficult for some companies to meet the accelerated filing deadlines for their annual reports. More importantly, such a process, combined with the accelerated filing deadlines, might put the auditor under significant pressure to complete the audit of the financial statements in too short a time period thereby impairing, rather than improving, audit quality. Therefore, some type of information-sharing on a timely basis between management and the auditor is necessary.
>
> A company may share interim drafts of the financial statements with the auditor. The company can minimize the risk that the auditor would determine that his or her involvement in this process might represent a significant deficiency or material weakness through clear communications (either written or oral) with the auditor about the following:
>
> - State of completion of the financial statements;
> - Extent of controls that had operated or not operated at the time; and
> - Purpose for which the company was giving the draft financial statements to the auditor.
>
> For example, a company might give the auditor draft financial statements to audit that lack two notes required by generally accepted accounting principles. Absent any communication from the company to clearly indicate that the company recognizes that two specific required notes are lacking, the auditor might determine that the lack of those notes constitutes a material misstatement of the financial statements that represents a significant deficiency and is a strong indicator of a material weakness. On the other hand, if the company makes it clear when it provides the draft financial statements to the auditor that two specific required notes

are lacking and that those completed notes will be provided at a later time, the auditor would not consider their omission at that time a material misstatement of the financial statements.

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

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

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

Observations About the Guidance

Even though the staff's answer was directed to specific situations, it sets forth several broad principles that can be analyzed for how they apply to others. These broad principles include the following.

- Management cannot consider the results of the external auditor's procedures when evaluating internal control effectiveness. That is, "the auditor's review of the draft financial statements" is *not a control procedure* encompassed by the company's internal control over financial reporting. The company's internal control must exist separately and independently from the audit.

- In working with external auditors, the company should take care to emphasize that management, not the external auditor, is responsible for internal control.
- Information-sharing on a timely basis between management and the external auditors is clearly necessary.
- It is incumbent on management to clearly communicate with the external auditors the nature of the advice they are seeking and the purpose for which the auditor is being involved.
- Some aspects of the traditional relationship between management and its external auditors will change. Companies may not be able to reflexively turn to their external auditors to provide the same type of advice and counsel that they have in the past. Other sources of knowledge and expertise will have to be used, either through the development of in-house resources or the establishment of relationships with experts that are *not* members of the company's external audit firm.

Auditor Independence Issues

To render an opinion on either the financial statements or the effectiveness of internal control, the external auditors are required to maintain their independence, in accordance with applicable SEC rules. A failure to comply with these rules could have significant adverse consequences, not only for the auditors, but for the company as well. For example, if the SEC determines that the company's external auditors were not independent from the company, it could require a reaudit of the company's financial statements and its internal control.

The SEC independence rules are guided by four basic principles. If the detailed rules do not address a particular circumstance (such as internal control-related services), the SEC will consider the situation in light of the basic principles. The basic principles state that independence would be impaired whenever a relationship between the auditor and the company or the auditor's services to the company:

- Creates a mutual or conflicting interest between the firm and the client.
- Places the firm in a position where it subsequently audits its own work.
- Results in the firm acting as management or as an employee of the client.
- Places the firm in a position where it acts as an advocate for the client.

The PCAOB Auditing Standard incorporates these four basic principles in its guidance on independence when performing an audit of internal control. **Paragraph 32** of the standard clarifies that these four basic principles "do not preclude the auditor from making substantive recommendations as to how management may improve the design or operation of the company's internal controls as a by-product of an audit."

In addition to enumerating the basic principles of external auditor independence, paragraphs 32 through 35 of the Auditing Standard provide the following broad guidance on independence matters, as described in the subsequent bullets.

Maintaining independence is primarily the responsibility of the external auditors. However, note that several of the independence requirements impose certain responsibilities on management and the audit committee.

- *Preapproval by the audit committee.* Each internal control-related service to be provided by the external auditor must be preapproved by the audit committee. In its introduction to the standard, the PCAOB clarifies that "the audit committee cannot pre-approve internal control-related services as a category, but must approve each service."

  For proxy or other disclosure purposes, the company may designate some auditor services as "audit" or "nonaudit" services. The requirement to preapprove internal control services applies to *any* internal control-related services, regardless of how they might be designated.

  Paragraph A4 of the PCAOB staff's FAQs clarifies that there is no "grandfathering" for internal control-related engagements that were preapproved by the audit committee before the effective date of the Auditing Standard. If that preapproval does not meet the requirements in the Auditing Standard, the audit committee should "specifically evaluate the independence implications of the continuation of those services as soon as practicable."

- *Active involvement of management.* Management must be "actively involved" in a "substantive and extensive" way in all internal control services the external auditor provides. Management cannot delegate these responsibilities, nor can it satisfy the requirement to be actively involved by merely accepting responsibility for documentation and testing performed by the auditors.

- *Independence in fact and appearance.* The company's audit committee and external auditors must be diligent to ensure that independence both in fact and appearance is maintained. As articulated in **paragraph 35**:

  > The test for independence in fact is whether the activities would impede the ability of anyone on the engagement team or in a position to influence the engagement team from exercising objective judgment in the audits of the financial statements or internal control over financial reporting. The test for independence in appearance is whether a reasonable investor, knowing all relevant facts and circumstances, would perceive an auditor as having interests which could jeopardize the exercise of objective and impartial judgments on all issues encompassed within the auditor's engagement.

In its answers to FAQs, the SEC staff chose not to provide expanded, detailed guidance on independence matters. In question 17 of that document, they merely stated the following:

> The auditor is allowed to provide limited assistance to management in documenting internal controls and making recommendations for changes to internal controls.

SUMMARY

Section 404 of the Sarbanes-Oxley Act established a requirement for publicly traded companies that:

- Management assess and report on the effectiveness of the company's internal control; and
- The company's external auditors audit internal control and provide a separate, independent opinion on the company's internal control effectiveness.

Management's responsibilities—as defined by the SEC and incorporated into the Auditing Standard—are significant.

Some of the work performed by management in the company's self-assessment process may be able to be used by the external auditors in their audit of internal control. However, certain conditions must be met, including certain requirements related to the competence and objectivity of the individuals who performed the work.

CHAPTER 2: PROJECT SCOPE

DETERMINING THE SCOPE OF MANAGEMENT'S ASSESSMENT PROCESS

The Securities and Exchange Commission (SEC) rules relating to the scope of management's assessment of internal control effectiveness are rather general. In practice, companies frequently encounter situations for which the SEC has not provided guidance. In those situations, management should consider the Auditing Standard to help determine which business units or controls should be included in their assessment.

As described in Chapter 1 of this Practice Aid, Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, PC sec. 140), provides extensive guidance on the required scope of management's self-assessment of the company's internal control. This guidance is in the context of the external auditor's evaluation of the quality of the company's assessment process, stating that the external auditor should determine whether management's evaluation includes certain elements.

If the company's self-assessment process does *not* include all the elements listed in the standard, the external auditor will conclude that the process was inadequate, in which case he or she will be forced to determine that a scope limitation had been placed on the engagement.

When an audit scope limitation exists, the external auditor would choose either of the following:

- Issue a qualified opinion, stating that "management's assessment of internal control effectiveness was fairly stated, *except for* . . ." and then describing the elements of the assessment process that were missing.
- Disclaim an opinion on management's assessment process, or withdraw from the engagement.

The external auditor's course of action will depend on the relative significance of the elements that are missing from the company's assessment process.

Clearly, it is in the company's best interests for management to take care that their assessment process includes all the required elements listed in the standard.

THE REQUIRED ELEMENTS OF MANAGEMENT'S ASSESSMENT PROCESS

Paragraph 40 of the standard provides detailed guidance on what is required of management's process, stating that management should address the following elements.

- Determining which controls should be tested, including controls over all relevant assertions related to all significant accounts and disclosures in the financial statements. Generally, such controls include:
  - — Controls over initiating, authorizing, recording, processing, and reporting significant accounts and disclosures and related assertions embodied in the financial statements.
  - — Controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles.
  - — Antifraud programs and controls.
  - — Controls, including information technology general controls, on which other controls are dependent.
  - — Controls over significant nonroutine and nonsystematic transactions, such as accounts involving judgments and estimates.
  - — Company-level controls (as described in paragraph 53), including:
    - The control environment, and
    - Controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; to initiate, authorize, record, and process journal entries in the general ledger; and to record recurring and nonrecurring adjustments to the financial statements (for example, consolidating adjustments, report combinations, and reclassifications).

  Note: References to the period-end financial reporting process in this standard refer to the preparation of both annual and quarterly financial statements.
- Evaluating the likelihood that failure of the control could result in a misstatement, the magnitude of such a misstatement, and the degree to which other controls, if effective, achieve the same control objectives.
- Determining the locations or business units to include in the evaluation for a company with multiple locations or business units (See paragraphs B1 through B17).
- Evaluating the design effectiveness of controls.
- Evaluating the operating effectiveness of controls based on procedures sufficient to assess their operating effectiveness. Examples of 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 report (see paragraphs B18 through B29), 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. Inquiry alone is not adequate to complete this evaluation. To evaluate the effectiveness of the company's internal control over financial reporting, management must have evaluated controls over all relevant assertions related to all significant accounts and disclosures.
- Determining the deficiencies in internal control over financial reporting that are of such a magnitude and likelihood of occurrence that they constitute significant deficiencies or material weaknesses.
- Communicating findings to the auditor and to others, if applicable.
- Evaluating whether findings are reasonable and support management's assessment.

Observations About the Requirements

- The first bullet point in paragraph 40 provides definitive guidance for determining which controls should be included within the scope of management's assessment process. That guidance includes a wide variety of controls that *go beyond* what you typically might consider an accounting control, such as:
  - — The selection and application of accounting policies
  - — Antifraud programs and controls
  - — The company's "tone at the top" and other elements of the control environment
- The standard states that "inquiry alone is not adequate" to test operating effectiveness. The testing of controls is discussed in Chapter 4 of this Practice Aid.
- The remaining guidance in paragraph 40 describes an extremely comprehensive and complex process for testing, evaluating, documenting, and communicating internal control effectiveness. These other requirements are covered in other chapters of this Practice Aid.

This chapter focuses primarily on the requirements of paragraph 40 that have an effect on determining the scope of the controls that should be included in the assessment process.

What if management decides to forgo the required testing or documentation that is required by the Auditing Standard and the SEC? Would it be acceptable for the external auditors to simply render an adverse opinion on internal control or management's assessment process and then "move on"?

The PCAOB staff addresses this question in question 8 of its *Staff Questions and Answers: Auditing Internal Control Over Financial Reporting* (http://www.pcaobus.org/documents/Staff_Q_and_A/Staff_Interal_Control.pdf). The answer is no. As described in Chapter 1 of this Practice Aid, management's responsibilities in an audit of internal control include evaluating the effectiveness of the company's internal control. If management does not fulfill these responsibilities (as described more completely in Chapter 4 of this Practice Aid), the external auditors will communicate to the audit committee that the internal control audit cannot be satisfactorily completed, and that they are required to *disclaim an opinion.*

The PCAOB staff goes on to point out:

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

What if the company's assessment does not encompass certain controls that should have been included because it does not have the ability to evaluate those controls. For example, what if the company was unable to obtain evidence of operating effectiveness of controls at a service organization because:

- A Type 2 SAS No. 70 report is not available; and
- Management cannot perform its own tests of controls at the service organization because they don't have a contractual right to do so.

Answer 19 of the SEC staff's *Management's Report on Internal Control Over Financial Reporting and Disclosure in Exchange Act Periodic Reports: Frequently Asked Questions* (http://www.sec.gov/info/accountants/controlfaq1004.htm) provides guidance on this situation and states that:

> Management's annual report on internal control over financial reporting must include a statement as to whether or not internal control over financial reporting is effective. While the staff will allow the exceptions outlined in Questions 1, 2, and 3 [of their Frequently Asked Questions document], the disclosure requirement does not permit management to issue a report on internal control over financial reporting with a scope limitation. Therefore, management must determine whether the inability to assess controls over a particular process is significant enough to conclude in their report that internal control over financial reporting is not effective. Further, management is precluded from concluding that the registrant's internal control over financial reporting is effective if there are one or more material weaknesses in the internal control over financial reporting.

Additional Guidance Necessary for Understanding the Required Scope of Management's Process

The first bullet point in paragraph 40 describes the definitive guidance on the scope of management's process for assessing internal control. However, many of the terms used in this section are defined elsewhere in the standard or, in some cases, described outside the standard itself. To properly set the scope of your project, you should have a working definition of the following terms.

- Relevant assertions
- Significant accounts
- Controls over the selection and application of accounting policies
- Antifraud programs and controls
- Information technology (IT) general controls
- Accounting estimates
- Company-level controls
- Period-end financial reporting processes

The following provides guidance and suggestions on each of these items.

Relevant Assertions

The term *assertions* is not defined in PCAOB Auditing Standard No. 2. *Assertions* is an auditing term that is defined elsewhere in the auditing literature.

Assertions are the representations of management that are embodied in the entity's financial statements. These assertions may be either explicit or implicit. For example, the balance sheet line item that reads "Cash.....$xx,xxx" is an *explicit* assertion that the company's cash accounts at the balance sheet date totaled the stated amount. *Implicit* assertions include the following.

- The company has the right to spend the cash.
- The stated amount includes *all* the company's cash accounts.
- The accounts included in the total are valid company accounts that exist at bona fide financial institutions.

The auditing literature describes the following financial statement assertions.

- *Existence (of assets or liabilities) or occurrence (of transactions).* Assertions about existence or occurrence address whether assets or liabilities of the entity exist at a given date and whether recorded transactions have occurred during the period. For example, management asserts that finished goods inventories in the balance sheet are available for sale. Similarly, management asserts that sales in the income statement represent the exchange of goods or services with customers for cash or other consideration.
- *Valuation or allocation of the amounts reported in the financial statements.* Assertions about valuation or allocation address whether asset, liability, equity, revenue, and expense components have been included in the financial statements at appropriate amounts. For example, management asserts that property is recorded at historical cost and that such cost is systematically allocated to appropriate accounting periods. Similarly, management asserts that trade accounts receivable included in the balance sheet are stated at net realizable value.
- *Completeness of the financial statements.* Assertions about completeness address whether all transactions and accounts that should be presented in the financial statements are so included. For example, management asserts that all purchases of goods and services are recorded and are included in the financial statements. Similarly, management asserts that notes payable in the balance sheet include all such obligations of the entity.
- *Rights (to reported assets) and obligations (for reported liabilities).* Assertions about rights and obligations address whether assets are the rights of the entity and liabilities are the obligations of the entity at a given date. For example, management asserts that amounts capitalized for leases in the balance sheet represent the cost of the entity's rights to leased property and that the corresponding lease liability represents an obligation of the entity.

- *Presentation and disclosure of the amounts and captions in the financial statements.* Assertions about presentation and disclosure address whether particular components of the financial statements are properly classified, described, and disclosed. For example, management asserts that obligations classified as long-term liabilities in the balance sheet will not mature within one year. Similarly, management asserts that amounts presented as extraordinary items in the income statement are properly classified and described.

Auditing Standard No. 2 requires you to describe the "relevant" assertions for each significant account. It does not require you to use the five assertions listed above, and the company may choose to define different relevant assertions. The articulation of relevant assertions is important because ultimately it will drive your testing and evaluation of individual controls. That is, for each significant account, there should be an effective control or combination of controls that addresses each of the relevant assertions.

Paragraph 70 provides the following guidance on the consideration of relevant assertions.

> *Relevant assertions* are assertions that have a meaningful bearing on whether the account is fairly stated. For example, valuation may not be relevant to the cash account unless currency translation is involved; however, existence and completeness are always relevant. Similarly, valuation may not be relevant to the gross amount of the accounts receivable balance, but is relevant to the related allowance accounts.

Significant Accounts

The scope of management's assessment of the company's internal control should include all "significant" accounts and disclosures in the financial statements.

Paragraph 60 of the standard requires that external auditors identify all significant accounts "first at the financial-statement level and then at the account or disclosure-component level." That is, the audit of internal control will be conducted *not* at the highly aggregated financial statement line-item level, but rather, at the more detailed general ledger account level. Management should conduct its assessment at this same detailed level.

The standard observes that some accounts may comprise different components with different levels of risk. For example, the company may have two locations or two kinds of inventory that are aggregated for financial statement reporting purposes. In those situations, you should evaluate the relative significance of the components separately.

Paragraph 61 of the Auditing Standard defines a significant account as one in which:

> [T]here is more than a remote likelihood that the account could contain misstatements that individually, or when aggregated with others, could have a material effect on the financial statements, considering the risks of both overstatement and understatement. Other accounts may be significant on a qualitative basis based on the expectations of a reasonable user.

It is important to note that:

- The threshold for determining whether an account is significant turns on whether there is "more than a remote likelihood," which is a fairly low threshold. The term *remote* has the same meaning as defined in Financial Accounting Standards Board (FASB) Statement No. 5, *Accounting for Contingencies*, that is, "the chance of the future event or events occurring is slight." Thus, a significant account is one in which there is more than a slight chance that the account could contain a misstatement, either individually or when aggregated with others.
- When considering whether an account is significant, you have to consider *both* quantitative and qualitative factors.

Paragraph 65 of the standard lists several factors that you should consider when determining whether an account is significant. These factors are presented in the first column of Exhibit 2-1, together with an interpretation of how the factors might be considered.

Exhibit 2-1 Significant Accounts

	How the Factor Might Be Considered	
Guidance Included in the Auditing Standard	*Indicates Account is* More *Significant*	*Indicates Account is* Less *Significant*
Size and composition of the account;	Large balance	Small balance
Susceptibility of loss due to errors or fraud;	Highly susceptible	Less susceptible
Volume of activity, complexity, and homogeneity of the individual transactions processed through the account;	Large volume, complex transactions, great variety of transactions included in the account	Small volume, simple, homogeneous transactions
Nature of the account (for example, suspense accounts generally warrant greater attention);	Relative significance based on several factors that will require judgment to evaluate	Relative significance based on several factors that will require judgment to evaluate
Accounting and reporting complexities associated with the account;	Complex accounting and reporting	Relatively simple accounting and reporting
Exposure to losses represented by the account, (for example, loss accruals related to a consolidated construction contracting subsidiary);	Significant exposure to loss	Minimal exposure to loss

(continued)

Exhibit 2-1 Significant Accounts *(continued)*

Guidance Included in the Auditing Standard	*How the Factor Might Be Considered*	
	Indicates Account is More *Significant*	*Indicates Account is* Less *Significant*
Likelihood (or possibility) of significant contingent liabilities arising from the activities represented by the account;	Greater than remote possibility of significant contingent loss	Remote possibility of significant contingent loss
Existence of related-party transactions in the account; and	Related-party transactions included in account	No related-party transactions included in account
Changes from the prior period in account characteristics, (for example, new complexities or subjectivity or new types of transactions).	Substantial changes from prior period	Minimal changes from prior period

Practice Pointer. In determining which accounts are considered significant, consider creating a two-dimensional matrix to summarize your judgments made about each financial statement account and disclosure. To create such a matrix:

1. Across the horizontal axis (the first row), list each of the factors mentioned in the auditing literature, as described in Exhibit 2-1.
2. Down the vertical axis (the first column), list each account.
3. Start with the first account listed and work left to right. For that account, review the factor listed in each column. Determine the degree to which the factor is relevant to the given account, for example, "high," "medium," or "low."
4. Accounts with a preponderance of "high" or "medium" designations are probably significant, while those where all of the factors have "low" relevance probably will not be considered significant.

Exhibit 2-2 is an example of a matrix like the one described here.

Exhibit 2-2 Example Matrix of Significant Accounts

Purpose

This matrix can be used to document management's identification of significant accounts to be included within the scope of its assessment of internal control effectiveness.

The account characteristics across the horizontal axis are defined in PCAOB Auditing Standard No. 2 as:

- *Size and composition.* Size and composition of the account.
- *Loss.* Susceptibility of loss due to errors or fraud.
- *Transactions.* Volume of activity, complexity, and homogeneity of the individual transactions processed through the account.
- *Account type.* Nature of the account, for example, suspense accounts generally warrant greater attention.
- *Complexities.* Accounting and reporting complexities associated with the account.
- *Loss exposure.* Exposure to losses represented by the account, for example, loss accruals related to a consolidated construction contracting subsidiary.
- *Contingent liability.* Likelihood (or possibility) of significant contingent liabilities arising from the activities represented by the account.
- *Related party.* Existence of related-party transactions in the account.
- *Changes.* Changes from the prior period in account characteristics, for example, new complexities or subjectivity or new types of transactions.

Note that the accounts illustrated here have been presented at the financial statement account level. An additional analysis, done at the general ledger account level, also may be required to identify all the entity's significant accounts.

(continued)

	Account Characteristics								
Accounts	Size and Composition	Loss	Transactions	Account Type	Complexities	Loss Exposure	Contingent Liability	Related Party	Changes
Cash									
Receivables									
Inventory									
Prepaids									
Fixed Assets									
Goodwill and intangible assets									
Payables									
Debt									
Current income taxes									
Deferred taxes									
Capital									
Retained earnings									

	Account Characteristics *(continued)*								
Accounts	Size and Composition	Loss	Transactions	Account Type	Complexities	Loss Exposure	Contingent Liability	Related Party	Changes
Revenue									
Cost sales									
Occupancy									
Marketing									
Payroll									
G&A									
Income tax									

Controls Over the Selection and Application of Accounting Policies

Financial statement preparers frequently have many decisions to make in the selection and application of accounting policies. For example, generally accepted accounting principles may allow a company to account for a given event or transaction in a variety of ways. One example would be depreciation expense, which the company may determine using several different methods, each of which is acceptable (that is, *select* an accounting policy). To apply a given accounting method, the company may need to make several judgments. In the case of depreciation expense, once the company chooses a depreciation method, judgments would need to be made about asset useful lives, salvage values (for example, *apply* the selected policy). In the final analysis, the company's selection and application of accounting policies should produce financial statements that are "presented fairly."

Auditing Standard No. 2 does not provide guidance on the controls that should be in place relative to a company's selection and application of the accounting policies included in the company's financial statements. However, other auditing literature[1] on this topic requires the external auditor to make certain communications to company management and the audit committee regarding the company's:

- Selection of new accounting policies
- Changes to existing accounting policies
- Accounting policies relating to significant financial statement items, including the timing of transactions and the period in which they are recorded

Guidance pertaining to the controls that should be in place regarding the selection and application of significant accounting policies indicates that:[2]

- The audit committee should be informed about the initial selection of and subsequent changes to significant accounting policies or their application.
- The audit committee should be informed about the methods used to account for significant unusual transactions, which may include:[3]
  - — Bill-and-hold transactions
  - — Self-insurance

[1] See AICPA Statement on Auditing Standards (SAS) No. 61, *Communication With Audit Committees* (AICPA, *Professional Standards,* vol. 1, AU sec. 380). The Securities and Exchange Commission (SEC) references this same guidance in Release No. 33-8040, "Cautionary Advice Regarding Disclosure About Critical Accounting Policies."

[2] See SAS No. 61 (AU sec. 380.07).

[3] The following list of items was adapted from nonauthoritative technical guidance provided by the SEC Practice Section of the AICPA. See PITF 2000-2, *Quality of Accounting Principles—Guidance for Discussions with Audit Committees*, item 3.7.

— Multielement arrangements contemporaneously negotiated

— Sales of assets or licensing arrangements with continuing involvement of the enterprise

- The audit committee should be informed about the effect of significant accounting policies in controversial or emerging areas for which there is a lack of authoritative accounting guidance or consensus. For example, significant accounting issues may exist in areas such as:

  — Revenue recognition

  — Off-balance-sheet financing

  — Accounting for equity investments

  — Research and development activities

  — Special purpose financing structures that affect ownership rights (such as leveraged recapitalizations, joint ventures, and preferred stock of subsidiaries)

Antifraud Programs and Controls

Management is responsible for designing and implementing systems and procedures for the prevention and detection of fraud and, along with the board of directors, for ensuring a culture and environment that promotes honesty and ethical behavior. The internal control Auditing Standard requires these antifraud programs and controls to be included within the scope of management's documentation, testing, and evaluation process.

The framework, *Internal Control—Integrated Framework*, issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), does not include a discussion of antifraud measures, and there is no widely accepted antifraud equivalent to COSO. However, in 2002 a group of seven accounting professional organizations (including the AICPA) jointly published *Management Antifraud Programs and Controls: Guidance to Help Prevent, Deter, and Detect Fraud.* This document listed three fundamental activities as being essential to implementing antifraud programs and controls:

- Create and maintain a culture of honesty and high ethics
- Evaluate the risks of fraud and implement the processes, procedures, and controls needed to mitigate the risks and reduce the opportunities for fraud
- Develop an appropriate oversight process

This document should be helpful in understanding the elements of an entity's antifraud programs and controls that should be documented. The entire document is included as Appendix C to this Practice Aid.

IT General Controls

The COSO framework identifies two types of IT-related controls: general computer controls and application-specific controls.

- *General controls* include controls over:
  - — Data center operations, for example, job scheduling, backup and recovery procedures.
  - — Systems software controls, for example, the acquisition and implementation of operating systems.
  - — Access security.
  - — Application system development and maintenance controls, for example, the acquisition and implementation of individual computer software applications.
- *Application controls* are designed to control information processing and ensure the completeness and accuracy of transaction processing, authorization, and validity. Application controls also encompass the way in which different applications interface with each other and exchange data.

The COSO report does not mandate this framework for assessing the effectiveness of internal controls but states that this is one set of groupings of IT-related control activities that can be used.

Many entities will find the COSO guidance on IT-related controls to be insubstantial and may look for additional guidance. The Control Objectives for Information and Related Technology (COBIT) framework is a good source for such guidance.

The COBIT Framework

Since the release of COSO, the Information Systems Audit and Control Association and Foundation (ISACA) has developed its COBIT framework, which provides a generally applicable and accepted standard for information technology (IT) security and control practices. Among IT audit professionals, COBIT is widely accepted.

The COBIT framework is similar to COSO in that it puts controls in the context of an entity's need to achieve certain business objectives and the risks it faces in reaching those objectives. In defining the goals of IT governance and control, COBIT takes a rather broad brush and does not limit itself to the financial reporting process. For the purpose of complying with the SEC internal control reporting requirements, management should limit its consideration of IT controls to those that affect the reliability of financial reporting, either directly (for example, application controls) or indirectly (for example, general controls).

COBIT groups the IT processes into four categories, each of which is critical in delivering information that meets certain stated criteria:

- *Planning and organization.* These processes cover strategy and tactics, and address how IT can best contribute to the achievement of stated business objectives, both now and in the future.
- *Acquisition and implementation.* To realize the IT strategy, IT solutions need to be identified, developed, or acquired, as well as implemented and integrated into business processes.
- *Delivery and support.* These processes include the actual processing of data by application systems.
- *Monitoring.* All IT processes need to be regularly assessed over time for their quality and compliance with control requirements.

Note that the delivery and support category of processes is analogous to the COSO category of application controls. The other categories identified by COBIT approximate the general controls described by COSO but are somewhat broader in scope.

Information Technology Governance Institute (ITGI), in conjunction with the ISACA, has published *IT Control Objectives for Sarbanes-Oxley*. This publication is intended to help IT professionals understand management's required reporting on the effectiveness of internal control and to plan and perform procedures to help management comply with these requirements. The document also provides an important bridge between the control components described in the COBIT framework and those described by COSO.

The document also can be used by company management as a means for understanding the overall objectives and general procedures for an IT review of internal control over financial reporting. The document can be downloaded from either the ITGI Web site at www.itgi.org or the ISACA Web site at www.isaca.org.

Accounting Estimates

The internal control Auditing Standard requires management's assessment process to include controls over significant estimates. Guidance on these controls is provided in another auditing standard,[4] which states:

> Specific relevant aspects of internal control [over accounting estimates] include the following.
>
> *a.* Management communication of the need for proper accounting estimates
>
> *b.* Accumulation of relevant, sufficient, and reliable data on which to base an accounting estimate

[4] See AICPA SAS No. 57, *Auditing Accounting Estimates* (AICPA, *Professional Standards*, vol. 1, AU sec. 342.06).

c. Preparation of the accounting estimate by qualified personnel

d. Adequate review and approval of the accounting estimates by appropriate levels of authority, including—

1. Review of sources of relevant factors
2. Review of development of assumptions
3. Review of reasonableness of assumptions and resulting estimates
4. Consideration of the need to use the work of specialists
5. Consideration of changes in previously established methods to arrive at accounting estimates

e. Comparison of prior accounting estimates with subsequent results to assess the reliability of the process used to develop estimates

f. Consideration by management of whether the resulting accounting estimate is consistent with the operational plans of the entity.

In addition, the audit committee should be informed about the process used by management in formulating particularly sensitive accounting estimates.

Company-Level Controls

The Auditing Standard introduces a new term, *company-level controls*, which it uses to describe certain controls, such as the control environment, that have a pervasive effect on the functioning of other controls and that reside at the company level. Company-level controls are in contrast to activity-level controls, which exist at the transaction or business process level, for example, the matching of invoices and shipping documents for the sale of goods, and whose influence is limited to that transaction or process.

Although the term *company-level controls* is new, the concept is not; many of the control components described in the COSO report are acknowledged as being applied at the company level, rather than at the activity level.

The Auditing Standard requires the scope of management's assessment process to include company-level controls. **Paragraphs 52 and 53** of the standard state the following.

> 52. *Identifying Company-Level Controls.* Controls that exist at the company level often have a pervasive impact on controls at the process, transaction, or application level. For that reason, as a practical consideration, it may be appropriate for the auditor to test and evaluate the design effectiveness of company-level controls first, because the results of that work might affect the way the auditor evaluates the other aspects of internal control over financial reporting.
>
> 53. Company-level controls are controls such as the following:
>
> - Controls within the control environment, including tone at the top, the assignment of authority and responsibility, consistent policies and procedures, and company-wide programs, such as codes of conduct and fraud prevention, that apply to all locations and business units (see paragraphs 113 through 115 for further discussion);

- Management's risk assessment process;
- Centralized processing and controls, including shared service environments;
- Controls to monitor results of operations;
- Controls to monitor other controls, including activities of the internal audit function, the audit committee, and self-assessment programs;
- The period-end financial reporting process; and
- Board-approved policies that address significant business control and risk management practices.

Note: The controls listed above are not intended to be a complete list of company-level controls nor is a company required to have all the controls in the list to support its assessment of effective company-level controls. However, ineffective company-level controls are a deficiency that will affect the scope of work performed, particularly when a company has multiple locations or business units, as described in Appendix B.

Practice Pointer. The standard recommends that external auditors test company-level controls *first* before testing activity-level controls. The standard points out that these controls should be tested first because what you learn from these tests will affect the nature, timing, and extent of your tests of activity-level controls. There is another equally important reason to test company-level controls first. If weaknesses are found in company-level controls, management must make changes to correct these deficiencies. Some changes, most notably to the control environment and the "tone at the top," will require a significant period of time to effectively implement.

Although not required, company management also may want to test company-level controls first, before testing activity-level controls.

Observations About the Requirements

- Paragraphs 52 and 53 in the standard impose no additional requirements on company management. However, they do make the point of distinguishing between activity-level and company-level controls, and there is a good reason for doing this. First, as noted in the standard, testing company-level controls will lead to more effective and efficient audits. Understanding the distinction between company-level and activity-level controls is important for other reasons as well.

  — *Nature of the control.* Activity-level controls tend to be transaction-oriented. During an audit period, the control procedure may be performed hundreds or thousands of times. Company-level controls may not be transaction-oriented but more policy-oriented. Some company-level control procedures may be performed only a few times during the audit period.

  — *Nature of tests.* Because of their transaction-oriented nature, activity-level controls lend themselves to the testing of individual transactions; because the procedures may have been performed numerous times, sampling techniques may be necessary. Policy-oriented controls may not lend themselves to transactions testing or walkthroughs. If a company-level procedure is performed only once a quarter, for example, period-end financial reporting process, the company will need to carefully plan its tests if you are to observe the procedure on a real-time basis.

- The standard describes three of the COSO components as operating at the company level: risk assessment, monitoring, and the control environment. It is natural to consider risk assessment and moni-

toring at the activity level, but these paragraphs remind you that these two control components also should function at the company level.

- The standard makes reference to centralized processes and controls, and these may include processes and controls that are physically maintained and implemented at a separate entity—for example, a third-party service organization. Appendix B to the standard discusses considerations when the entity uses a third-party service organization, and this guidance will be discussed later in this chapter.

Period-End Financial Reporting Processes

Paragraph 78 of the standard states that the client's period-end financial reporting process is *always* a significant process.

Paragraph 76 defines the period-end financial reporting process as consisting of the following:

- The procedures used to enter transaction totals into the general ledger;
- The procedures used to initiate, authorize, record, and process journal entries in the general ledger;
- Other procedures used to record recurring and non-recurring adjustments to the annual and quarterly financial statements, such as consolidating adjustments, report combinations, and classifications; and
- Procedures for drafting annual and quarterly financial statements and related disclosures.

Paragraph 77 requires an understanding of the following:

- The inputs, procedures performed, and outputs of the processes the company uses to produce its annual and quarterly financial statements;
- The extent of information technology involvement in each period-end financial reporting process element;
- Who participates from management;
- The number of locations involved;
- Types of adjusting entries (for example, standard, non-standard, eliminating, and consolidating); and
- The nature and extent of the oversight of the process by appropriate parties, including management, the board of directors, and the audit committee.

Other Engagement Scope Considerations

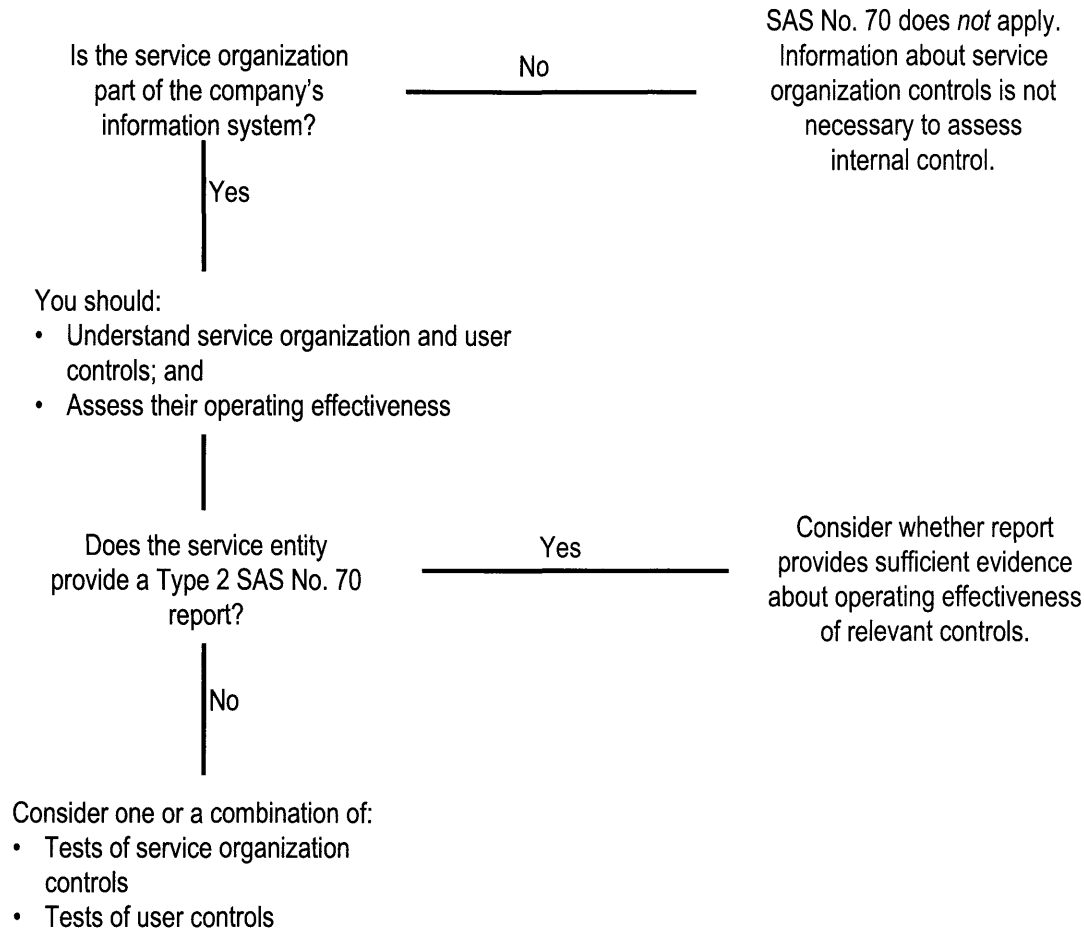
Use of Service Organizations

Your company may use a service organization to perform a wide variety of services related to the preparation of its financial statements. These services may include executing transactions and maintaining related accountability, recording transactions, and processing data. When a company uses a service organization to process transactions, those transactions are subject to the service organization's controls. This situation raises the issue of the nature and extent of documentation and testing management should obtain about the controls in place at the service organization.

Appendix B, paragraphs B18 through B29 of the Auditing Standard, provide guidance on how the company's use of a service organization should be considered in an audit of internal control. Essentially, the guidance summarizes and refers you to the guidance provided in AICPA Statement on Auditing Standards (SAS) No. 70, *Service Organizations* (AICPA, *Professional Standards*, vol. 1, AU sec. 324).

Exhibit 2-3 provides an overview of the key questions you should consider when your company uses a service organization.

Exhibit 2-3 Use of a Service Organization



Determining Whether the Service Organization Is Part of the Information System

SAS No. 70 (AU sec. 324.03) states that a service organization's services are part of your company's information system if they affect any of the following.

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

When a service organization performs services that are part of a company's information system, the related controls over those services may reside either at the service organization, the company (referred to in the auditing literature as the "user organization") or, as frequently is the case, at both locations.

Practice Pointer. Over the past several years, many entities have "outsourced" many of their business activities that previously were performed in-house. Typically, these outsourced service providers have not been considered "service organizations." However, in some circumstances, these service providers may meet the criteria listed above and may be considered part of the client's information system. In planning your company's assessment of internal control, you should review its use of outsourcing and determine whether controls at any outsourced service providers should be in the scope of the project.

Service Organization Is Part of Information System

When a service organization is part of your company's information system you should:

- Obtain an understanding of the controls at the service organization that are relevant to the company's internal control and the controls at the company over the services provided by the service organization.
- Obtain evidence that the controls that are relevant to management's assessment *are operating effectively*.

To obtain this understanding of controls and their operating effectiveness, the company may:

- Perform tests of the controls located at the company that pertain to the services provided by the service organization, for example, testing the company's independent reperformance of selected items processed by the service organization or testing the company's reconciliation of the service organization's output reports with source documents that were prepared by the company.
- Perform tests of controls at the service organization.
- Obtain a service auditor's report on controls placed in operation and tests of operating effectiveness, or a report on the application of agreed-upon procedures that describes relevant tests of controls.

Not all of a service organization's controls are relevant for planning and performing an assessment of internal control. In determining which service organization controls are relevant, you should consider:

- The relevant assertions in the company's financial statements
- The control objectives of the service organization related to those assertions
- The controls in place at the service organization to meet those control objectives

The Service Organization and SAS No. 70 Reports

A service organization may engage an auditor (the service auditor) to report on controls at the service organization that affect the financial statements of user organizations; such reports may be used by user organizations and their external auditors. There are two types of reports a service auditor might issue, which are summarized in Exhibit 2-4.

Exhibit 2-4 Summary of Service Auditor Reports

Title	*Contents*	*Relevance to the Company*
Reports on Controls Placed in Operation (Type 1 Report)	• Describes controls and whether they are suitably designed to achieve specified control objectives. • States whether controls had been placed in operation by a specified date.	• Provides an understanding of control design effectiveness. • Does *not* provide a basis for assessing operating effectiveness.
Report on Controls Placed in Operation and Tests of Operating Effectiveness (Type 2 Report)	Includes all elements of the Report on Controls Placed in Operation, *plus*: • An opinion about whether the controls that were tested were operating effectively.	Has the same utility as a Type 1 report, and, in addition: • Provides a basis for assessing operating effectiveness of controls for a period of time.

In your assessment of internal control you must evaluate the operating effectiveness of internal control. Only a Type 2 SAS No. 70 report allows you to draw conclusions about the operating effectiveness of internal controls that are located at the service organization and affect user organizations' financial statements. In evaluating whether such a report provides sufficient evidence, you should consider the following:

- The time period covered by the tests of controls and its relation to the date of management's assessment.
- The scope of the examination and applications covered, the controls tested, and the way in which tested controls relate to the company's controls.
- The results of those tests of controls and the service auditor's opinion on the operating effectiveness of the controls.

When a significant period of time has elapsed between the time period covered by the tests of controls in the service auditor's report and the date of your assessment of control effectiveness, you should determine whether additional procedures should be performed. **Paragraph B26** of the standard states that as the following factors increase in significance, the need for you to perform additional procedures also increases.

- The elapsed time between the time period covered by the tests of controls in the service auditor's report and the date of management's assessment,
- The significance of the activities of the service organization,
- Whether there are errors that have been identified in the service organization's processing, and
- The nature and significance of any changes in the service organization's controls identified by management or the auditor.

Recall from Chapter 1 of this Practice Aid that the company is *prohibited* from using the work of the company's external auditors to support management's conclusion about internal control effectiveness. Question 14 of the SEC staff's *Management's Report on Internal Control Over Financial Reporting and Disclosure in Exchange Act Periodic Reports: Frequently Asked Questions* (http://www.sec.gov/info/accountants/controlfaq0604.htm) addresses those situations in which the company's auditors are the same as the service organization's auditors. The staff's view is that, in those situations, "management would be able to rely on the Type 2 SAS No. 70 report even if the auditors for both companies were the same." However, if management *engages* its external auditors to prepare a Type 2 SAS No. 70 report on its service organization, then management would not be able to rely on that report for purposes of assessing internal control. (See SEC staff's FAQ, question 14.)

Additional Resources

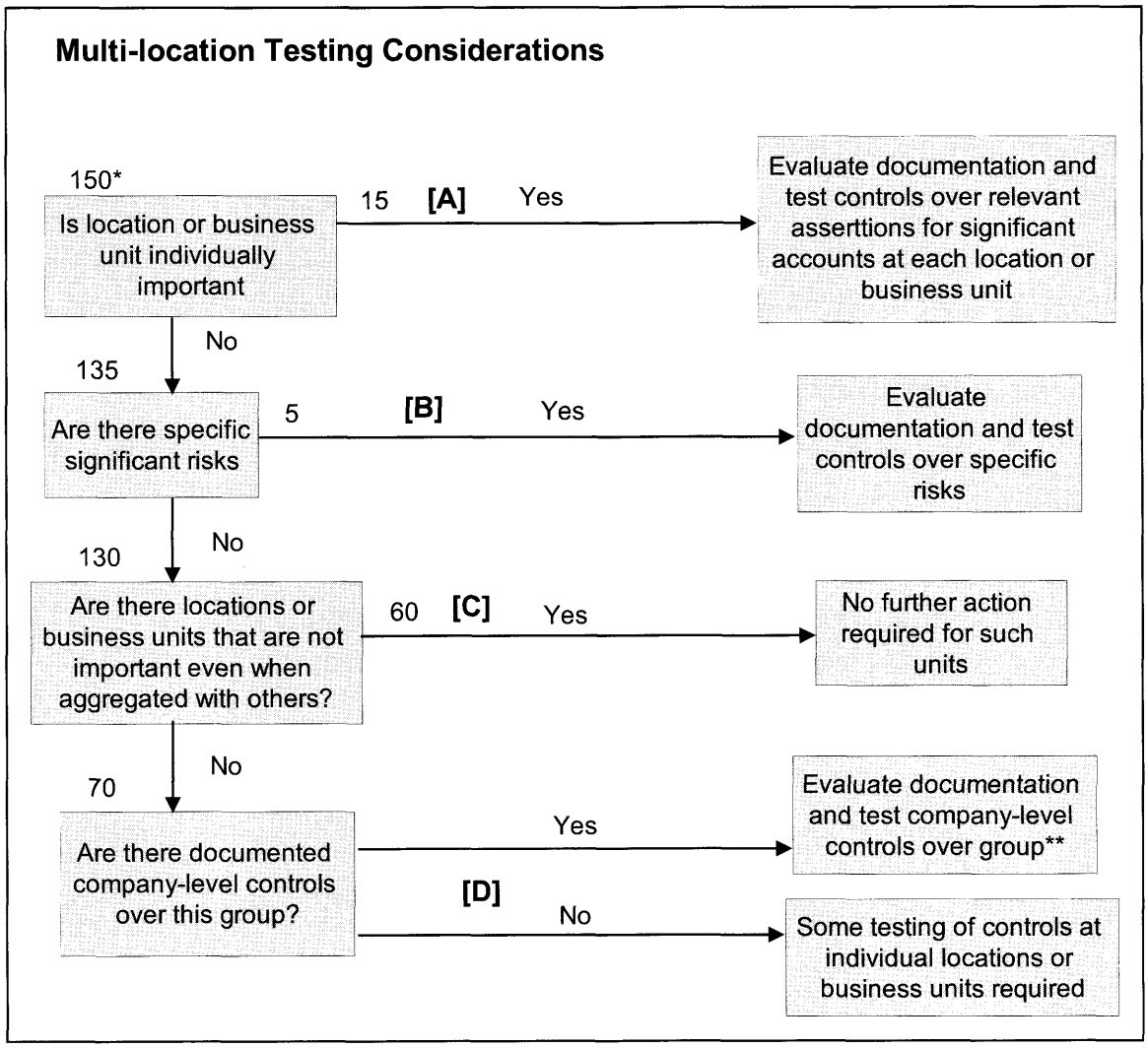
SAS No. 70 provides extensive guidance to external auditors when their clients use service organizations to process information. Although this guidance is applicable to audits of financial statements of nonpublic companies, PCAOB Auditing Standard No. 2 incorporates much of this guidance in establishing standards for management's assessment and the audit of internal control.

The scope of this Practice Aid does not allow a thorough exploration of all the guidance provided in SAS No. 70. For additional information please refer to the Auditing Standard or the AICPA Audit Guide *Service Organizations: Applying SAS No. 70, as Amended.*

Multiple Location/Multiple Business Unit Entities

When your company comprises more than one business unit or it operates in more than one location, you must determine which of those locations or business units should be included in the scope of your assessment project. The Auditing Standard provides explicit guidance on how to make this determination. Exhibit 2-5 is a reproduction of **Illustration B-1** from Appendix B of the standard, and this illustration summarizes the guidance contained in paragraphs B1 through B12. This illustration is annotated here to cross-reference the guidance to the comments that follow.

Exhibit 2-5



Observations About the Requirements

In this example from the Auditing Standard, the company that is evaluating its internal control operates in 150 locations. For example, suppose that the company is a retailer that operates 150 stores. The question is which and how many of these retail stores should be included in the scope of its assessment project. Note that the numbers represent the number of locations in our illustrative company that meet the criterion.

A. The first step in the process is to determine the relative financial significance of the locations and identify those locations that *individually* are considered to be financially significant. The standard states that, "generally, a relatively small number of locations or business units will encompass a large portion of a company's operations and financial position, making them financially significant." In this example, 15 of the retail stores are considered to be individually significant.

For each of these individually significant locations, you should, for all relevant assertions related to significant accounts and disclosures:

- Evaluate the documentation of internal control; and
- Perform tests to determine the design and operating effectiveness of the controls.

Paragraph A16 of the PCAOB staff's FAQs clarifies that to apply this guidance you should first determine the significant accounts and relevant assertions at the consolidated financial statement level. Next, you would evaluate documentation and test the controls for those accounts only at the significant location for which the selected accounts are material. Thus, if you identify accounts receivable as a significant account, but at location A, receivables are immaterial, you do not have to test the controls over receivables at location A. However, if accounts receivable is material at a location or business unit that is not otherwise considered financially significant, the external auditor should test controls over all relevant assertions for accounts receivable at that location. This direction is consistent with the directions in paragraph B6 addressing locations or business units that involve specific risk.

B. In this example, we started with 150 separate locations. Of these, 15 were determined to be individually significant, which leaves 135 to evaluate.

The next test is to determine whether any of these remaining locations pose certain specific risks that, by themselves, could create a material misstatement. For example, suppose that, instead of a retailer, the company in our example was a financial institution that operated in multiple locations. One of the locations was actively involved in trading derivatives. Suppose that the financial results and level of activity of the derivatives trading were not significant to the entity's financial statements. However, because of the significant potential risks posed to the company by the derivatives trading activity, you would want to include this location within the scope of your engagement. In these circumstances, you would limit your testwork to *the specific identified risks* and not consider the entire location or business unit.

C. In this example, 20 locations meet one of the conditions already considered. What remains are 130 locations, and none of these locations is individually significant. The next step is to consider which of these remaining locations, *when aggregated*, might have a high level of financial significance, which is defined as one that:

> Could create a greater than remote risk of material misstatement of the financial statement.

Locations that meet this condition are passed along to Step D in the process. Those that do *not* meet this condition are locations that are insignificant, both individually and when combined. No additional work is required for these locations. In our example, 60 locations meet this condition.

D. Finally, we are left with locations that are not individually significant but which, if left untested, would constitute a high level of financial significance as a group. You are now faced with determining which of these locations should be visited and/or tested individually.

To do this, you first should determine whether the client has company-level controls that are operating effectively over this remaining group of locations or business units. To determine whether these company-level controls are indeed effective, **paragraph B9** of the Auditing Standard notes only that you "might conclude that [you] cannot evaluate the operating effectiveness of such [company-level] controls without visiting some or all of the locations or business units." Thus, if company-level controls exist, you must use your judgment to determine which, if any, locations need to be tested to support your conclusion about the operating effectiveness of these controls over this population of locations.

However, **paragraph B11** cautions that "testing company-level controls is not a substitute for . . . testing of controls over a large portion of the company's operations or financial position. If [you] cannot test a large portion of the company's operations and financial position by selecting a relatively small number of locations or business units, [you] should expand the number of locations or business units selected." The standard does *not* name a specific percentage of what would constitute a "large portion" but leaves that to your judgment.

If company-level controls do *not* exist, the standard requires you to select some or all locations for detailed testing. To determine which locations or business units to visit and the controls to test, **paragraph B10** requires you to evaluate the following factors.

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

Practice Pointer. For entities such as retailers, banks, or others that have a large network of branches or locations engaged in the same or essentially the same business transactions, the scope of the assessment project will depend largely on whether the company:

- Is characterized by strong, centralized controls and processes.
- Has effective company-level controls that encompass all its locations.

In these circumstances and others in which a company has a very large number of individually insignificant locations or business units and management believes that controls have been documented and are effective at all locations, you may be able to test a representative sample of these locations.

Paragraph A18 of the PCAOB staff's FAQs addresses this issue. When using sampling techniques for this purpose, the staff recommends the following:

- The sample should be representative of the entire population.
- Your sampling will be based on the expectation of no, or very few, control testing exceptions.
- The existence of testing exceptions would not support your underlying belief that controls had been documented and were effective.

- Therefore, if you use a sampling technique and encounter testing exceptions beyond a negligible rate, you may need to test a large number of individual locations or business units.

Early in the planning process, you should evaluate your company's overall approach to controlling its network of locations, and you should plan on testing company-level controls early. Be sure to allow yourself the flexibility to increase the scope of your project should you determine that company-level controls do *not* operate effectively.

Compliance With Laws and Regulations

The SEC rules (Release No. 33-8238) define *internal control over financial reporting*. Included in that definition is "compliance with applicable laws and regulations directly related to the preparation of financial statements."

Questions have been raised about whether this inclusion of laws and regulations includes the possible accrual or disclosure of a contingency related to the violation of laws and regulations—which is a circumstance that might have a material effect on the reliability of financial reporting. Answer 27 of the PCAOB staff's FAQs (http://www.pcaobus.org/documents/Staff_Q_and_A/Auditing_Internal_Control_over_Financial_Reporting_2004-10-06.pdf) provides guidance on this matter.

The PCAOB staff believes that, yes, the definition of internal control over financial reporting "encompasses controls over the identification, measurement, and reporting of all material actual loss events which have occurred, including controls over the monitoring and risk assessment of areas in which, given the nature of the company's operations, such actual loss events are reasonably possible." As such, these controls should be included in the scope of your assessment of internal control.

Other Scope Considerations

The SEC staff's answers to frequently asked questions provides additional guidance on issues relating to the scope of the company's assessment process.

- *Variable interest entities (VIEs) and proportional consolidations.* Ordinarily, the SEC would expect management's report on internal control to include *all* consolidated entities, including VIEs and those accounted for via proportional consolidation. However, these entities may be *excluded* from the scope of management's assessment if all of the following conditions are met.
  - — The variable interest entity was in existence before December 15, 2004.
  - — The VIE would *not* have been consolidated absent the application of FASB Interpretation No. 46, *Consolidation of Variable Interest Entities*.
  - — The company does not have the right or authority to assess the internal controls of the consolidated entity and also lacks the ability, in practice, to make that assessment.

If all of the above conditions are met, the company does *not* have to include the VIE in its control assessment process. However, the company should make the following disclosures.

— A reference in the 10K to the scope of management's report on internal control.

— A statement that the company has not evaluated the internal controls of the entity excluded from its scope and any conclusions regarding internal control do not extend to that entity.

— Key sub-totals that result from consolidation of entities whose internal controls have not been assessed.

— A statement that the financial statements include the accounts of certain entities consolidated pursuant to FASB Interpretation No. 46, Emerging Issues Task Force (EITF) Issue No. 00-1, *Investor Balance Sheet and Income Statement Display under the Equity Method for Investments in Certain Partnerships and Other Ventures*, but that management has been unable to assess the effectiveness of internal control at those entities due to the fact that the registrant does not have the ability to dictate or modify the controls of the entities and does not have the ability, in practice, to assess those controls.

- *Equity method investments.* Controls over the recording of transactions into the investee's accounts are not part of the company's internal control. That is, if the company has equity method investments, the controls that relate to investee's transactions are outside the scope of the company's internal control. However, the company should have controls over the recording of amounts in its own financial statements, such as the recognition of equity method earnings and losses, or its investment account balance.
- *Business combinations during the year.* Ordinarily, the SEC staff would expect management's assessment process to include controls over business combinations during the year. However, the staff recognizes that it might not always be possible to conduct such an assessment between the consummation date of the acquisition and year end. Thus, the SEC will not object to the company *excluding* such a business combination from its internal control assessment, provided that:

  — The company identifies the acquired business and its relative significance to the financial statements and discloses that the acquired business has been excluded from the company's assessment of internal control.

  — The company discloses any material change to its internal control due to the acquisition.

  — The exclusion of the acquired business from the scope of the company's internal control assessment may not extend beyond one year from the date of acquisition.

  — The exclusion of the acquired business cannot be for more than one annual management report on internal control.

SUMMARY

Determining the scope of your assessment project will be a significant part of your planning effort. The auditing standard requires the scope of the project to include all of the following control areas:

- Activity-level controls related to all relevant assertions for all significant accounts.
- Controls over the selection and application of accounting policies.
- Controls over accounting estimates.
- The monitoring of internal control effectiveness.
- The control environment.
- Other company-level controls, including:
  - — Centralized processing and controls, including shared services.
  - — Period-end financial reporting processes.
  - — Board-approved policies that address significant business control and risk management practices.
  - — Antifraud programs and controls.
  - — Information technology general controls.

Finally, you should consider how the company's use of a service organization or the existence of multiple locations or business units will affect engagement scope.

CHAPTER 3: DOCUMENTATION OF INTERNAL CONTROL

REQUIRED DOCUMENTATION

The previous chapter describes how the external auditors evaluate the company's process for assessing the effectiveness of its internal control. Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, PC sec. 140), provides detailed guidance to external auditors on what should be included in that process, and it is in the company's best interests to ensure that it, too, follows this guidance.

Similarly, the external auditors evaluate the adequacy of management's documentation of internal control. Again, the consequences of not complying with the requirements of the Auditing Standard are severe. Paragraphs 45 and 46 of the standard state that inadequate documentation is an internal control deficiency that may constitute a significant deficiency or may even rise to the level of a material weakness. Without adequate documentation, management's ability to adequately monitor the entity's internal control (one of the five control components defined by the framework, *Internal Control—Integrated Framework*, issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)) may be compromised. Lack of adequate documentation may also result in a scope limitation on the audit of internal control. The external auditor's options when a scope limitation exists are covered in Chapter 2 of this Practice Aid.

Paragraph 42 of the standard provides the requirements for your documentation of internal control. That paragraph requires management's documentation to include the following.

- The design of controls over all relevant assertions related to all significant accounts and disclosures in the financial statements. The documentation should include the five components of internal control over financial reporting as discussed in paragraph 49, including the control environment and company-level controls as described in paragraph 53;
- Information about how significant transactions are initiated, authorized, recorded, processed and reported;
- Sufficient information about the flow of transactions to identify the points at which material misstatements due to error or fraud could occur;
- Controls designed to prevent or detect fraud, including who performs the controls and the related segregation of duties;
- Controls over the period-end financial reporting process;
- Controls over safeguarding of assets (See paragraphs C1 through C6); and
- The results of management's testing and evaluation.

Observations About the Requirements

- The company's documentation must link the controls to financial statement assertions. A mere description of the control procedure, for example, "Ann Brown in the finance department performs bank reconciliations," is not sufficient. Without linking the control to the relevant assertion, there is no way of knowing whether all of the assertions relevant for a particular account have been "covered' by all the controls.
- The documentation is required for all "significant accounts," which were defined in Chapter 2 of this Practice Aid.
- You are required to document all five components of internal control. Additional guidance on complying with this requirement is discussed in the next section of this chapter.
- The Auditing Standard provides guidance on what is required of the entity's period-end financial reporting process. This guidance is in Chapter 2 of this Practice Aid.
- Safeguarding of assets is defined in **paragraph 7(3)** of the standard as those policies and procedures that "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements." Appendix B of this Practice Aid provides further guidance on the safeguarding of assets.
- The Auditing Standard does not require the documentation to be in a particular format. **Paragraph 43** of the standard states, "Documentation might take many forms, such as paper, electronic files, or other media, and can include a variety of information, including policy manuals, process models, flowcharts, job descriptions, documents, and forms. The form and extent of documentation will vary depending on the size, nature, and complexity of the company."

COSO Control Components

The first bullet point in **paragraph 42** states that your documentation should include "the five components of internal control." The remaining bullet points describe certain other required elements of documentation and refer the reader to the definition of company-level controls provided in paragraph 53. Questions may arise about the relationship between the detailed bullet points in paragraphs 42 and 53 and the five COSO components. For example:

- How do the bullet points in paragraphs 42 and 53 relate to the five COSO components?
- If the company's documentation includes each of the bullet points listed in paragraphs 42 and 53, does it satisfy the requirement to document each of the five control components?

Exhibit 3-1 sets forth the relationship between the requirements of paragraphs 42 and 53 and how these relate to the COSO components. As the table points out, there is some overlap between the two requirements; however, the requirement that you document each of the COSO components will require you to prepare additional documentation that goes beyond the detailed requirements of paragraph 42.

Exhibit 3-1 Documenting Each Component of Internal Control

Documentation Requirement of Paragraph 42	*Related COSO Control Component*	*Author's Observations*
1. Controls for all significant accounts	Control activities	Compliance with the requirements of paragraph 42 probably allows you to satisfy the requirements to document the COSO control components, as indicated. However, note that items 2 and 3 refer only to the accounting information system and *not* to the communications part of COSO's "information and communication" component.
2. Information about initiation, authorization, processing and reporting	Information	
3. Flow of transactions	Information	
4. Antifraud programs and controls	N/A	
5. Period-end financial reporting process	Information control activities	
6. Safeguarding of assets	N/A	

Documentation Requirement of Paragraph 53	*Related COSO Control Component*	*Author's Observations*
1. Control environment	Control environment	Compliance with the requirements of paragraph 53 probably allows you to satisfy the requirements to document the COSO control components, as indicated.
2. Management's risk assessment process	Risk assessment	
3. Centralized processing and controls	N/A	
4. Controls to monitor results of operations	N/A	
5. Controls to monitor other controls	Monitoring	
6. Period-end financial reporting process	N/A	
7. Certain board-approved policies	Control environment	

—	Communications	The control component listed in the middle column will require you to prepare documentation *in addition to* the documentation listed in detailed bullet point items of paragraphs 42 and 53.

The Auditing Standard does not provide guidance on the how to document "each of the five components of internal control." However, paragraph 42 does reference you to the requirements of paragraph 49. That paragraph of the standard describes the *external auditor's* requirements, not management's.

Paragraph 49 of the standard requires *the external auditor* to obtain an understanding of the five COSO components, and it provides guidance on what is required of the external auditor to obtain this understanding. As you read this paragraph, you should consider that part of the external auditors' procedures for obtaining the requisite understanding will be their review of your documentation. In that context, your understanding of what the external auditors will look for may be helpful as you prepare your documentation of each of the five COSO components.

Paragraph 49 provides guidance to external auditors on what to consider when reviewing the company's documentation of the COSO control components. Exhibit 3-2 reproduces this guidance combined with some observations about its implications.

Exhibit 3-2 The Five Elements of Internal Control

Requirements of the Standard	*Observations*
• *Control Environment.* Because of the pervasive effect of the control environment on the reliability of financial reporting, the auditor's preliminary judgment about its effectiveness often influences the nature, timing, and extent of the tests of operating effectiveness considered necessary. Weaknesses in the control environment should cause the auditor to alter the nature, timing, or extent of tests of operating effectiveness that otherwise should have been performed in the absence of the weaknesses.	In general, the standard emphasizes the importance of the control environment. During your assessment of internal control, you should be sure to test and evaluate the control environment. The standard also recommends that you evaluate the control environment first, before you test activity-level control procedures. As indicated here, the results of your tests of the control environment will influence your tests of activity-level controls.

Exhibit 3-2 The Five Elements of Internal Control *(continued)*

Requirements of the Standard	*Observations*
• *Risk Assessment.* When obtaining an understanding of the company's risk assessment process, the auditor should evaluate whether management has identified the risks of material misstatement in the significant accounts and disclosures and related assertions of the financial statements and has implemented controls to prevent or detect errors or fraud that could result in material misstatements. For example, the risk assessment process should address how management considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements. Risks relevant to reliable financial reporting also relate to specific events or transactions.	In an assessment of internal control, be sure you are evaluating the risk assessment process. What does management do to evaluate and respond to the risk of misstatement in an account?
• *Control Activities.* The auditor's understanding of control activities relates to the controls that management has implemented to prevent or detect errors or fraud that could result in material misstatement in the accounts and disclosures and related assertions of the financial statements. For the purposes of evaluating the effectiveness of internal control over financial reporting, the auditor's understanding of control activities encompasses a broader range of accounts and disclosures than what is normally obtained for the financial statement audit.	The last sentence in this paragraph is significant. In an audit of internal control, the auditors will test controls over more accounts than they traditionally have in their financial statement audit. Be prepared for this increased scope.

(continued)

Exhibit 3-2 The Five Elements of Internal Control *(continued)*

Requirements of the Standard	*Observations*
• *Information and Communication.* The auditor's understanding of management's information and communication involves understanding the same systems and processes that he or she addresses in an audit of financial statements. In addition, this understanding includes a greater emphasis on comprehending the safeguarding controls and the processes for authorization of transactions and the maintenance of records, as well as the period-end financial reporting process (discussed further beginning at paragraph 76).	This paragraph also describes how the scope of an audit of internal control will be greater than the tests of controls the external auditor normally performs in a financial statement audit.
• *Monitoring.* The auditor's understanding of management's monitoring of controls extends to and includes its monitoring of all controls, including control activities, which management has identified and designed to prevent or detect material misstatement in the accounts and disclosures and related assertions of the financial statements.	The requirement that you understand management's monitoring of all controls should be taken to imply that management should monitor the other four components described by the COSO framework.

Significant Processes and Major Classes of Transactions

In an assessment of internal control, you are evaluating the controls over a *process*—for example, the way in which information was processed to report transactions in a given general ledger account. In an internal control assessment, your planning does not end when you identify significant accounts. Once those accounts have been identified, you must understand the significant processes and major classes of transactions that affect those accounts.

Paragraph 71 of the standard requires you to "identify each significant process over each major class of transactions affecting significant accounts or groups of accounts." It goes on to state that "major classes of transactions are those classes of transactions that are significant to the company's financial statements."

For each significant process, **paragraph 74** of the standard requires you to:

- 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.

Observations About the Requirements

The second bullet point requires you to identify the "points within the process at which a misstatement . . . could arise." The third bullet point requires you to "identify the controls that management has implemented to address these potential misstatements." In the author's opinion, the requirements of the third bullet should *not* be interpreted to mean that you are required to identify controls at each point where a misstatement could occur. For example, a given control, such as a reconciliation, may be designed to prevent or detect several errors that could occur at various points in the process. In this instance, you may focus your attention on the reconciliation and not necessarily on redundant controls resident at various points in the processing stream.

The key point to the third bullet would seem to be that you should identify the controls that have been implemented to address all of the potential misstatements, not all of the points at which the misstatements may occur.

Optional Documentation Considerations

Documenting Management's Assessment Process

As part of their internal control audit, the external auditors are required to obtain an understanding of and evaluate management's process for assessing the effectiveness of the company's internal control. Paragraph 40 of the Auditing Standard describes a list of elements that should be included in this process, and this list is discussed in detail in Chapter 2 of this Practice Aid.

To facilitate an effective and efficient review of its process, management should consider preparing summary-level documentation that guides the external auditors through the steps the company followed to assess its internal control and comply with the requirements of paragraph 40 of the Auditing Standard.

Organization Scheme

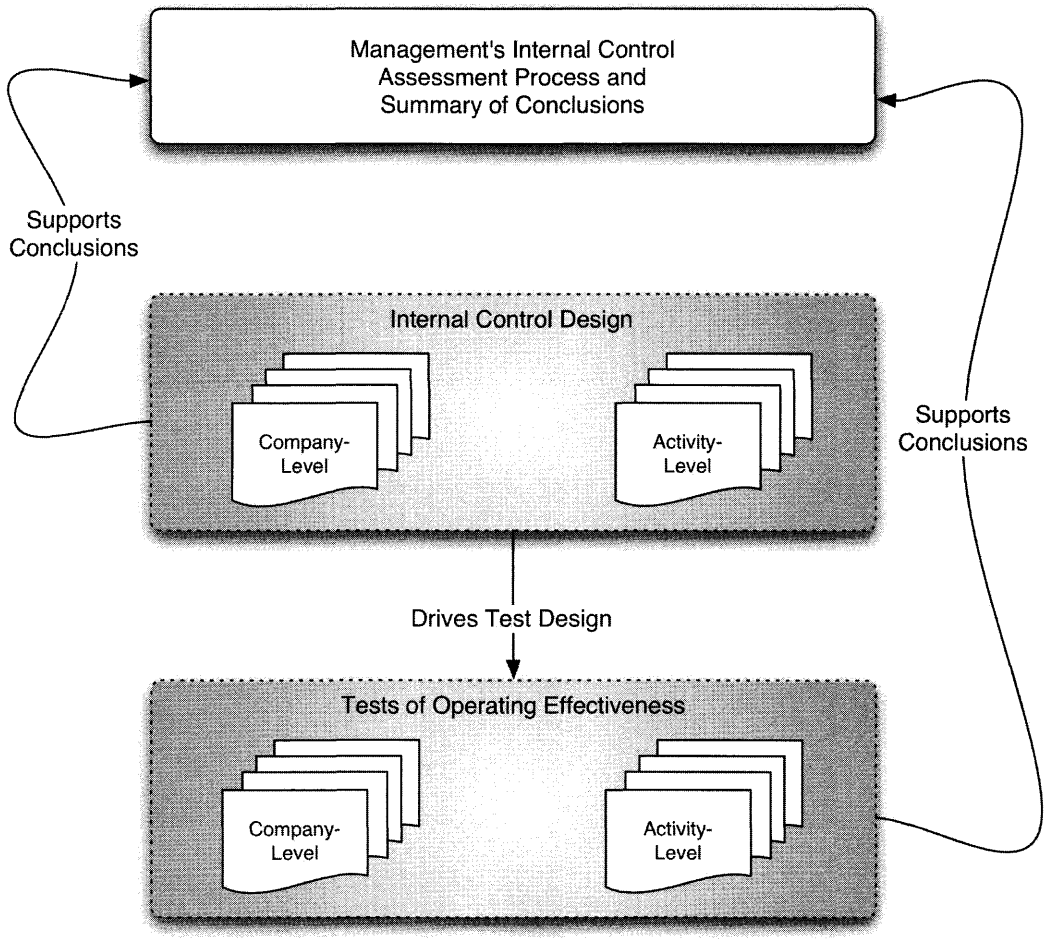
By clearly documenting its process and conclusions, management will effectively guide the external auditors through the support of its assessment of internal control effectiveness. Guiding the external auditors in this way should:

- Decrease the time spent by the external auditors in their audit

- Increase the confidence the external auditors have in the quality of management's process, which allows them to rely more on the company's testwork to reach their audit conclusion
- Improve the effectiveness of management's communications with the external auditors regarding the basis for its conclusions

The documentation of management's process and conclusions will create a three-tiered system of documentation, as indicated in Exhibit 3-3.

Exhibit 3-3 Organizing the Entity's Documentation



In Exhibit 3-3, the summary of management's assessment process and conclusions provides a top-level overview of the entire process. Documentation of internal control design, of both company- and activity-level controls, feeds into this top-level documentation and supports management's conclusions about design effectiveness. The documented design of internal control then serves as a basis for designing tests of operating effectiveness.

Tests of operating effectiveness are performed and the results documented. These results provide the basis for management's conclusions about operating effectiveness of controls.

What to Include in the Documentation of Process and Conclusions

The following are some suggestions for what management might include to document its assessment process.

Significant Accounts and Disclosures

Provide a list of all significant accounts and disclosures together with a rationale for how management made the determination of which accounts were deemed significant. Merely listing all the accounts tested probably will not be sufficient for most external auditors; management should describe how they made their determination.

Chapter 2 of this Practice Aid discusses the Auditing Standard's guidance on determining whether an account is significant and it provides a matrix for how management might document its judgments.

Summary of Conclusions

To facilitate the external audit process and to avoid miscommunication between the external auditor and the company, management should summarize:

- The nature, timing, and extent of tests performed.
- The results of those tests, including the identification and assessment of any internal control deficiencies.
- Management's conclusions about control effectiveness, based on the testwork results.

To clearly communicate the company's control assessment process, the summary of conclusions should distinguish between the following:

- Those related to design effectiveness versus operating effectiveness.
- Those related to the control environment and company-level controls versus activity-level controls.

Subcertification A great deal of the information included in financial statements originates in areas of the company that are outside the direct control of the CEO and CFO. Because of the significance of information prepared by others, the CEO and CFO may request those individuals who are directly responsible for this information to certify it. This process is known as "subcertification," and it usually requires the individuals to provide a written affidavit to the CEO and CFO that will allow them to reach a conclusion on internal control effectiveness in good faith.

Items that may be the subject of subcertification affidavits include the following:

- Adequacy of specific disclosures in the financial statements or other reports filed with the SEC, such as Management's Disclosure and Analysis included in the entity's 10Q or 10K.
- Accuracy of specific account balances.
- Compliance with company policies and procedures, including the company's code of conduct.
- Adequacy of the design and/or operating effectiveness of departmental internal controls and disclosure controls.
- Accuracy of reported financial results of the department, subsidiary, or business segment.

To the extent that management has relied on subcertifications to support their conclusions about internal control, these should be summarized and made available to the external auditors for their review.

Summary of Communications

As discussed in Chapter 1 of this Practice Aid, the external auditors will require management to provide certain written representations. Included in these representations is a statement "that management has disclosed to the auditor all deficiencies in the design or operation of internal control over financial reporting identified as part of management's assessment, including separately disclosing to the auditor all such deficiencies that it believes to be significant deficiencies or material weaknesses in internal control over financial reporting."

To help ensure the effective communication between the company and its external auditors, management should consider briefly summarizing the disclosures it has made to the external auditors regarding internal control deficiencies, including:

- The form of the communication, for example, written or oral
- The content of the communication and the deficiencies identified
- When the communication was made
- The individuals, both from the company and the external auditors, who were involved in the communication

Project Team Qualifications and Work Performed

As discussed in Chapter 1 of this Practice Aid, if certain conditions are met, the external auditors can rely on the work of company employees or others under the direction of management to support their conclusion about internal control effectiveness. In general, the more the external auditors can use the work of the company, the lower the overall costs of compliance for the entity. Thus, it is in the company's best interests to understand the conditions that must be met for the

external auditors to place reliance on the company's work and to document those instances where the conditions have been met.

In general, to use the work of company personnel and others, the external auditors will have to evaluate their:

- Competence
- Objectivity

Details on how the external auditors will evaluate these qualities are provided in Chapter 1 of this Practice Aid.

To facilitate the external auditor's evaluation, the company should document all the items described in Chapter 1 that the external auditor will evaluate and make this documentation available to the external auditors as early in the audit process as possible, to enable them to better plan the scope of their audit.

SUMMARY

Paragraphs 42 and 43 of the Auditing Standard provide guidance to management on the elements that must be included in the company's documentation of its internal control. Failure to comply with these requirements, that is, providing inadequate documentation, is considered a control deficiency that may rise to the level of material weakness. It also may impose a scope restriction on the audit of internal control. Thus, management should take steps to understand the documentation requirements of the Auditing Standard and ensure that its documentation complies. There are no requirements on the form of the documentation, only its content.

In addition to documenting its internal control, management should consider documenting the steps it followed in its assessment process. By clearly documenting these steps, the company will be in a better position to communicate to the external auditors how it complied with the requirements of paragraph 40 of the standard.

CHAPTER 4: INTERNAL CONTROL TESTING

As described in Chapter 2 of this Practice Aid, Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, PC sec. 140), requires that your company's assessment process include:

- Evaluating the design effectiveness of controls.
- Evaluating the operating effectiveness of controls based on procedures sufficient to assess their operating effectiveness.

You are required to evaluate controls over all relevant assertions related to all significant accounts and disclosures.

This chapter summarizes the guidance contained in the Auditing Standard relating to the testing of internal controls. Although this guidance applies directly to the external auditor's testing of internal control effectiveness, you are strongly encouraged to apply this same guidance when planning and performing the company's tests of internal control.

TESTING THE CONTROL ENVIRONMENT AND OTHER COMPANY-LEVEL CONTROLS

Note: Much of the guidance provided in the Auditing Standard relating to the tests of controls is geared toward tests of process-level and transaction-level controls. You should *not* conclude that this paucity of guidance on the control environment and other company-level controls means that these controls do not need to be tested. To the contrary, you definitely are required to assess the design and operating effectiveness of the company's control environment and other company-level controls. Judgment and creativity will be required to apply the general principles regarding the nature, timing, and extent of tests of design and operating effectiveness provided in the Auditing Standard to the testing of company-level controls.

TESTING ACTIVITY-LEVEL CONTROLS

Within an information processing stream, there is often a myriad of different control procedures. In an assessment of internal control, your objective is to assess the effectiveness of internal control *as a whole*, not the effectiveness of each individual control procedure. Thus, when designing your control tests, one of the first issues you must face is determining which activity-level controls to test. That is, you are *not* required to test all controls.

Control Procedures Versus Control Objectives

The internal control Auditing Standard provides guidance to external auditors on determining which control procedures to test. To properly apply this guidance to the company's assessment process, you need to have a solid conceptual understanding of control *objectives* and how these differ from and relate to individual control *procedures*. The purpose of this section is to provide that necessary background.

Control procedures have no value, without a related and well-defined control objective. A company does not perform a control procedure, for example, reconciling a subsidiary ledger to the general ledger account total, because doing so is "good" and to not do so is "bad." A control procedure has value only to the extent that it addresses a specific well-defined control objective.

At its most general level, the objective of internal control over financial reporting is to provide reasonable assurance that the company's financial statements are fairly stated in accordance with generally accepted accounting principles (GAAP). Similarly, at the account level, you could say that the overall objective of internal control is to provide reasonable assurance that the account is free of material misstatement.

The company faces risks in achieving its objectives. The objective of individual control procedures is to reduce these risks to an acceptable level. These risks and the related control objectives are directly related to financial statement assertions. For example, there is a risk that valid transactions are not captured and processed (completeness) or that unauthorized transactions are mistakenly processed (existence or occurrence).

When determining which controls to test, you will need to first understand the control objectives for the relevant assertions for significant accounts. From there, you will be able to determine which controls are most significant and should be tested to determine whether internal controls are designed and operating effectively to meet the stated objective.

Determining the Controls to Test

Paragraph 83 of the standard requires external auditors to (and would therefore strongly suggest that management) evaluate the following to identify the controls to be tested:

- Points at which errors or fraud could occur;
- The nature of the controls implemented by management;
- The significance of each control in achieving the objectives of the control criteria and whether more than one control achieves a particular objective or whether more than one control is necessary to achieve a particular objective; and
- The risk that the controls might not be operating effectively. Factors that affect whether the control might not be operating effectively include the following:
  - — Whether there have been changes in the volume or nature of transactions that might adversely affect control design or operating effectiveness;

— Whether there have been changes in the design of controls;
— The degree to which the control relies on the effectiveness of other controls (for example, the control environment or information technology general controls);
— Whether there have been changes in key personnel who perform the control or monitor its performance;
— Whether the control relies on performance by an individual or is automated; and
— The complexity of the control.

Exhibit 4-1 summarizes these factors and how they might affect the operating effectiveness of a control.

Exhibit 4-1 Risks of Control Not Operating Effectively

	Risk That Control Might Not Operate Effectively	
Factor	*Increased Risk*	*Decreased Risk*
Changes in the volume or nature of transactions	Significant changes	Few if any changes
Changes in the design of controls	Significant changes	Few if any changes
Reliance of control on the effectiveness of other controls	Extensive reliance on other controls	Minimal reliance on other controls
Changes in key personnel	Significant changes	Few if any changes
Performance by an individual or automated	Individual	Automated
Complexity of the control	Complex	Relatively simple

Paragraph 84 of the standard requires a clear link between the individual controls you will be testing with the significant accounts and assertions to which they relate.

Practice Pointer. The linking or mapping of individual control procedures to the financial statement assertions to which they relate is crucial if you are to perform an effective and efficient assessment of internal control. To perform an effective assessment, you should be sure that you have tested controls that relate to each assertion for all significant accounts. Similarly, to perform an efficient assessment, you should be sure *not* to test too many controls directed at the same assertions for the same account. To make these decisions about the controls to test, you need to link the controls to the related account and assertion.

Observations About the Requirements

- To evaluate the "points at which errors or fraud could occur," you will need to develop a solid understanding of the entire information system, from the initiation of the transaction through processing and eventual posting in the general ledger and inclusion in the financial statements. In general, errors or fraud can occur:

—At the initiation of a transaction, when data about it is first captured by the information system; and

—At any point where that data is subsequently processed, manipulated, or changed.

- Control procedures that are highly significant to achieving given control objectives generally should be tested.
- It is not uncommon for an information processing stream to have redundant controls. For example, a cash disbursements system may have controls related to each assertion at each step of the transaction initiation and processing stream. Additionally, the company's monthly bank reconciliation may achieve some of the same control objectives achieved by controls at each processing step within the information system. In this example, when the reconciliation achieves more than one control objective, it may be more efficient to test the reconciliation, rather than detail testing all the individual control procedures.
- In those circumstances where more than one control procedure is required to achieve a given control objective, you need to test *all* the control procedures related to that objective.

TESTING AND EVALUATING DESIGN EFFECTIVENESS

Paragraphs 88 and 89 of the standard provide relatively easy-to-understand guidance about the testing and evaluation of internal control design effectiveness.

> 88. Internal control over financial reporting is effectively designed when the controls complied with would be expected to prevent or detect errors or fraud that could result in material misstatements in the financial statements. The [external] auditor should determine whether the company has controls to meet the objectives of the control criteria by:
>
> - Identifying the company's control objectives in each area;
> - Identifying the controls that satisfy each objective; and
> - Determining whether the controls, if operating properly, can effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements.
>
> 89. Procedures the auditor performs to test and evaluate design effectiveness include inquiry, observation, walkthroughs, inspection of relevant documentation, and a specific evaluation of whether the controls are likely to prevent or detect errors or fraud that could result in misstatements if they are operated as prescribed by appropriately qualified persons.

Practice Pointer. Paragraph 88 states that internal control is effectively designed when it would be expected to prevent or detect material misstatements. Central to your judgment about whether the design of controls is effective is your understanding of the relevant control objectives and whether the individual or combination of controls, as designed, meets those objectives. As described earlier in this chapter, control objectives can be linked to financial statement assertions. In an effectively designed system, control objectives (and the related control procedures) will exist to ensure that each financial statement assertion is free of material misstatement. Exhibit 4-2 summarizes this link between financial statement assertions and control objectives.

Exhibit 4-2* Linking Financial Statement Assertions to Control Objectives

Assertion	*Description*	*Control Objectives*
Existence	Reported assets and liabilities exist at the reporting date.	• Only properly authorized assets and liabilities are recorded. • Assets are safeguarded and protected from unauthorized use or disposition. • Accountability for assets is maintained.
Occurrence	Reported transactions or events took place during the reporting period.	• Proper cut-off exists between accounting periods. • Fictitious, unauthorized, or duplicate transactions are detected and prevented from being recorded.
Valuation or Measurement	Assets, liabilities, transactions, and events are recorded at their proper amount.	• Assets and liabilities are initially recorded at the appropriate amount. • Recoverability of assets and valuation of liabilities are assessed periodically. • Transactions are recorded at correct amounts.
Completeness	The financial statements include ***all*** the assets and liabilities of the entity and the effect of its transactions during the reporting period.	• All authorized valid transactions are reported in the financial statements. • Proper cut-off exists between accounting periods.
Rights and Obligations	The entity has the rights to use reported assets and is obligated to settle reported liabilities.	• Entity has legal title to assets. • Proper authorization exists for the assignment of rights or encumbrance of assets. • Only the obligations of the entity are reported or disclosed.
Presentation and Disclosure	Items are properly classified, described, and disclosed in the financial statements.	• Financial statements are fairly presented in accordance with GAAP. • Disclosure is adequate and not misleading.

* From *How to Comply With Sarbanes-Oxley Section 404* by Michael Ramos, page 208; © Michael Ramos 2004. This material is used by permission of John Wiley & Sons, Inc.

Observations About the Requirements

Paragraph 88 of the standard describes the requirement for determining effective design as an evaluation of whether the controls would "prevent or detect errors or fraud that could result in material misstatements." This definition is appropriate and easy to understand in the context of activity-level controls. However, many company-level controls, such as the control environment or information technology (IT) general controls, are not designed to directly prevent or detect errors or fraud. Rather, these controls are designed to have a positive effect on the performance of activity-level controls. In that regard, some company-level controls have only an *indirect* effect on the company's ability to prevent or detect errors or fraud.

When considering the design effectiveness of these company-level controls, it might be helpful to consider whether the control helps create an overall environment or "tone at the top" that facilitates the effective operation of activity-level controls.

Walkthroughs

A walkthrough is a procedure in which you trace a transaction from its origination, through the company's information processing system, all the way to the transaction's reporting in the financial statements. The Auditing Standard places a great deal of emphasis on walkthroughs as an audit procedure. In fact:

- External auditors are required to perform at least one walkthrough for each major class of transactions.
- External auditors must perform the walkthroughs themselves. They are prohibited from relying on the work of management or others to satisfy the standard's walkthrough requirement.

The Auditing Standard does *not* require management to perform their own walkthroughs. However, the walkthrough procedure will allow you to confirm your understanding of the information processing stream, the design of related controls, and whether they have been placed in operation. As such, the walkthrough can help you evaluate the effectiveness of the design of internal control for each major transaction. While performing your walkthrough, you also may obtain evidence about the operating effectiveness of controls. For these reasons, the company should seriously consider performing walkthroughs as part of its self-assessment process.

Walkthrough Scope and Procedures

Paragraph 80 of the Auditing Standard describes what is required by the walkthrough procedures. Exhibit 4-3 reproduces these requirements together with some observations.

Exhibit 4-3 Walkthrough Scope and Procedures

Auditing Standard Requirements (Paragraph 80)	*Observations About the Requirements*
The auditor's walkthroughs should encompass the entire process of initiating, authorizing, recording, processing, and reporting individual transactions and controls for each of the significant processes identified, including controls intended to address the risk of fraud.	As indicated, the walkthrough is a complete tracing of the entire information processing stream. It is common to begin the walkthrough at the transaction initiation and proceed forward. Authorization is a control that usually is located at the point the transaction is initiated. Other controls should be identified and confirmed at each major processing step.
During the walkthrough, at each point at which important processing procedures or controls occur, the auditor should question the company's personnel about their understanding of what is required by the company's prescribed procedures and controls and determine whether the processing procedures are performed as originally understood and on a timely basis. (Controls might not be performed regularly but may still be timely.) During the walkthrough, the auditor should be alert for exceptions to the company's prescribed procedures and controls.	Paragraph 81 of the standard provides additional guidance on performing walkthrough procedures. The standard requires you to "be alert" for exceptions to prescribed procedures. However, to improve the effectiveness of your audit, particularly the detailed tests of activity-level controls, you may wish to more actively seek out the existence of situations in which personnel do not or did not perform the control procedures as described in the company's internal control documentation. The requirements of Paragraph 81 (discussed in the next section) suggest this more active approach to identifying exceptions.

Performance of the Walkthrough Procedures

Paragraph 81 provides detailed guidance on how to perform a walkthrough. Exhibit 4-4 reproduces these requirements together with some observations.

Exhibit 4-4 Walkthrough Scope and Procedures

Auditing Standard Requirements (Paragraph 81)	*Observations About the Requirements*
While performing a walkthrough, the auditor should evaluate the quality of the evidence obtained and perform walkthrough procedures that produce a level of evidence consistent with the objectives listed in Paragraph 79.	How much work is required in a walkthrough? It depends. This sentence provides broad guidance that says you essentially should use your judgment to make sure that your work is sufficient to meet your audit objective, for example, confirming your understanding of internal control design.

(continued)

Exhibit 4-4 Walkthrough Scope and Procedures *(continued)*

Auditing Standard Requirements (Paragraph 81)	*Observations About the Requirements*
Rather than reviewing copies of documents and making inquiries of a single person at the company, the auditor should follow the process flow of actual transactions using the same documents and information technology that company personnel use and make inquiries of relevant personnel involved in significant aspects of the process or controls.	This requirement suggests a relatively "hands-on" approach to performing the procedures in which you observe and test "live" transactions and documents and make inquiries of the individuals who *actually perform the control procedures on a daily basis.* There is a strong suggestion to make inquiries of more than one person. For many information processing streams, it is unlikely that one person will have a complete, thorough understanding of the entire information system.
To corroborate information at various points in the walkthrough, the auditor might ask personnel to describe their understanding of the previous and succeeding processing or control activities and to demonstrate what they do.	Note that: • Inquiries are used not only to gather information for the first time, but also to corroborate your understanding of information you may have received previously. • In a walkthrough, your inquiries may be supplemented with other procedures, such as observation.

Practice Pointer. Nothing in the standard requires you to make your inquiries with each individual one-on-one. Consider performing your walkthroughs as part of a focus group that includes all individuals who participate in the information processing stream. The focus group approach may improve audit efficiency. It may also improve your effectiveness, since the group can exchange ideas and share experiences to provide a deeper, more complete picture of the process.

Making Inquiries

Paragraph 81 of the Auditing Standard also requires external auditors to ask follow-up questions during the walkthroughs that are specifically designed to help identify the abuse of controls or indicators of fraud. Examples of the types of questions are provided by the standard, which recommends asking company personnel:

- What they do when they find an error or what they are looking for to determine if there is an error (rather than simply asking them if they perform listed procedures and controls).
- What kind of errors they have found.
- What happened as a result of finding the errors, and how the errors were resolved. (*Note:* If the person being interviewed has never found an error, you should evaluate whether that situation is due to good preventive controls or whether the individual performing the control lacks the necessary skills.)

- Whether they have ever been asked to override the process or controls, and if so, to describe:
  - — The situation
  - — Why it occurred
  - — What happened

Practice Pointer. Consider the difference between asking the question "Do you perform the procedures?" and the question "What happens when you find an error?" The standard recommends asking the second type of question.

With the first question, you address the issue of control exceptions only in the most indirect manner, and the structure of the question (closed-ended) leaves no room for explanation. A reasonable person, when asked the first question, might think that, if he or she performs the procedure 99 percent of the time, the answer to your question is, "Yes, I perform the procedure." Unfortunately, what you are most interested in is an explanation of what happens the other 1 percent of the time. By asking the second type of question (direct, open-ended) you will be better able to solicit the response you need.

Practice Pointer. To test the operating effectiveness of certain control procedures, you may perform detailed tests of a sampling of transactions. Some of the sampling methods used to determine sample sizes are based on an assumption that there are one or fewer exceptions in the population to be sampled. When this is the case, you should be careful when defining the population to be sampled. To improve the effectiveness of your tests—especially when you assume that there are one or fewer exceptions—it is best to make the population as homogeneous as possible. During your walkthrough procedures, you should identify all circumstances that employees regularly encounter that can lead to a deviation from established procedures. These circumstances should then be evaluated separately from the population from which the sample is drawn. It is much better to discover exceptions during the walkthrough rather than during the performance of detailed tests based on a sampling plan that provides little or no margin for error.

Updating Your Walkthrough

Whenever there is a significant change in the information processing stream, you should consider the need to evaluate the change and consider whether to update your walkthrough for transactions subsequent to the change.

After your initial walkthrough, the standard allows for the carryforward of the documentation to subsequent years, updating as necessary for any changes to procedures.

Practice Pointer. The procedures you perform and inquiries you make to identify changes in the processes should be just as structured and rigorous as those you made during the initial walkthrough. Again, you want to avoid unexpected surprises during detailed testing, so it is important that your walkthroughs retain their integrity over time. Appendix D to this Practice Aid provides a list of illustrative inquiries you might use to update your walkthroughs.

TESTING AND EVALUATING OPERATING EFFECTIVENESS

As part of your assessment of internal control, you must do more than merely evaluate design effectiveness. To support your conclusion on control effectiveness, paragraph 40 of the standard (as discussed in Chapter 1 of this Practice Aid) requires the following.

- You should evaluate the operating effectiveness of controls based on procedures sufficient to assess their operating effectiveness. Inquiry alone is not adequate to complete an evaluation of operating effectiveness.
- You must evaluate controls over all relevant assertions related to all significant accounts and disclosures.

Paragraph 92 of Auditing Standard No. 2 provides guidance to external auditors on what to consider when evaluating operating effectiveness. To avoid misunderstandings between you and the external auditors, you should consider this guidance provided to the external auditors. **Paragraph 92** of the Auditing Standard requires external auditors to perform tests of individual controls to determine "whether the control is operating as designed *and* whether the person performing the control possesses [both] the necessary authority and qualifications to perform the control effectively." [Emphasis added.]

Paragraph 106 reminds the external auditor that even though a control procedure is performed by the same person who historically performed the procedure effectively, he or she should not let this past performance color his or her judgment about the current period; circumstances may have changed.

The Auditing Standard goes on to provide guidance on the nature, timing, and extent of the external auditor's tests of operating effectiveness. Since this is an auditing standard, the guidance is not so detailed that it provides an audit program of how to design and perform these tests. However, the guidance is quite specific, and—even though it pertains directly to external auditors—company management should find it useful when designing and performing its assessment of internal control.

Nature of Tests

When testing operating effectiveness, paragraph 93 of the Auditing Standard recommends that you *include a mix* of the following types of procedures:

- Inquiry of appropriate personnel.
- Inspection of relevant documentation.
- Observation of the company's operations.
- Reperformance of the application of the control.

Paragraphs 94 through 97 of the standard provide additional guidance on the performance of these various types of procedures. Some of this guidance imposes certain requirements on the external auditor regarding the design or performance of tests. Other guidance is more akin to a recommendation or suggestion. Exhibit 4-5 summarizes this guidance regarding the nature of the tests of operating effectiveness.

Exhibit 4-5 Procedures to Test Operating Effectiveness

Type of Test	*Audit Requirement*	*Other Guidance*
Inquiry	• Seek information, both financial and nonfinancial, from knowledgeable persons throughout the company. • Inquiry alone is not sufficient to support conclusions about the operating effectiveness of internal control. • Evaluating company personnel responses to questions is an integral part of the procedure.	• Inquiries may be formal or informal. • Responses to inquiries might provide you with new information or corroborative evidence.
Inspection	None	• When documentary evidence of the control does not exist (and is not expected to exist) your tests probably will consist of inquiries and observation.
Observation	• Pertinent only at the point in time when the observation is made. • Supplement observation with other procedures.	None
Reperformance	None	• An employee's "sign-off" on having performed a given control procedure may not be persuasive evidence that the procedure was performed correctly. • If signature alone is not persuasive, reperform the test.

Timing of Tests

The Auditing Standard provides broad guidance on the timing of your tests of controls, and this guidance, together with some observations, is presented below.

General Principles

Paragraphs 98, 99, and 101 impose the following general requirements on the timing of audit tests of operating effectiveness. This guidance may be highly relevant to your company's assessment of internal control.

- The tests must be performed over a period of time that is "adequate to determine whether, as of the date specified in management's report, the controls necessary for achieving the objectives of the control criteria are operating effectively."
- Tests of operating effectiveness should occur at the time the controls are operating, even if they normally operate after the as-of reporting date. For example, some controls over the period-end financial reporting process normally operate only after the as-of date.
- The following controls should be tested closer to or at the "as-of" date rather than at an interim date:
  - — Controls over significant nonroutine transactions.
  - — Controls over accounts or processes with a high degree of subjectivity or judgment in measurement.
  - — Controls over the recording of period-end adjustments.

Remember that you are testing operating effectiveness "as of" year end. In the section of the standard relating to timing, the guidance refers to tests "over a period of time." This does not imply that you are trying to determine whether controls were effective throughout the year. The reference to "over a period of time" simply recognizes that to determine whether a control is effective as of a certain date, you may need to test its performance over a period of time preceding that date to gauge its overall reliability. That is, if you test a control procedure on December 31 only, the results of your test may reflect only the effectiveness of the control under the conditions that existed on that date. By testing the control over a period of time, you will be able to draw a more reliable conclusion about its effectiveness. What constitutes an "adequate" period of time (a week? a month? two months?) is a decision that the standard leaves to your professional judgment.

In those instances where the company has replaced an old accounting system with a new one during the year, your tests of the internal control effectiveness will be limited to testing the new system and not the old system. Again, you are testing operating effectiveness as of year end. At year end, the new system was operational, so that is the one that is relevant for your tests. (For additional guidance, please refer to paragraph A6 of the PCAOB *Staff Questions and Answers: Auditing Internal Control Over Financial Reporting* (http://www.pcaobus.org/documents/Staff_Q_and_A/Staff_Interal_Control.pdf).)

Practice Pointer. When companies install a new accounting system, controls over the installation process, including the testing of the system and the transfer of data from the old system to the new one, typically would be included within the scope of the company's review of IT general controls.

Interim Testing

When you test control effectiveness at an interim date, you should determine what additional evidence, if any, you should obtain concerning the operation of the control during the period between the interim testing date and year end. **Paragraph 100** of the Auditing Standard requires external auditors to evaluate the following to make their determination about control testing during this period:

- The specific controls tested prior to the "as of" date and the results of those tests;
- The degree to which evidence about the operating effectiveness of those controls was obtained;
- The length of the remaining period; and
- The possibility that there may have been any significant changes in internal control over financial reporting subsequent to the interim date.

Extent of Tests

Paragraphs 104 and 105 of the Auditing Standard provide general guidance on determining the extent of the tests of operating effectiveness. Guidance in these paragraphs that is most relevant to management includes the following.

- Design your procedures to provide a high level of assurance that the control being tested is operating effectively.
- Obtain sufficient evidence about operating effectiveness each year. That is, use caution when relying on evidence obtained in previous years to support a conclusion about the current operating effectiveness of a control.
- Consider varying from year to year the nature, timing, and extent of testing controls as a way to:
  - — Respond to changing circumstances.
  - — Introduce unpredictability into the testing.

Paragraph 105 of the standard provides additional guidance on the factors to consider when determining the extent of your tests. Exhibit 4-6 summarizes this guidance regarding the extent of tests of operating effectiveness.

Exhibit 4-6 Extent of Tests Related to Operating Effectiveness

Factor to Consider	*Audit Requirement*	*Other Guidance*
Nature of the Control	• Manual controls should be subject to more extensive testing than automated controls. • Also assess: — Complexity of the controls. — Significance of the judgments made in connection with their operation. — Level of competence required to perform the control effectively.	None
Frequency of operation	None	• Generally, the more frequently a manual control operates, the more operations of the control you should test.
Importance of the control	• More important controls require more extensive tests.	None

The Auditing Standard includes several examples of how to apply the guidance related to the extent-of-testing decisions. For your convenience, these examples have been included in Appendix F of this Practice Aid.

Sampling in Compliance Tests

Statement on Auditing Standards (SAS) No. 39, *Audit Sampling* (AICPA, *Professional Standards*, vol. 1, AU sec. 350), and the AICPA Audit Guide *Audit Sampling* provide guidance on using statistical and nonstatistical sampling methods for determining the extent of testing of controls to be performed. Although this guidance is designed specifically for tests of controls in conjunction with a financial statement audit, many aspects of it may be applied to an assessment of internal control. Relevant portions of the Audit Guide have been reproduced in Appendix E of this Practice Aid. In reading this material, note the following:

- The guidance is taken from an Audit Guide, which applies directly to external auditors. However, the statistical concepts and procedures underlying the guidance can be adapted easily to management's assessment of internal control.
- Determining the sample size for tests of control begins with your decision about what the Guide labels the "risk of assessing control risk too low." The notion of "control risk" is relevant only for external auditors performing a financial statement audit, but it is analogous to

the idea of "level of assurance" expressed in the Auditing Standard on internal control. In fact, paragraph 3.31 of the audit sampling Guide equates "high level of assurance" with "low level of risk of assessing control risk too low." Essentially, they are two sides to the same coin: a 5 percent risk is the same as a 95 percent (100 percent – 5 percent) level of assurance.

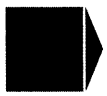
- You are not required to quantify "high level of assurance." Table A.1, which shows statistical sample sizes, is based on a 95 percent level of assurance. Table A-2 shows sample sizes based on a 90 percent level of assurance.
- To determine the sample size for a test of controls, you also are required to assess the "tolerable rate" of deviation from the control procedure. The audit sampling Guide defines the "tolerable rate" as the "rate of deviation from a prescribed control that external auditors are willing to accept without altering the planned assessed level of control risk." Again the reference to "control risk" is pertinent only to external auditors performing a financial statement audit, but for management's assessment of internal control the tolerable rate should be equated to "control effectiveness." That is, how many deviations from a control procedure would you be willing to accept before you determined that the procedure was not effective?
- Table 3.2 of the Audit Sampling Guide provides an example of relating control effectiveness to a tolerable rate. In this example, an effective control procedure (expressed as a "low level of control risk") is equated to a tolerable rate ranging from 3 percent to 7 percent. That is, in this example, if the control procedure operates as designed 93 percent of the time or greater, the control is considered effective.
- Determining the tolerable rate is a judgment decision that will require you to consider a variety of factors, including the relative significance of the control.
- The third and final factor that must be considered to determine a sample size is the expected population deviation rate. That is, what do you believe to be the true deviation rate in the sample?
- Logically, the expected deviation rate must be less than your established tolerable rate of deviation. If the control must be performed as described 95 percent of the time, but you believe that in practice the control is performed properly only 90 percent of the time, you essentially have concluded that you have an ineffective control.
- In some sampling plans for financial statement audits, the external auditor assumes that the expected population deviation rate is 0 percent. Although this assumption reduces the initial sample size, if a deviation is discovered, the sample size must be increased to reach the same conclusion about control effectiveness.

Practice Pointer. Be cautious in assuming that a given control procedure was performed without a single deviation during the entire period covered by your tests. Although not required by the audit sampling Guide or Auditing Standard No. 2, you should have some basis for assuming a population deviation rate of 0 percent. If you believe that some deviations in the control probably do exist in the population, it usually is more efficient to build this assumption into your original sample size determination rather than increasing your sample sizes subsequently as deviations are discovered.

EVALUATING DEFICIENCIES

As stated in **paragraph 8** of the Auditing Standard:

> A *control deficiency* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.
>
> - A deficiency in *design* exists when (*a*) a control necessary to meet the control objective is missing, or (*b*) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not always met.
> - A deficiency in *operation* exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.



Practice Pointer. The definition of a control deficiency requires you to assess the authority and qualifications of the person assigned to perform the control procedure. This requirement will affect:

- *The company's documentation of internal control policies.* To help you assess design effectiveness, the documentation of internal control should indicate who is responsible for performing the procedure.
- *Your tests of operating or design effectiveness.* These should include an assessment of the authority and qualifications of the individual assigned to perform the control procedure.

A "compensating control" is one that is designed to achieve the same control objective as an ineffective control. As discussed in Chapter 5 of this Practice Aid, compensating controls should be considered when evaluating the relative significance of a control deficiency. However, compensating controls should *not* be considered when determining whether a control deficiency *exists*. A control deficiency exists irrespective of the existence of another control that is designed to achieve the same objective.

When your tests of operating effectiveness uncover exceptions to the company's prescribed control procedures, you are required to determine whether additional tests are required to assess operating effectiveness. That is, a control testing exception is *not necessarily* a control deficiency. Judgment is required to determine whether such an exception is in fact, a control deficiency. If you determine that the exception is *not* a control deficiency, for example, an "isolated instance," of noncompliance, you may be able to justify that no additional tests are required. However, **paragraph 107** of the standard cautions that:

> A conclusion that an identified exception does not represent a control deficiency is appropriate only if evidence beyond what the auditor had initially planned and beyond inquiry supports that conclusion.

In other words, you should perform and document additional testwork to support your conclusion that the exception was, indeed, an isolated instance of noncompliance. Even though this requirement pertains directly to external auditors, management should consider following the guidance as well.

Practice Pointer. When exceptions are discovered, it may be more effective and efficient to extend your work to determine the underlying causes for the deviation. By understanding these root causes, you will have a better understanding of the magnitude of the exception and its true effect on control effectiveness.

SUMMARY

Your tests of internal control begin with a determination of which controls to test. You should focus this determination on an understanding of control *objectives*, which ultimately are related to the relevant assertions for significant accounts. You are not required to test all control *procedures*, only enough of the procedures to ensure you have addressed all control objectives.

Your tests should be directed toward an assessment of both design and operating effectiveness. Walkthroughs are a suggested procedure that will provide you with evidence about control design effectiveness. They also may provide you with evidence relating to operating effectiveness.

CHAPTER 5: EVALUATION OF INTERNAL CONTROL EFFECTIVENESS

UNDERSTANDING KEY DEFINITIONS

As discussed in Chapter 1 of this Practice Aid, the objective of an assessment of internal control is to obtain reasonable assurance that no material weaknesses exist as of the reporting date. If one or more material weaknesses do exist, you are precluded from stating that internal control is "effective." Thus, to properly evaluate internal control effectiveness, you must be able to determine whether a control deficiency rises to the level of *material weakness* or the related term *significant deficiency*.

Paragraphs 9 and 10 of Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, PC sec. 140), provide the following definitions and guidance.

> 9. A *significant deficiency* is 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 reliably in accordance with generally accepted accounting principles 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.
>
> **Note:** The term "remote likelihood" as used in the definitions of *significant deficiency* and *material weakness* (Paragraph 10) has the same meaning as the term "remote" as used in Financial Accounting Standards Board Statement No. 5, *Accounting for Contingencies* ("FAS No. 5"). Paragraph 3 of FAS No. 5 states:
>
> > When a loss contingency exists, the likelihood that the future event or events will confirm the loss or impairment of an asset or the incurrence of a liability can range from probable to remote." This Statement uses the terms *probable, reasonably possible,* and *remote* to identify three areas within that range, as follows:
> >
> > a. *Probable.* The future event or events are likely to occur.
> > b. *Reasonably possible.* The chance of the future event or events occurring is more than remote but less than likely.
> > c. *Remote.* The chance of the future events or events occurring is slight.
>
> Therefore, the likelihood of an event is "more than remote" when it is either reasonably possible or probable.

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

10. A *material weakness* is a significant deficiency, or 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.

EVALUATING INTERNAL CONTROL DEFICIENCIES

The definitions of *significant deficiency* and *material weakness* indicate that your evaluation of the severity of an internal control deficiency considers two different factors:

- The *likelihood* that a deficiency could result in a misstatement; and
- The *magnitude* of the potential misstatement resulting from the deficiency.

Thus, as defined in paragraph 10 of the standard, a material weakness is one in which there is more than a remote *likelihood* that a *material* error will not be prevented or detected.

When evaluating the severity of an internal control deficiency, paragraph 132 of the standard states that severity depends on *the potential for misstatement,* not on whether a misstatement actually has occurred. Put another way, the fact that no material misstatement in the financial statements exists provides no basis for concluding that a control deficiency is inconsequential.

Additionally, when evaluating the severity of a deficiency, **paragraph 137** requires you to "determine the level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles."

Assessing Likelihood

When assessing the likelihood that a control deficiency would result in a misstatement, you should evaluate how the controls interact with other controls. In this regard, **paragraph 134** of the standard notes, "There are controls, such as information technology general controls, on which other controls depend."

Author's Observation

Typically, a deficiency in a control that has a pervasive effect on other controls will be more likely to result in a misstatement than a comparable deficiency in a control that does not have a pervasive effect.

Paragraph 134 continues, "Some controls function together as a group of controls." Also, some controls may overlap with others, that is, more than one control is designed to achieve the same control objective.

Author's Observation

The likelihood that a deficiency in a control will result in a misstatement diminishes to the extent that other effective controls exist that achieve the same control objective.

Paragraph 133 of the Auditing Standard suggests that you consider the following factors when evaluating the likelihood that a deficiency will result in a financial statement misstatement:

- The nature of the financial statement accounts, disclosures, and assertions involved; for example, suspense accounts and related party transactions involve greater risk.
- The susceptibility of the related assets or liability to loss or fraud; that is, greater susceptibility increases risk.
- The subjectivity, complexity, or extent of judgment required to determine the amount involved; that is, greater subjectivity, complexity, or judgment, like that related to an accounting estimate, increases risk.
- The cause and frequency of known or detected exceptions for the operating effectiveness of a control; for example, a control with an observed non-negligible deviation rate is a deficiency.
- The interaction or relationship of the control with other controls; that is, the interdependence or redundancy of the control.
- The interaction of the deficiencies; for example, when evaluating a combination of two or more deficiencies, whether the deficiencies could affect the same financial statement accounts and assertions.
- The possible future consequences of the deficiency.

Observations About the Guidance

The first three factors listed introduce the notion of "risk," stating that certain conditions involve "greater risk." It may be helpful to consider "risk" as the "risk that a misstatement in the account could occur, irrespective of the company's internal controls." The implication in this context is that the greater the inherent risk of misstatement associated with an account, the greater the likelihood that a control deficiency could result in a misstatement.

The standard provides that you should evaluate the effect of "compensating controls" when evaluating control deficiencies. A compensating control is designed to achieve the same control objective as a missing or ineffective control. The existence of a strong compensating control can mitigate the risk of misstatement (and therefore lesson the significance) of a control deficiency. To evaluate the relative effectiveness of a compensating control, **paragraph A14** of the PCAOB *Staff Questions and Answers: Auditing Internal Control Over Financial Reporting* (http://www.pcaobus.org/documents/Staff_Q_and_A/Staff_Interal_Control.pdf) states that "to have a mitigating effect [on the relative magnitude of a missing or ineffective control], the compensating control should operate at a level of precision that would prevent or detect a misstatement that was more than inconsequential or material, respectively."

Evaluating Magnitude

Paragraph 135 of the Auditing Standard lists the factors you should consider when assessing the magnitude of a potential misstatement resulting from a control deficiency:

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

The standard goes on to note that the maximum amount that an account balance or total of transactions can be *overstated* is generally the recorded amount; however, this is not true for *understatements* of an account.

De Facto Significant Deficiencies and Strong Indicators of Material Weakness

Paragraphs 139 and 140 of the Auditing Standard provide specific guidance on a number of circumstances that are presumed to be significant deficiencies and "strong indicators" of a material weakness.

> 139. The interaction of qualitative considerations that affect internal control over financial reporting with quantitative considerations ordinarily results in deficiencies in the following areas being at least significant deficiencies in internal control over financial reporting:
>
> - Controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles;
> - Antifraud programs and controls;
> - Controls over non-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
>
> 140. Each of the following circumstances should be regarded as at least a significant deficiency and 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.
>
> **Note:** The correction of a misstatement includes misstatements due to error or fraud; it does not include restatements to reflect a change in accounting principle to comply with a new accounting principle or a voluntary change from one generally accepted accounting principle to another generally accepted accounting principle.
> - Identification by the [external] auditor of a material misstatement in financial statements in the current period that was not initially identified by the company's internal control over financial reporting. (This is a strong indicator of a material weakness even if management subsequently corrects the misstatement.)

- Oversight of the company's external financial reporting and internal control over financial reporting by the company's audit committee is ineffective. (Paragraphs 55 through 59 present factors to evaluate when determining whether the audit committee is ineffective.)
- The internal audit function or the risk assessment function is ineffective at a company for which such a function needs to be effective for the company to have an effective monitoring or risk assessment component, such as for very large or highly complex companies.

  Note: The evaluation of the internal audit or risk assessment functions is similar to the evaluation of the audit committee, as described in paragraphs 55 through 59, that is, the evaluation is made within the context of the monitoring and risk assessment components. The [external] auditor is not required to make a separate evaluation of the effectiveness and performance of these functions. Instead, the external auditor should base his or her evaluation on evidence obtained as part of evaluating the monitoring and risk assessment components of internal control over financial reporting.
- For complex entities in highly regulated industries, an ineffective regulatory compliance function. This relates solely to those aspects of the ineffective regulatory compliance function in which associated violations of laws and regulations could have a material effect on the reliability of financial reporting.
- Identification of fraud of any magnitude on the part of senior management.

  Note: The [external] auditor is required to plan and perform procedures to obtain reasonable assurance that material misstatement caused by fraud is detected by the [external] auditor. However, for the purposes of evaluating and reporting deficiencies in internal control over financial reporting, the [external] auditor should evaluate fraud of any magnitude (including fraud resulting in immaterial misstatements) on the part of senior management of which he or she is aware. Furthermore, for the purposes of this circumstance, "senior management" includes the principal executive and financial officers signing the company's certifications as required under Section 302 of the Act as well as any other member of management who plays a significant role in the company's financial reporting process.
- Significant deficiencies that have been communicated to management and the audit committee remain uncorrected after some reasonable period of time.
- An ineffective control environment.

Observations About the Requirements

- The listing of significant deficiencies and "strong indicators" of material weakness will affect your audit objectives and the scope of your work. That is, your assessment process should be designed to provide reasonable assurance that the circumstances listed in paragraphs 139 and 140 will be identified.

AUDIT COMMITTEE OVERSIGHT

The Auditing Standard states that ineffective audit committee oversight is a "strong indicator" of a material weakness.

The Treadway Commission's Committee of Sponsoring Organizations' (COSO) report, *Internal Control—Integrated Framework*, describes the audit committee and board of director oversight as a key element of an entity's control environment and the monitoring component of internal control. Because of the importance of the audit committee and the board of directors, the Auditing Standard requires external auditors to assess the effectiveness of the audit committee and the board *in the context* of obtaining an understanding about the company's control environment and the monitoring of its internal control.

During the standard's public comment period, this requirement relating to the audit committee and board drew many comments asking for clarification. In the final standard, the PCAOB took great pains to note their intention that the requirement does *not*:

- Transfer the responsibility for maintaining internal control from management to the audit committee. Management retains the ultimate responsibility for the company's internal control. (See Note to paragraph 55.)
- Require you to make a separate and distinct evaluation of the audit committee effectiveness. Your evaluation of the audit committee is solely in the context of understanding the control environment and the monitoring components of internal control. (See paragraph 56.)

Paragraphs 57 and 58 provide examples of factors the external auditors might consider when evaluating the audit committee. Although these factors relate directly to external auditors, you may find them helpful when performing your own evaluation of audit committee effectiveness. The list of these factors provided by the standard are:

- The independence of the audit committee members from management.
- The clarity with which the audit committee's responsibilities are articulated (for example, in the audit committee's charter).
- How well the audit committee and management understand those responsibilities.
- The audit committee's involvement and interaction with the external auditor and with internal auditors, as well as interaction with key members of financial management, including the chief financial officer and chief accounting officer.
- Whether the right questions are raised and pursued with management and the external auditor, including questions that indicate an understanding of the critical accounting policies and judgmental accounting estimates, and the responsiveness to issues raised by the external auditor.

SUMMARY

To prepare your report on internal control effectiveness, you will need to evaluate the magnitude of the control deficiencies noted during your assessment. These deficiencies can range from a material weakness (most severe) to a significant deficiency (severe) to other deficiencies of lesser magnitude. The Auditing Standard provides extensive guidance on how to evaluate control deficiencies.

The presence of one or more material weaknesses as of year end will preclude you from concluding that internal control is effective.

APPENDIX A: EXAMPLES OF USING THE WORK OF OTHERS

This appendix reproduces paragraph 126 of Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, PC sec. 140). The material applies directly to auditors, not to company management, and it directly addresses auditors only. However, this material may also be helpful to management in applying the guidance in PCAOB Auditing Standard No. 2 that directly affects the planning and performance of the company's self-assessment of internal control effectiveness.

If certain conditions are met, the company's external auditors may rely on the work performed by the company in its assessment of internal control to reduce the extent of their work during the internal control audit. This paragraph from the Auditing Standard provides examples that apply the guidance discussed in Chapter 1 of this Practice Aid.

> 126. The following examples illustrate how to apply the directions discussed in this section:
>
> *Controls over the period-end financial reporting process.* Many of the controls over the period-end financial reporting process address significant risks of misstatement of the accounts and disclosures in the annual and quarterly financial statements, may require significant judgment to evaluate their operating effectiveness, may have a higher potential for management override, and may affect accounts that require a high level of judgment or estimation. Therefore, the auditor could determine that, based on the nature of controls over the period-end financial reporting process, he or she would need to perform more of the tests of those controls himself or herself. Further, because of the nature of the controls, the auditor should use the work of others only if the degree of competence and objectivity of the individuals performing the work is high; therefore, the auditor might use the work of internal auditors to some extent but not the work of others within the company.
>
> *Information technology general controls.* Information technology general controls are part of the control activities component of internal control; therefore, the nature of the controls might permit the auditor to use the work of others. For example, program change controls over routine maintenance changes may have a highly pervasive effect, yet involve a low degree of judgment in evaluating their operating effectiveness, can be subjected to objective testing, and have a low potential for management override. Therefore, the auditor could determine that, based on the nature of these program change controls, the auditor could use the work of others to a moderate extent so long as the degree of competence and objectivity of the individuals performing the test is at an appropriate level. On the other hand, controls to detect attempts to override controls that prevent unauthorized journal entries from being posted may have a highly pervasive effect, may involve a high degree of judgment in evaluating their operating effectiveness, may involve a subjective evaluation, and may have a reasonable possibility for management override. Therefore, the auditor could determine that, based on the nature of these controls over systems access, he or she would need to perform

more of the tests of those controls himself or herself. Further, because of the nature of the controls, the auditor should use the work of others only if the degree of competence and objectivity of the individuals performing the tests is high.

Management self-assessment of controls. As described in paragraph 40, management may test the operating effectiveness of controls using a self assessment process. Because such an assessment is made by the same personnel who are responsible for performing the control, the individuals performing the self-assessment do not have sufficient objectivity as it relates to the subject matter. Therefore, the auditor should not use their work.

Controls over the calculation of depreciation of fixed assets. Controls over the calculation of depreciation of fixed assets are usually not pervasive, involve a low degree of judgment in evaluating their operating effectiveness, and can be subjected to objective testing. If these conditions describe the controls over the calculation of depreciation of fixed assets and if there is a low potential for management override, the auditor could determine that, based on the nature of these controls, the auditor could use the work of others to a large extent (perhaps entirely) so long as the degree of competence and objectivity of the individuals performing the test is at an appropriate level.

Alternating tests of controls. Many of the controls over accounts payable, including controls over cash disbursements, are usually not pervasive, involve a low degree of judgment in evaluating their operating effectiveness, can be subjected to objective testing, and have a low potential for management override. When these conditions describe the controls over accounts payable, the auditor could determine that, based on the nature of these controls, he or she could use the work of others to a large extent (perhaps entirely) so long as the degree of competence and objectivity of the individuals performing the test is at an appropriate level. However, if the company recently implemented a major information technology change that significantly affected controls over cash disbursements, the auditor might decide to use the work of others to a lesser extent in the audit immediately following the information technology change and then return, in subsequent years, to using the work of others to a large extent in this area. As another example, the auditor might use the work of others for testing controls over the depreciation of fixed assets (as described in the point above) for several years' audits but decide one year to perform some extent of the work himself or herself to gain an understanding of these controls beyond that provided by performing a walk-through.

APPENDIX B: SAFEGUARDING OF ASSETS

This appendix reproduces Appendix C of Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, PC sec. 140). The Securities and Exchange Commission's definition of internal control includes control procedures relating to the safeguarding of assets. The material that follows provides guidance on how to apply the definition of safeguarding of assets to an assessment of internal control effectiveness. The material applies directly to auditors, not to company management, and it directly addresses auditors only. However, this material may also be helpful to management in applying the guidance in PCAOB Auditing Standard No. 2 that directly affects the planning and performance of the company's self-assessment of internal control effectiveness.

C1. *Safeguarding of assets* is defined in paragraph 7 as those policies and procedures that "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements." This definition is consistent with the definition provided in the Committee of Sponsoring Organizations (COSO) of the Treadway Commission's Addendum, *Reporting to External Parties*, which provides the following definition of internal control over safeguarding of assets:

> Internal control over safeguarding of assets against unauthorized acquisition, use or disposition is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the entity's assets that could have a material effect on the financial statements. Such internal control can be judged effective if the board of directors and management have reasonable assurance that unauthorized acquisition, use or disposition of the entity's assets that could have a material effect on the financial statements is being prevented or detected on a timely basis.

C2. For example, a company has safeguarding controls over inventory tags (preventive controls) and also performs periodic physical inventory counts (detective control) timely in relation to its quarterly and annual financial reporting dates. Although the physical inventory count does not safeguard the inventory from theft or loss, it prevents a material misstatement to the financial statements if performed effectively and timely.

C3. Therefore, given that the definitions of material weakness and significant deficiency relate to the likelihood of misstatement of the financial statements, the failure of a preventive control such as inventory tags will not result in a significant deficiency or material weakness if the detective control (physical inventory) prevents a misstatement of the financial statements. The COSO Addendum also indicates that to the extent that such losses might occur, controls over financial reporting are effective if they provide reasonable assurance that those losses are properly reflected in the financial statements, thereby alerting financial statement users to consider the need for action.

Note: *Properly reflected* in the financial statements includes both correctly recording the loss and adequately disclosing the loss.

C4. Material weaknesses relating to controls over the safeguarding of assets would only exist when the company does not have effective controls (considering both safeguarding and other controls) to prevent or detect a material misstatement of the financial statements.

C5. Furthermore, management's plans that could potentially affect financial reporting in future periods are not controls. For example, a company's business continuity or contingency planning has no effect on the company's current abilities to initiate, authorize, record, process, or report financial data. Therefore, a company's business continuity or contingency planning is not part of internal control over financial reporting.

C6. The COSO Addendum provides further information about safeguarding of assets as it relates to internal control over financial reporting.

APPENDIX C: MANAGEMENT ANTIFRAUD PROGRAMS AND CONTROLS

This appendix reproduces the exhibit in AICPA Statement on Auditing Standards No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 316). As discussed in Chapter 2 of this Practice Aid, management's assessment process is required to include the documentation, testing, and evaluation of management's antifraud programs and controls. This document provides guidance on suggested elements of such programs. The material applies directly to auditors, not to company management, and it directly addresses auditors only. However, this material may also be helpful to management in applying the guidance in PCAOB Auditing Standard No. 2 that directly affects the planning and performance of the company's self-assessment of internal control effectiveness.

Exhibit

Management Antifraud Programs and Controls
Guidance to Help Prevent, Deter, and Detect Fraud

* * *

Preface

Some organizations have significantly lower levels of misappropriation of assets and are less susceptible to fraudulent financial reporting than other organizations because these organizations take proactive steps to prevent or deter fraud. It is only those organizations that seriously consider fraud risks and take proactive steps to create the right kind of climate to reduce its occurrence that have success in preventing fraud. This document identifies the key participants in this antifraud effort, including the board of directors, management, internal and independent auditors, and certified fraud examiners.

Management may develop and implement some of these programs and controls in response to specific identified risks of material misstatement of financial statements due to fraud. In other cases, these programs and controls may be a part of the entity's enterprise-wide risk management activities.

Management is responsible for designing and implementing systems and procedures for the prevention and detection of fraud and, along with the board of directors, for ensuring a culture and environment that promotes honesty and ethical behavior. However, because of the characteristics of fraud, a material misstatement of financial statements due to fraud may occur notwithstanding the presence of programs and controls such as those described in this document.

Introduction

Fraud can range from minor employee theft and unproductive behavior to misappropriation of assets and fraudulent financial reporting. Material financial statement fraud can have a significant adverse effect on an entity's market value, reputation, and ability to achieve its strategic objectives. A number of highly publicized cases have heightened the

awareness of the effects of fraudulent financial reporting and have led many organizations to be more proactive in taking steps to prevent or deter its occurrence. Misappropriation of assets, though often not material to the financial statements, can nonetheless result in substantial losses to an entity if a dishonest employee has the incentive and opportunity to commit fraud.

The risk of fraud can be reduced through a combination of prevention, deterrence, and detection measures. However, fraud can be difficult to detect because it often involves concealment through falsification of documents or collusion among management, employees, or third parties. Therefore, it is important to place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals that they should not commit fraud because of the likelihood of detection and punishment. Moreover, prevention and deterrence measures are much less costly than the time and expense required for fraud detection and investigation.

An entity's management has both the responsibility and the means to implement measures to reduce the incidence of fraud. The measures an organization takes to prevent and deter fraud also can help create a positive workplace environment that can enhance the entity's ability to recruit and retain high-quality employees.

Research suggests that the most effective way to implement measures to reduce wrongdoing is to base them on a set of core values that are embraced by the entity. These values provide an overarching message about the key principles guiding all employees' actions. This provides a platform upon which a more detailed code of conduct can be constructed, giving more specific guidance about permitted and prohibited behavior, based on applicable laws and the organization's values. Management needs to clearly articulate that all employees will be held accountable to act within the organization's code of conduct.

This document identifies measures entities can implement to prevent, deter, and detect fraud. It discusses these measures in the context of three fundamental elements. Broadly stated, these fundamental elements are (1) create and maintain a *culture* of honesty and high ethics; (2) *evaluate* the risks of fraud and implement the processes, procedures, and controls needed to mitigate the risks and reduce the opportunities for fraud; and (3) develop an appropriate *oversight* process. Although the entire management team shares the responsibility for implementing and monitoring these activities, with oversight from the board of directors, the entity's chief executive officer (CEO) should initiate and support such measures. Without the CEO's active support, these measures are less likely to be effective.

The information presented in this document generally is applicable to entities of all sizes. However, the degree to which certain programs and controls are applied in smaller, less-complex entities and the formality of their application are likely to differ from larger organizations. For example, management of a smaller entity (or the owner of an owner-managed entity), along with those charged with governance of the financial reporting process, are responsible for creating a culture of honesty and high ethics. Management also is responsible for implementing a system of internal controls commensurate with the nature and size of the organization, but smaller entities may find that certain types of control activities are not relevant because of the involvement of and controls applied by management. However, all entities must make it clear that unethical or dishonest behavior will not be tolerated.

Creating a Culture of Honesty and High Ethics

It is the organization's responsibility to create a culture of honesty and high ethics and to clearly communicate acceptable behavior and expectations of each employee. Such a culture is rooted in a strong set of core values (or value system) that provides the foundation for employees as to how the organization conducts its business. It also allows an entity to develop an ethical framework that covers (1) fraudulent financial reporting, (2) misappropriation of assets, and (3) corruption as well as other issues.[1]

Creating a culture of honesty and high ethics should include the following.

Setting the Tone at the Top

Directors and officers of corporations set the "tone at the top" for ethical behavior within any organization. Research in moral development strongly suggests that honesty can best be reinforced when a proper example is set—sometimes referred to as the tone at the top. The management of an entity cannot act one way and expect others in the entity to behave differently.

In many cases, particularly in larger organizations, it is necessary for management to both behave ethically and openly communicate its expectations for ethical behavior because most employees are not in a position to observe management's actions. Management must show employees through its words and actions that dishonest or unethical behavior will not be tolerated, even if the result of the action benefits the entity. Moreover, it should be evident that all employees will be treated equally, regardless of their position.

For example, statements by management regarding the absolute need to meet operating and financial targets can create undue pressures that may lead employees to commit fraud to achieve them. Setting unachievable goals for employees can give them two unattractive choices: fail or cheat. In contrast, a statement from management that says, "We are aggressive in pursuing our targets, while requiring truthful financial reporting at all times," clearly indicates to employees that integrity is a requirement. This message also conveys that the entity has "zero tolerance" for unethical behavior, including fraudulent financial reporting.

The cornerstone of an effective antifraud environment is a culture with a strong value system founded on integrity. This value system often is reflected in a code of conduct.[2] The code of conduct should reflect the core values of the entity and guide employees in making appropriate decisions during their workday. The code of conduct might include such topics as ethics, confidentiality, conflicts of interest, intellectual property, sexual harassment, and fraud.[3] For a code of conduct to be effective, it should be communicated

---

[1] Corruption includes bribery and other illegal acts.

[2] An entity's value system also could be reflected in an ethics policy, a statement of business principles, or some other concise summary of guiding principles.

[3] Although the discussion in this document focuses on fraud, the subject of fraud often is considered in the context of a broader set of principles that govern an organization. Some organizations, however, may elect to develop a fraud policy separate from an ethics policy. Specific examples of topics in a fraud policy might include a requirement to comply with all laws and regulations and explicit guidance regarding making payments to obtain contracts, holding pricing discussions with competitors, environmental discharges, relationships with vendors, and maintenance of accurate books and records.

to all personnel in an understandable fashion. It also should be developed in a participatory and positive manner that will result in both management and employees taking ownership of its content. Finally, the code of conduct should be included in an employee handbook or policy manual, or in some other formal document or location (for example, the entity's intranet) so it can be referred to when needed.

Senior financial officers hold an important and elevated role in corporate governance. While members of the management team, they are uniquely capable and empowered to ensure that all stakeholders' interests are appropriately balanced, protected, and preserved. For examples of codes of conduct, see Attachment 1, "AICPA 'CPA's Handbook of Fraud and Commercial Crime Prevention,' An Organizational Code of Conduct," and Attachment 2, "Financial Executives International Code of Ethics Statement" provided by Financial Executives International. In addition, visit the Institute of Management Accountants' Ethics Center at www.imanet.org for their members' standards of ethical conduct.

Creating a Positive Workplace Environment

Research results indicate that wrongdoing occurs less frequently when employees have positive feelings about an entity than when they feel abused, threatened, or ignored. Without a positive workplace environment, there are more opportunities for poor employee morale, which can affect an employee's attitude about committing fraud against an entity. Factors that detract from a positive work environment and may increase the risk of fraud include:

- Top management that does not seem to care about or reward appropriate behavior
- Negative feedback and lack of recognition for job performance
- Perceived inequities in the organization
- Autocratic rather than participative management
- Low organizational loyalty or feelings of ownership
- Unreasonable budget expectations or other financial targets
- Fear of delivering "bad news" to supervisors and/or management
- Less-than-competitive compensation
- Poor training and promotion opportunities
- Lack of clear organizational responsibilities
- Poor communication practices or methods within the organization

The entity's human resources department often is instrumental in helping to build a corporate culture and a positive work environment. Human resource professionals are responsible for implementing specific programs and initiatives, consistent with management's strategies, that can help to mitigate many of the detractors mentioned above. Mitigating factors that help create a positive work environment and reduce the risk of fraud may include:

- Recognition and reward systems that are in tandem with goals and results
- Equal employment opportunities
- Team-oriented, collaborative decision-making policies
- Professionally administered compensation programs
- Professionally administered training programs and an organizational priority of career development

Employees should be empowered to help create a positive workplace environment and support the entity's values and code of conduct. They should be given the opportunity to provide input to the development and updating of the entity's code of conduct, to ensure that it is relevant, clear, and fair. Involving employees in this fashion also may effectively contribute to the oversight of the entity's code of conduct and an environment of ethical behavior (see the section titled "Developing an Appropriate Oversight Process").

Employees should be given the means to obtain advice internally before making decisions that appear to have significant legal or ethical implications. They should also be encouraged and given the means to communicate concerns, anonymously if preferred, about potential violations of the entity's code of conduct, without fear of retribution. Many organizations have implemented a process for employees to report on a confidential basis any actual or suspected wrongdoing, or potential violations of the code of conduct or ethics policy. For example, some organizations use a telephone "hotline" that is directed to or monitored by an ethics officer, fraud officer, general counsel, internal audit director, or another trusted individual responsible for investigating and reporting incidents of fraud or illegal acts.

Hiring and Promoting Appropriate Employees

Each employee has a unique set of values and personal code of ethics. When faced with sufficient pressure and a perceived opportunity, some employees will behave dishonestly rather than face the negative consequences of honest behavior. The threshold at which dishonest behavior starts, however, will vary among individuals. If an entity is to be successful in preventing fraud, it must have effective policies that minimize the chance of hiring or promoting individuals with low levels of honesty, especially for positions of trust.

Proactive hiring and promotion procedures may include:

- Conducting background investigations on individuals being considered for employment or for promotion to a position of trust[4]
- Thoroughly checking a candidate's education, employment history, and personal references
- Periodic training of all employees about the entity's values and code of conduct, (training is addressed in the following section)
- Incorporating into regular performance reviews an evaluation of how each individual has contributed to creating an appropriate workplace environment in line with the entity's values and code of conduct
- Continuous objective evaluation of compliance with the entity's values and code of conduct, with violations being addressed immediately

Training

New employees should be trained at the time of hiring about the entity's values and its code of conduct. This training should explicitly cover expectations of all employees regarding (1) their duty to communicate certain matters; (2) a list of the types of matters, including actual or suspected fraud, to be communicated along with specific examples;

[4] Some organizations also have considered follow-up investigations, particularly for employees in positions of trust, on a periodic basis (for example, every five years) or as circumstances dictate.

and (3) information on how to communicate those matters. There also should be an affirmation from senior management regarding employee expectations and communication responsibilities. Such training should include an element of "fraud awareness," the tone of which should be positive but nonetheless stress that fraud can be costly (and detrimental in other ways) to the entity and its employees.

In addition to training at the time of hiring, employees should receive refresher training periodically thereafter. Some organizations may consider ongoing training for certain positions, such as purchasing agents or employees with financial reporting responsibilities. Training should be specific to an employee's level within the organization, geographic location, and assigned responsibilities. For example, training for senior manager level personnel would normally be different from that of nonsupervisory employees, and training for purchasing agents would be different from that of sales representatives.

Confirmation

Management needs to clearly articulate that all employees will be held accountable to act within the entity's code of conduct. All employees within senior management and the finance function, as well as other employees in areas that might be exposed to unethical behavior (for example, procurement, sales and marketing) should be required to sign a code of conduct statement annually, at a minimum.

Requiring periodic confirmation by employees of their responsibilities will not only reinforce the policy but may also deter individuals from committing fraud and other violations and might identify problems before they become significant. Such confirmation may include statements that the individual understands the entity's expectations, has complied with the code of conduct, and is not aware of any violations of the code of conduct other than those the individual lists in his or her response. Although people with low integrity may not hesitate to sign a false confirmation, most people will want to avoid making a false statement in writing. Honest individuals are more likely to return their confirmations and to disclose what they know (including any conflicts of interest or other personal exceptions to the code of conduct). Thorough follow-up by internal auditors or others regarding nonreplies may uncover significant issues.

Discipline

The way an entity reacts to incidents of alleged or suspected fraud will send a strong deterrent message throughout the entity, helping to reduce the number of future occurrences. The following actions should be taken in response to an alleged incident of fraud:

- A thorough investigation of the incident should be conducted.[5]
- Appropriate and consistent actions should be taken against violators.
- Relevant controls should be assessed and improved.
- Communication and training should occur to reinforce the entity's values, code of conduct, and expectations.

[5] Many entities of sufficient size are employing antifraud professionals, such as certified fraud examiners, who are responsible for resolving allegations of fraud within the organization and who also assist in the detection and deterrence of fraud. These individuals typically report their findings internally to the corporate security, legal, or internal audit departments. In other instances, such individuals may be empowered directly by the board of directors or its audit committee.

Expectations about the consequences of committing fraud must be clearly communicated throughout the entity. For example, a strong statement from management that dishonest actions will not be tolerated, and that violators may be terminated and referred to the appropriate authorities, clearly establishes consequences and can be a valuable deterrent to wrongdoing. If wrongdoing occurs and an employee is disciplined, it can be helpful to communicate that fact, on a no-name basis, in an employee newsletter or other regular communication to employees. Seeing that other people have been disciplined for wrongdoing can be an effective deterrent, increasing the perceived likelihood of violators being caught and punished. It also can demonstrate that the entity is committed to an environment of high ethical standards and integrity.

Evaluating Antifraud Processes and Controls

Neither fraudulent financial reporting nor misappropriation of assets can occur without a perceived opportunity to commit and conceal the act. Organizations should be proactive in reducing fraud opportunities by (1) identifying and measuring fraud risks, (2) taking steps to mitigate identified risks, and (3) implementing and monitoring appropriate preventive and detective internal controls and other deterrent measures.

Identifying and Measuring Fraud Risks

Management has primary responsibility for establishing and monitoring all aspects of the entity's fraud risk-assessment and prevention activities.[6] Fraud risks often are considered as part of an enterprise-wide risk management program, though they may be addressed separately.[7] The fraud risk-assessment process should consider the vulnerability of the entity to fraudulent activity (fraudulent financial reporting, misappropriation of assets, and corruption) and whether any of those exposures could result in a material misstatement of the financial statements or material loss to the organization. In identifying fraud risks, organizations should consider organizational, industry, and country-specific characteristics that influence the risk of fraud.

The nature and extent of management's risk assessment activities should be commensurate with the size of the entity and complexity of its operations. For example, the risk assessment process is likely to be less formal and less structured in smaller entities. However, management should recognize that fraud can occur in organizations of any size or type, and that almost any employee may be capable of committing fraud given the right set of circumstances. Accordingly, management should develop a heightened "fraud awareness" and an appropriate fraud risk-management program, with oversight from the board of directors or audit committee.

---

[6] Management may elect to have internal audit play an active role in the development, monitoring, and ongoing assessment of the entity's fraud risk-management program. This may include an active role in the development and communication of the entity's code of conduct or ethics policy, as well as in investigating actual or alleged instances of noncompliance.

[7] Some organizations may perform a periodic self-assessment using questionnaires or other techniques to identify and measure risks. Self-assessment may be less reliable in identifying the risk of fraud due to a lack of experience with fraud (although many organizations experience some form of fraud and abuse, material financial statement fraud or misappropriation of assets is a rare event for most) and because management may be unwilling to acknowledge openly that they might commit fraud given sufficient pressure and opportunity.

Mitigating Fraud Risks

It may be possible to reduce or eliminate certain fraud risks by making changes to the entity's activities and processes. An entity may choose to sell certain segments of its operations, cease doing business in certain locations, or reorganize its business processes to eliminate unacceptable risks. For example, the risk of misappropriation of funds may be reduced by implementing a central lockbox at a bank to receive payments instead of receiving money at the entity's various locations. The risk of corruption may be reduced by closely monitoring the entity's procurement process. The risk of financial statement fraud may be reduced by implementing shared services centers to provide accounting services to multiple segments, affiliates, or geographic locations of an entity's operations. A shared services center may be less vulnerable to influence by local operations managers and may be able to implement more extensive fraud detection measures cost-effectively.

Implementing and Monitoring Appropriate Internal Controls

Some risks are inherent in the environment of the entity, but most can be addressed with an appropriate system of internal control. Once fraud risk assessment has taken place, the entity can identify the processes, controls, and other procedures that are needed to mitigate the identified risks. Effective internal control will include a well-developed control environment, an effective and secure information system, and appropriate control and monitoring activities.[8] Because of the importance of information technology in supporting operations and the processing of transactions, management also needs to implement and maintain appropriate controls, whether automated or manual, over computer-generated information.

In particular, management should evaluate whether appropriate internal controls have been implemented in any areas management has identified as posing a higher risk of fraudulent activity, as well as controls over the entity's financial reporting process. Because fraudulent financial reporting may begin in an interim period, management also should evaluate the appropriateness of internal controls over interim financial reporting.

Fraudulent financial reporting by upper-level management typically involves override of internal controls within the financial reporting process. Because management has the ability to override controls, or to influence others to perpetrate or conceal fraud, the need for a strong value system and a culture of ethical financial reporting becomes increasingly important. This helps create an environment in which other employees will decline to participate in committing a fraud and will use established communication procedures to report any requests to commit wrongdoing. The potential for management override also increases the need for appropriate oversight measures by the board of directors or audit committee, as discussed in the following section.

Fraudulent financial reporting by lower levels of management and employees may be deterred or detected by appropriate monitoring controls, such as having higher-level managers review and evaluate the financial results reported by individual operating units or subsidiaries. Unusual fluctuations in results of particular reporting units, or the lack of

[8] The report of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Internal Control—Integrated Framework*, provides reasonable criteria for management to use in evaluating the effectiveness of the entity's system of internal control.

expected fluctuations, may indicate potential manipulation by departmental or operating unit managers or staff.

Developing an Appropriate Oversight Process

To effectively prevent or deter fraud, an entity should have an appropriate oversight function in place. Oversight can take many forms and can be performed by many within and outside the entity, under the overall oversight of the audit committee (or board of directors where no audit committee exists).

Audit Committee or Board of Directors

The audit committee (or the board of directors where no audit committee exists) should evaluate management's identification of fraud risks, implementation of antifraud measures, and creation of the appropriate "tone at the top." Active oversight by the audit committee can help to reinforce management's commitment to creating a culture with "zero tolerance" for fraud. An entity's audit committee also should ensure that senior management (in particular, the CEO) implements appropriate fraud deterrence and prevention measures to better protect investors, employees, and other stakeholders. The audit committee's evaluation and oversight not only helps make sure that senior management fulfills its responsibility, but also can serve as a deterrent to senior management engaging in fraudulent activity (that is, by ensuring an environment is created whereby any attempt by senior management to involve employees in committing or concealing fraud would lead promptly to reports from such employees to appropriate persons, including the audit committee).

The audit committee also plays an important role in helping the board of directors fulfill its oversight responsibilities with respect to the entity's financial reporting process and the system of internal control.[9] In exercising this oversight responsibility, the audit committee should consider the potential for management override of controls or other inappropriate influence over the financial reporting process. For example, the audit committee may obtain from the internal auditors and independent auditors their views on management's involvement in the financial reporting process and, in particular, the ability of management to override information processed by the entity's financial reporting system (for example, the ability for management or others to initiate or record nonstandard journal entries). The audit committee also may consider reviewing the entity's reported information for reasonableness compared with prior or forecasted results, as well as with peers or industry averages. In addition, information received in communications from the independent auditors[10] can assist the audit committee in assessing the strength of the entity's internal control and the potential for fraudulent financial reporting.

As part of its oversight responsibilities, the audit committee should encourage management to provide a mechanism for employees to report concerns about unethical behavior, actual or suspected fraud, or violations of the entity's code of conduct or ethics policy.

---

[9] See the Report of the NACD Blue Ribbon Commission on the Audit Committee, (Washington, D.C.: National Association of Corporate Directors, 2000). For the board's role in the oversight of risk management, see Report of the NACD Blue Ribbon Commission on Risk Oversight, (Washington, D.C.: National Association of Corporate Directors, 2002).

[10] See section 325, *Communication of Internal Control Related Matters Noted in an Audit,* and section 380, *Communications With Audit Committees.*

The committee should then receive periodic reports describing the nature, status, and eventual disposition of any fraud or unethical conduct. A summary of the activity, follow-up and disposition also should be provided to the full board of directors.

If senior management is involved in fraud, the next layer of management may be the most likely to be aware of it. As a result, the audit committee (and other directors) should consider establishing an open line of communication with members of management one or two levels below senior management to assist in identifying fraud at the highest levels of the organization or investigating any fraudulent activity that might occur.[11] The audit committee typically has the ability and authority to investigate any alleged or suspected wrongdoing brought to its attention. Most audit committee charters empower the committee to investigate any matters within the scope of its responsibilities, and to retain legal, accounting, and other professional advisers as needed to advise the committee and assist in its investigation.

All audit committee members should be financially literate, and each committee should have at least one financial expert. The financial expert should possess:

- An understanding of generally accepted accounting principles and audits of financial statements prepared under those principles. Such understanding may have been obtained either through education or experience. It is important for someone on the audit committee to have a working knowledge of those principles and standards.
- Experience in the preparation and/or the auditing of financial statements of an entity of similar size, scope and complexity as the entity on whose board the committee member serves. The experience would generally be as a chief financial officer, chief accounting officer, controller, or auditor of a similar entity. This background will provide a necessary understanding of the transactional and operational environment that produces the issuer's financial statements. It will also bring an understanding of what is involved in, for example, appropriate accounting estimates, accruals, and reserve provisions, and an appreciation of what is necessary to maintain a good internal control environment.
- Experience in internal governance and procedures of audit committees, obtained either as an audit committee member, a senior corporate manager responsible for answering to the audit committee, or an external auditor responsible for reporting on the execution and results of annual audits.

Management

Management is responsible for overseeing the activities carried out by employees, and typically does so by implementing and monitoring processes and controls such as those discussed previously. However, management also may initiate, participate in, or direct the commission and concealment of a fraudulent act. Accordingly, the audit committee (or the board of directors where no audit committee exists) has the responsibility to oversee the activities of senior management and to consider the risk of fraudulent financial reporting involving the override of internal controls or collusion (see discussion on the audit committee and board of directors above).

[11] *Report of the NACD Best Practices Council: Coping with Fraud and Other Illegal Activity, A Guide for Directors, CEOs, and Senior Managers* (1998) sets forth "basic principles" and "implementation approaches" for dealing with fraud and other illegal activity.

Public companies should include a statement in the annual report acknowledging management's responsibility for the preparation of the financial statements and for establishing and maintaining an effective system of internal control. This will help improve the public's understanding of the respective roles of management and the auditor. This statement has also been generally referred to as a "Management Report" or "Management Certificate." Such a statement can provide a convenient vehicle for management to describe the nature and manner of preparation of the financial information and the adequacy of the internal accounting controls. Logically, the statement should be presented in close proximity to the formal financial statements. For example, it could appear near the independent auditor's report, or in the financial review or management analysis section.

Internal Auditors

An effective internal audit team can be extremely helpful in performing aspects of the oversight function. Their knowledge about the entity may enable them to identify indicators that suggest fraud has been committed. The *Standards for the Professional Practice of Internal Auditing* (IIA Standards), issued by the Institute of Internal Auditors, state, "The internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud." Internal auditors also have the opportunity to evaluate fraud risks and controls and to recommend action to mitigate risks and improve controls. Specifically, the IIA Standards require internal auditors to assess risks facing their organizations. This risk assessment is to serve as the basis from which audit plans are devised and against which internal controls are tested. The IIA Standards require the audit plan to be presented to and approved by the audit committee (or board of directors where no audit committee exists). The work completed as a result of the audit plan provides assurance on which management's assertion about controls can be made.

Internal audits can be both a detection and a deterrence measure. Internal auditors can assist in the deterrence of fraud by examining and evaluating the adequacy and the effectiveness of the system of internal control, commensurate with the extent of the potential exposure or risk in the various segments of the organization's operations. In carrying out this responsibility, internal auditors should, for example, determine whether:

- The organizational environment fosters control consciousness.
- Realistic organizational goals and objectives are set.
- Written policies (for example, a code of conduct) exist that describe prohibited activities and the action required whenever violations are discovered.
- Appropriate authorization policies for transactions are established and maintained.
- Policies, practices, procedures, reports, and other mechanisms are developed to monitor activities and safeguard assets, particularly in high-risk areas.
- Communication channels provide management with adequate and reliable information.
- Recommendations need to be made for the establishment or enhancement of cost-effective controls to help deter fraud.

Internal auditors may conduct proactive auditing to search for corruption, misappropriation of assets, and financial statement fraud. This may include the use of computer-assisted audit techniques to detect particular types of fraud. Internal auditors also can employ analytical and other procedures to isolate anomalies and perform detailed re-

views of high-risk accounts and transactions to identify potential financial statement fraud. The internal auditors should have an independent reporting line directly to the audit committee, to enable them to express any concerns about management's commitment to appropriate internal controls or to report suspicions or allegations of fraud involving senior management.

Independent Auditors

Independent auditors can assist management and the board of directors (or audit committee) by providing an assessment of the entity's process for identifying, assessing, and responding to the risks of fraud. The board of directors (or audit committee) should have an open and candid dialogue with the independent auditors regarding management's risk assessment process and the system of internal control. Such a dialogue should include a discussion of the susceptibility of the entity to fraudulent financial reporting and the entity's exposure to misappropriation of assets.

Certified Fraud Examiners

Certified fraud examiners may assist the audit committee and board of directors with aspects of the oversight process either directly or as part of a team of internal auditors or independent auditors. Certified fraud examiners can provide extensive knowledge and experience about fraud that may not be available within a corporation. They can provide more objective input into management's evaluation of the risk of fraud (especially fraud involving senior management, such as financial statement fraud) and the development of appropriate antifraud controls that are less vulnerable to management override. They can assist the audit committee and board of directors in evaluating the fraud risk assessment and fraud prevention measures implemented by management. Certified fraud examiners also conduct examinations to resolve allegations or suspicions of fraud, reporting either to an appropriate level of management or to the audit committee or board of directors, depending upon the nature of the issue and the level of personnel involved.

Other Information

To obtain more information on fraud and implementing antifraud programs and controls, please go to the following Web sites where additional materials, guidance, and tools can be found.

American Institute of Certified Public Accountants	www.aicpa.org
Association of Certified Fraud Examiners	www.cfenet.com
Financial Executives International	www.fei.org
Information Systems Audit and Control Association	www.isaca.org
The Institute of Internal Auditors	www.theiia.org
Institute of Management Accountants	www.imanet.org
National Association of Corporate Directors	www.nacdonline.org
Society for Human Resource Management	www.shrm.org

Attachment 1: AICPA "CPA's Handbook of Fraud and Commercial Crime Prevention," An Organizational Code of Conduct

The following is an example of an organizational code of conduct, which includes definitions of what is considered unacceptable, and the consequences of any breaches thereof.

The specific content and areas addressed in an entity's code of conduct should be specific to that entity.

Organizational Code of Conduct
The Organization and its employees must, at all times, comply with all applicable laws and regulations. The Organization will not condone the activities of employees who achieve results through violation of the law or unethical business dealings. This includes any payments for illegal acts, indirect contributions, rebates, and bribery. The Organization does not permit any activity that fails to stand the closest possible public scrutiny.

All business conduct should be well above the minimum standards required by law. Accordingly, employees must ensure that their actions cannot be interpreted as being, in any way, in contravention of the laws and regulations governing the Organization's worldwide operations.

Employees uncertain about the application or interpretation of any legal requirements should refer the matter to their superior, who, if necessary, should seek the advice of the legal department.

General Employee Conduct
The Organization expects its employees to conduct themselves in a businesslike manner. Drinking, gambling, fighting, swearing, and similar unprofessional activities are strictly prohibited while on the job.

Employees must not engage in sexual harassment, or conduct themselves in a way that could be construed as such, for example, by using inappropriate language, keeping or posting inappropriate materials in their work area, or accessing inappropriate materials on their computer.

Conflicts of Interest
The Organization expects that employees will perform their duties conscientiously, honestly, and in accordance with the best interests of the Organization. Employees must not use their position or the knowledge gained as a result of their position for private or personal advantage. Regardless of the circumstances, if employees sense that a course of action they have pursued, are presently pursuing, or are contemplating pursuing may involve them in a conflict of interest with their employer, they should immediately communicate all the facts to their superior.

Outside Activities, Employment, and Directorships
All employees share a serious responsibility for the Organization's good public relations, especially at the community level. Their readiness to help with religious, charitable, educational, and civic activities brings credit to the Organization and is encouraged. Employees must, however, avoid acquiring any business interest or participating in any other activity outside the Organization that would, or would appear to:

- Create an excessive demand upon their time and attention, thus depriving the Organization of their best efforts on the job.
- Create a conflict of interest—an obligation, interest, or distraction—that may interfere with the independent exercise of judgment in the Organization's best interest.

Relationships With Clients and Suppliers
Employees should avoid investing in or acquiring a financial interest for their own accounts in any business organization that has a contractual relationship with the Organization, or that provides goods or services, or both to the Organization, if such investment or interest could influence or create the impression of influencing their decisions in the performance of their duties on behalf of the Organization.

Gifts, Entertainment, and Favors
Employees must not accept entertainment, gifts, or personal favors that could, in any way, influence, or appear to influence, business decisions in favor of any person or organization with whom or with which the Organization has, or is likely to have, business dealings. Similarly, employees must not accept any other preferential treatment under these circumstances because their position with the Organization might be inclined to, or be perceived to, place them under obligation.

Kickbacks and Secret Commissions
Regarding the Organization's business activities, employees may not receive payment or compensation of any kind, except as authorized under the Organization's remuneration policies. In particular, the Organization strictly prohibits the acceptance of kickbacks and secret commissions from suppliers or others. Any breach of this rule will result in immediate termination and prosecution to the fullest extent of the law.

Organization Funds and Other Assets
Employees who have access to Organization funds in any form must follow the prescribed procedures for recording, handling, and protecting money as detailed in the Organization's instructional manuals or other explanatory materials, or both. The Organization imposes strict standards to prevent fraud and dishonesty. If employees become aware of any evidence of fraud and dishonesty, they should immediately advise their superior or the Law Department so that the Organization can promptly investigate further.

When an employee's position requires spending Organization funds or incurring any reimbursable personal expenses, that individual must use good judgment on the Organization's behalf to ensure that good value is received for every expenditure.

Organization funds and all other assets of the Organization are for Organization purposes only and not for personal benefit. This includes the personal use of organizational assets, such as computers.

Organization Records and Communications
Accurate and reliable records of many kinds are necessary to meet the Organization's legal and financial obligations and to manage the affairs of the Organization. The Organization's books and records must reflect in an accurate and timely manner all business transactions. The employees responsible for accounting and recordkeeping must fully disclose and record all assets, liabilities, or both, and must exercise diligence in enforcing these requirements.

Employees must not make or engage in any false record or communication of any kind, whether internal or external, including but not limited to:

- False expense, attendance, production, financial, or similar reports and statements
- False advertising, deceptive marketing practices, or other misleading representations

Dealing With Outside People and Organizations
Employees must take care to separate their personal roles from their Organization positions when communicating on matters not involving Organization business. Employees must not use Organization identification, stationery, supplies, and equipment for personal or political matters.

When communicating publicly on matters that involve Organization business, employees must not presume to speak for the Organization on any topic, unless they are certain that the views they express are those of the Organization, and it is the Organization's desire that such views be publicly disseminated.

When dealing with anyone outside the Organization, including public officials, employees must take care not to compromise the integrity or damage the reputation of either the Organization, or any outside individual, business, or government body.

Prompt Communications
In all matters relevant to customers, suppliers, government authorities, the public and others in the Organization, all employees must make every effort to achieve complete, accurate, and timely communications—responding promptly and courteously to all proper requests for information and to all complaints.

Privacy and Confidentiality
When handling financial and personal information about customers or others with whom the Organization has dealings, observe the following principles:

1. Collect, use, and retain only the personal information necessary for the Organization's business. Whenever possible, obtain any relevant information directly from the person concerned. Use only reputable and reliable sources to supplement this information.
2. Retain information only for as long as necessary or as required by law. Protect the physical security of this information.
3. Limit internal access to personal information to those with a legitimate business reason for seeking that information. Use only personal information for the purposes for which it was originally obtained. Obtain the consent of the person concerned before externally disclosing any personal information, unless legal process or contractual obligation provides otherwise.

Attachment 2: Financial Executives International Code of Ethics Statement

The mission of Financial Executives International (FEI) includes significant efforts to promote ethical conduct in the practice of financial management throughout the world. Senior financial officers hold an important and elevated role in corporate governance. While members of the management team, they are uniquely capable and empowered to ensure that all stakeholders' interests are appropriately balanced, protected, and preserved. This code provides principles that members are expected to adhere to and advocate. They embody rules regarding individual and peer responsibilities, as well as responsibilities to employers, the public, and other stakeholders.

All members of FEI will:

1. Act with honesty and integrity, avoiding actual or apparent conflicts of interest in personal and professional relationships.

2. Provide constituents with information that is accurate, complete, objective, relevant, timely, and understandable.
3. Comply with rules and regulations of federal, state, provincial, and local governments, and other appropriate private and public regulatory agencies.
4. Act in good faith; responsibly; and with due care, competence, and diligence, without misrepresenting material facts or allowing one's independent judgment to be subordinated.
5. Respect the confidentiality of information acquired in the course of one's work except when authorized or otherwise legally obligated to disclose. Confidential information acquired in the course of one's work will not be used for personal advantage.
6. Share knowledge and maintain skills important and relevant to constituents' needs.
7. Proactively promote ethical behavior as a responsible partner among peers, in the work environment, and in the community.
8. Achieve responsible use of and control over all assets and resources employed or entrusted.

APPENDIX D: ILLUSTRATIVE INQUIRIES FOR UPDATING WALKTHROUGH PROCEDURES[1]

It is recommended that management perform walkthrough procedures to understand the design of internal control. Periodically, the walkthrough should be updated, and this material provides recommendations and example inquiries for updating these walkthroughs. The material applies directly to auditors, not to company management, and it directly addresses auditors only. However, this material may also be helpful to management in applying the guidance in PCAOB Auditing Standard No. 2 that directly affects the planning and performance of the company's self-assessment of internal control effectiveness.

When updating your understanding of significant processes and major transactions, your objective is to determine whether the engagement team's previous understanding of the client's information processing stream remains relevant and, if not, to make any required changes to your documentation—including walkthroughs—to reflect your updated knowledge. Your primary method for gathering information will be inquiries of company personnel. When making these inquiries—

- Expand your inquiries to include those outside of management. Ask people who perform control procedures and process information as part of their daily job requirements.
- Make inquiries of those outside of the accounting department, for example, individuals involved in operations.

Your inquiries should be designed to gather information about—

- Changes in the company's business activities that have resulted in new or increased risks.
- Whether and how specific information processes and related controls were changed in response to new or increased risks.
- Changes to information processes or controls that should have been made based on previously identified internal control deficiencies.
- Other changes to processes, controls, or transactions.

Illustrative Inquiries

Consider asking the following questions of company personnel.

- Over the past year, what have been the most significant changes made to the following.
  - — The business environment in which the company operates.
  - — Company personnel, especially those with information processing or control duties
  - — Information technology
  - — Lines of business
  - — Accounting and financial reporting standards that affect the company

[1] From *The SOX 404 Toolkit*, by Michael Ramos, published by John Wiley & Sons. Copyright Michael Ramos, 2004. This material is used by permission of John Wiley & Sons, Inc.

- What effect have these changes had on the company's—
  - — Operations
  - — Types of transactions entered into or counterparties to those transactions
  - — Ability to capture, process or report financial information
- How has company growth or retrenchment affected—
  - — Operations
  - — Types of transactions entered into or counterparties to those transactions
  - — Ability to capture, process or report financial information
- How has the company modified its information processing and controls to respond to new financial reporting risks?
- What internal control weaknesses were identified as part of last year's audit? Since last year's audit, what additional weaknesses has management identified?
- What actions has management taken in response to known internal control weaknesses, both those identified by the auditors and by management?

  Note. You should consider management's response to known internal control weaknesses, or lack of a response, when evaluating the entity's control environment.
- What kinds of accounting system or financial reporting errors—
  - — Persist
  - — Have surfaced in the past year
- What other changes, not yet discussed, has management made to its—
  - — Financial information processing system and related controls
  - — Internal control
- Why were these changes made?

APPENDIX E: SAMPLING IN COMPLIANCE TESTS OF INTERNAL CONTROL

Management may wish to sample a selection of transactions to perform procedures to evaluate the operating effectiveness of controls. These excerpts from Chapter 3, "Sampling in Tests of Controls," and Appendix A, "Statistical Sampling Tables for Tests of Controls," of the AICPA Audit and Accounting Guide *Audit Sampling* provide guidance on sample selection and determining sample sizes, including tables for calculating sample size. The material applies directly to auditors, not to company management, and it directly addresses auditors only. However, this material may also be helpful to management in applying the guidance in PCAOB Auditing Standard No. 2 that directly affects the planning and performance of the company's self-assessment of internal control effectiveness.

Determining the Method of Selecting the Sample

3.21 Sample items should be selected so the sample can be expected to be representative of the population. Therefore, all items in the population should have an opportunity to be selected. An overview of selection methods follows.

Random-Number Sampling

3.22 The auditor may select a random sample by matching random numbers generated by a computer or selected from a random-number table with, for example, document numbers. With this method every sampling unit has the same probability of being selected as every other sampling unit in the population, and every combination of sampling units has the same probability of being selected as every other combination of the same number of sampling units. This approach is appropriate for both nonstatistical and statistical sampling applications. Because statistical sampling applications require the auditor to select the sample so he or she can measure the probability of selecting the combination of sampling units actually chosen, this approach is especially useful for statistical sampling.

Systematic Sampling

3.23 For this method the auditor determines a uniform interval by dividing the number of physical units in the population by the sample size. A starting point is selected in the first interval, and one item is selected throughout the population at each of the uniform intervals from the starting point. For example, if the auditor wishes to select 100 items from a population of 20,000 items, the uniform interval is every 200th item. First the auditor selects a starting point and then selects every 200th item from the random start, including the starting point.

3.24 When a random starting point is used, the systematic method provides a sample that allows every sampling unit in the population an equal chance of being selected. If the population is arranged randomly, systematic selection is essentially the same as random-number selection. However, unlike random-number sampling, this method does not give every possible combination of sampling units the same probability of being selected. For example, a population of employees on a payroll for a construction company might be organized by

teams; each team consists of a crew leader and nine other workers. A selection of every tenth employee will either list every crew leader or no crew leaders, depending on the random start. No combination would include both crew leaders and other employees. In these circumstances the auditor may consider using a different sample selection method, such as random-number selection, or making a systematic selection using several random starting points or an interval that does not coincide with the pattern in the population. Systematic selection is useful for nonstatistical sampling, and if the starting point is a random number, it might be useful for statistical sampling.

Other Methods of Selection

3.25 Auditors sometimes use two other selection techniques, block sampling and haphazard sampling. A *block sample* consists of contiguous transactions.[2] For example, a block sample from a population of all vouchers processed for the year 20XX might be all vouchers processed on February 3, May 17, and July 19, 20XX. This sample includes only 3 sampling units out of 250 business days because the sampling unit, in this case, is a period of time rather than an individual transaction. A sample with so few blocks is generally not adequate to reach a reasonable audit conclusion. Although a block sample might be designed with enough blocks to minimize this limitation, using such samples might be inefficient. If an auditor decides to use a block sample, he or she should exercise special care to control sampling risk in designing that sample.

3.26 A *haphazard sample* consists of sampling units selected without any conscious bias, that is, without any special reason for including or omitting items from the sample. It does not consist of sampling units selected in a careless manner; rather, it is selected in a manner that can be expected to be representative of the population. For example, when the physical representation of the population is a file cabinet drawer of vouchers, a haphazard sample of all vouchers processed for the year 20XX might include any of the vouchers that the auditor pulls from the drawer, regardless of each voucher's size, shape, location, or other physical features.

3.27 The auditor using haphazard selection should be careful to avoid distorting the sample by selecting, for example, only unusual or physically small items or by omitting such items as the first or last in the physical representation of the population. Although haphazard sampling is useful for nonstatistical sampling, it is not used for statistical sampling because it does not allow the auditor to measure the probability of selecting the combination of sampling units.

Determining the Sample Size

3.28 This section discusses the factors that auditors consider when using judgment to determine appropriate sample sizes. Auditors using nonstatistical sampling do not need to quantify these factors; rather, they might consider using estimates in qualitative terms, such as *none*, *few*, or *many*. Appendix A includes additional guidance, along with several tables that should help auditors apply the following discussion to statistical sampling applications.

[2] A variation of block sampling that can be designed to yield an adequate statistical sampling approach is called *cluster sampling*. The considerations for designing a cluster sample are beyond the scope of this guide. Such guidance can be found in technical references on statistical sampling.

Considering the Acceptable Risk of Assessing Control Risk Too Low

3.29 The auditor is concerned with two aspects of sampling risk in performing tests of controls: The risk of assessing control risk too low and the risk of assessing control risk too high. The risk of assessing control risk too low is the risk that the assessed level of control risk based on the sample is less than the true operating effectiveness of the control. Conversely, the risk of assessing control risk too high is the risk that the assessed level of control risk based on the sample is greater than the true operating effectiveness of the control.

3.30 The risk of assessing control risk too high relates to the efficiency of the audit. The auditor's assessed level of control risk based on a sample may lead him or her to increase the scope of substantive tests unnecessarily to compensate for the perceived higher level of control risk. Although the audit might be less efficient in this circumstance, it is nevertheless effective. However, the second aspect of sampling risk in performing tests of controls—the risk of assessing control risk too low—relates to the effectiveness of the audit. If the auditor assesses control risk too low, he or she inappropriately reduces the evidence obtained from substantive tests. Therefore, the discussion of sampling risk in the following paragraphs relates primarily to the risk of assessing control risk too low.

3.31 Samples taken for tests of controls are intended to provide evidence about the operating effectiveness of the controls. Because a test of controls is the primary source of evidence about whether the controls are operating effectively, the auditor generally wishes to obtain a high degree of assurance that the conclusions from the sample would not differ from the conclusions that would be reached if the test were applied in the same way to all transactions. Therefore, in these circumstances the auditor should allow for a low level of risk of assessing control risk too low. Although consideration of risk is implicit in all audit sampling applications, it is explicit in statistical sampling.

3.32 There is an inverse relationship between the risk of assessing control risk too low and sample size. If the auditor is willing to accept only a low risk of assessing control risk too low, the sample size would ordinarily be larger than if a higher risk were acceptable. Although the auditor need not quantify this risk (for example, it may be assessed as low, moderate, or high), table 3.1 illustrates the relative effect on sample size of various levels of the risk of assessing control risk too low. Computations use statistical theory and assume a tolerable rate of 5 percent, a large population size, and an expected population deviation rate of approximately 1 percent.

Table 3.1 Effect of Risk of Assessing Control Risk Too Low on Sample Size

Risk of Assessing Control Risk Too Low (%)	*Sample Size*
10	77
5	93
1	165

3.33 Some auditors find it practical to select one level of risk for all tests of controls and to assess, for each separate test, a tolerable rate based on the planned assessed level of control risk.

Considering the Tolerable Rate

3.34 In designing substantive tests for a particular financial statement assertion, the auditor considers the assessed level of control risk. The tolerable rate is the maximum rate of deviation from a prescribed control that auditors are willing to accept without altering the planned assessed level of control risk. SAS No. 39, *Audit Sampling* (AICPA, *Professional Standards*, vol. 1, AU sec. 350), states that "in determining the tolerable rate, the auditor should consider (*a*) the planned assessed level of control risk, and (*b*) the degree of assurance desired by the evidential matter in the sample." Sometimes the auditor specifies a high tolerable rate because he or she plans to assess control risk at a higher level. A very high tolerable rate often indicates that the control's operating effectiveness does not significantly reduce the extent of related substantive tests. In that case, the particular test of controls might be unnecessary and may be omitted.

3.35 Table 3.2 illustrates one way in which an auditor might express the relationship between tolerable rates and the auditor's planned assessed levels of control risk. Overlapping ranges are presented.

Table 3.2 Relationship Between Tolerable Rates and the Auditor's Planned Assessed Levels of Control Risk

Planned Assessed Level of Control Risk	*Tolerable Rate (%)*
Low	3–7
Moderate	6–12
Slightly below the maximum	11–20
Maximum	Omit test

3.36 In assessing the tolerable rate, the auditor should consider that although deviations from pertinent controls increase the risk of material misstatements in the accounting records, such deviations do not necessarily result in misstatements. A recorded disbursement that does not show evidence of required approval might nevertheless be a transaction that is properly authorized and recorded. Therefore, a tolerable rate of 5 percent does not necessarily imply that 5 percent of the dollars is misstated. Auditors usually assess a tolerable rate for tests of controls that is greater than the tolerable rate of dollar misstatement. This conclusion is based on the fact that deviations would result in misstatements in the accounting records only if the deviations and the misstatements occurred on the same transactions.

3.37 There is an inverse relationship between the tolerable rate and sample size. Table 3.3 illustrates the relative effect of tolerable rate on sample size. The table is based on the assumptions of a 5 percent risk of assessing control risk too low, a large population size, and an expected population deviation rate of 0.0 percent.

Table 3.3 Effect of Tolerable Rate on Sample Size

Tolerable Rate (%)	*Sample Size*
2	149
4	74
6	49
8	36
10	29
20	14

3.38 When performing tests of controls, generally the auditor is concerned only that the actual rate of deviation in the population does not exceed the tolerable rate; that is, if, while evaluating the sample results, the auditor finds the sample deviation rate to be less than the tolerable rate for the population, he or she needs to consider only the risk that such a result might be obtained when the actual deviation rate in the population exceeds the tolerable rate. The sample-size illustrations in this chapter assume that the sample is designed to measure only the risk that the estimated deviation rate understates the population deviation rate. This is sometimes referred to as an *upper-limit approach.*[3]

3.39 If, after performing the sampling application, the auditor finds that the rate of deviation from the prescribed control is close to or exceeds the tolerable rate, the auditor might decide that there is an unacceptably high sampling risk that the deviation rate for the population exceeds the tolerable rate. In such cases the auditor should increase the assessed level of control risk.

3.40 An auditor using statistical sampling generally calculates an allowance for sampling risk. If the auditor finds that the rate of deviation from the prescribed control plus the allowance for sampling risk exceeds the tolerable rate, he or she should increase the assessed level of control risk.

Considering the Expected Population Deviation Rate

3.41 The auditor estimates the expected population deviation rate by considering such factors as results of the prior year's tests and the control environment. The prior year's results should be considered in light of changes in the entity's internal control and changes in personnel.

3.42 There is a direct relationship between the expected population deviation rate and the sample size to be used by the auditor. As the expected population deviation rate approaches the tolerable rate, the need arises for more precise information from the sample. Therefore, for a given tolerable rate, the auditor selects a larger sample size as the expected population deviation rate, sometimes referred to as the expected rate of occurrence, increases. Table 3.4 illustrates the relative effect of the expected population deviation rate on sample size. The

[3] For a discussion of interval estimates, see Donald Roberts, *Statistical Auditing* (New York: AICPA, 1978), p. 53.

table is based on the assumptions of a 5 percent tolerable rate, a large population size, and a 5 percent risk of assessing control risk too low.[4]

3.43 The expected population deviation rate should not equal or exceed the tolerable rate. If the auditor believes that the actual deviation rate is higher than the tolerable rate, he or she generally increases the assessed level of control risk or omits testing of that control.

3.44 The auditor might control the risk of assessing control risk too high by adjusting the sample size for the assessment of the deviation rate he or she expects to find in the population.

Table 3.4 Relative Effect of the Expected Population Deviation Rate on Sample Size

Expected Population Deviation Rate (%)	*Sample Size*
0.0*	59
1.0	93
1.5	124
2.0	181
2.5	234

* Some auditors use a sampling approach referred to as *discovery sampling*. Discovery sampling is essentially the same as the approach described in this chapter when the auditor assumes an expected population deviation rate of zero.

Considering the Effect of Population Size

3.45 The size of the population has little or no effect on the determination of sample size except for very small populations. For example, it is generally appropriate to treat any population of more than 5,000 sampling units as if it were infinite. If the population size is under 5,000 sampling units, the population size may have a small effect on the calculation of sample size.

3.46 Table 3.5 illustrates the limited effect of population size on sample size. Computations use statistical theory and assume a 5 percent risk of assessing control risk too low, a 1 percent expected population deviation rate, and a 5 percent tolerable rate.

[4] Large sample sizes, such as 234, are included for illustrative purposes, not to suggest that it would be cost beneficial to perform tests of controls using such large sample sizes.

Table 3.5 Limited Effect of Population Size on Sample Size

Population Size	*Sample Size*
50	45
100	64
500	87
1,000	90
2,000	92
5,000	93
10,000	93

3.47 Because population size has little or no effect on sample size, all other illustrations of sample sizes for tests of controls assume a large population size.

Considering a Sequential or a Fixed Sample-Size Approach

3.48 Audit samples may be designed using either a fixed sampling plan or a sequential sampling plan. Under a fixed sampling plan, the auditor examines a single sample of a specified size. In *sequential sampling* (sometimes referred to as *stop-or-go sampling*), the sample is taken in several steps, with each step conditional on the results of the previous step. Guidance on sequential sampling plans is included in appendix B of this Audit and Accounting Guide.

Developing Sample-Size Guidelines

3.49 An auditor may decide to establish guidelines for sample sizes for tests of controls based on attribute sampling tables. An example of such guidelines is illustrated in table 3.6.

Table 3.6 Sample Sizes for Tests of Controls Based on Attribute Sampling Tables

Planned Assessed Level of Control Risk	*Sample Size*
Slightly below the maximum	12–20
Moderate	20–35
Low	30–75

3.50 The numbers in the table were determined using a 10 percent risk of assessing control risk too low and an expected population deviation rate of 0 percent. If the auditor finds one or more deviations in the sample, he or she needs to increase the sample size or increase the assessed level of control risk.

Performing the Sampling Plan

3.51 After the sampling plan has been designed, the auditor selects the sample and examines the selected items to determine whether they contain deviations from the prescribed

control.[5] When selecting the sampling units, it is often practical to select several in addition, as extras. If the size of the remaining sample is inadequate for the auditor's objectives, he or she may use the extra sampling units. If the auditor has selected a random sample, any additional items used as replacements should be used in the same order in which the numbers were generated. The auditor who uses a systematic sampling selection needs to examine all extra selected items so each item in the entire population has a chance of selection.

Voided Documents

3.52 An auditor might select a voided item to be included in a sample. For example, an auditor performing a test of controls related to the entity's vouchers might match random numbers with voucher numbers for the period included in the population. However, a random number might match with a voucher that has been voided. If the auditor obtains reasonable assurance that the voucher has been properly voided and does not represent a deviation from the prescribed control, he or she should replace the voided voucher and, if random sampling is used, should match a replacement random number with the appropriate voucher.

Unused or Inapplicable Documents

3.53 The auditor's consideration of unused or inapplicable documents is similar to the consideration of voided documents. For example, a sequence of potential voucher numbers might include unused numbers or an intentional omission of certain numbers. If the auditor selects an unused number, he or she should obtain reasonable assurance that the voucher number actually represents an unused voucher and does not represent a deviation from the control. The auditor then replaces the unused voucher number with an additional voucher number. Sometimes a selected item is inapplicable for a given definition of a deviation. For example, a telephone expense selected as part of a sample for which a deviation has been defined as a "transaction not supported by receiving report" may not be expected to be supported by a receiving report. If the auditor has obtained reasonable assurance that the transaction is not applicable and does not represent a deviation from the prescribed control, he or she would replace the item with another transaction for testing the control of interest.

Misstatements in Estimating Population Sequences

3.54 If the auditor is using random-number sampling to select sampling units, the population size and numbering sequence might be estimated before the controls have been performed. The most common example of this situation occurs when the auditor has defined the population to include the entire period under audit but plans to perform a portion of the sampling procedure before the end of the period. If the auditor overestimates the population size and numbering sequence, any numbers that are selected as part of the sample and that exceed the actual numbering sequence used are treated as unused documents. Such numbers would be replaced by matching extra random numbers with appropriate documents.

3.55 In planning and performing an audit sampling procedure, the auditor should also consider the two following special situations that may occur.

Stopping the Test Before Completion

3.56 Occasionally the auditor might find a large number of deviations in auditing the first part of a sample. As a result, he or she might believe that even if no additional deviations

[5] Some auditors find it practical to select a single sample for more than one sample objective. This approach is appropriate if the sample size is adequate and selection procedures are appropriate for each of the related sampling objectives.

were to be discovered in the remainder of the sample, the results of the sample would not support the planned assessed level of control risk. Under these circumstances, the auditor should reassess the level of control risk and consider whether it is necessary to continue the test to support the new assessed level of control risk.

Inability to Examine Selected Items

3.57 The auditor should apply to each sampling unit auditing procedures that are appropriate to achieve the objective of the test of controls. In some circumstances, performance of the prescribed control being tested is shown only on the selected sample document. If that document cannot be located or if for any other reason the auditor is unable to examine the selected item, he or she will probably be unable to use alternative procedures to test whether that control was applied as prescribed. If the auditor is unable to apply the planned audit procedures or appropriate alternative procedures to selected items, he or she should consider selected items to be deviations from the controls for the purpose of evaluating the sample. In addition, the auditor should consider the reasons for this limitation and the effect that such a limitation might have on his or her understanding of internal control and assessment of control risk.

Evaluating the Sample Results

3.58 After completing the examination of the sampling units and summarizing the deviations from prescribed controls, the auditor evaluates the results. Whether the sample is statistical or nonstatistical, the auditor uses judgment in evaluating the results and reaching an overall conclusion.

Calculating the Deviation Rate

3.59 Calculating the deviation rate in the sample involves dividing the number of observed deviations by the sample size. The deviation rate in the sample is the auditor's best estimate of the deviation rate in the population from which it was selected.

Considering Sampling Risk

3.60 As discussed in chapter 2, sampling risk arises from the possibility that when testing is restricted to a sample, the auditor's conclusions might differ from those he or she would have reached if the test were applied in the same way to all items in the account balance or class of transactions.

3.61 When evaluating a sample for a test of controls, the auditor should consider sampling risk. If the estimate of the population deviation rate (the sample deviation rate) is less than the tolerable rate for the population, the auditor should consider the risk that such a result might be obtained even if the deviation rate for the population exceeds the tolerable rate for the population. SAS No. 39 (AICPA, *Professional Standards*, vol. 1, AU sec. 350.41) provides the following general example of how an auditor might consider sampling risk for tests of controls:

> If the tolerable rate for a population is 5 percent and no deviations are found in a sample of 60 items, the auditor may conclude that there is an acceptably low sampling risk that the true deviation rate in the population exceeds the tolerable rate of 5 percent. On the other hand, if the sample includes, for example, two or more deviations, the auditor may conclude that there is an unacceptably high sampling risk that the rate of deviations in the population exceeds the tolerable rate of 5 percent.

3.62 If an auditor is performing a statistical sampling application, he or she often uses a table or computer program to assist in measuring the allowance for sampling risk. For example, most computer programs used to evaluate sampling applications calculate an estimate of the upper limit of the possible deviation rate based on the sample size and the sample results at the auditor's specified risk of assessing control risk too low.

3.63 If the auditor is performing a nonstatistical sampling application, sampling risk cannot be measured directly. However, it is generally appropriate for the auditor to assume that the sample results do not support the planned assessed level of control risk if the rate of deviation identified in the sample exceeds the expected population deviation rate used in designing the sample. In that case, there is likely to be an unacceptably high risk that the true deviation rate in the population exceeds the tolerable rate. If the auditor concludes that there is an unacceptably high risk that the true population deviation rate could exceed the tolerable rate, it might be practical to expand the test to sufficient additional items to reduce the risk to an acceptable level. Rather than testing additional items, however, it is generally more efficient to increase the auditor's assessed level of control risk to the level supported by the results of the original sample.

3.64 Appendix A includes statistical sampling tables that should help the auditor in using professional judgment to evaluate the results of statistical samples for tests of controls. The tables may also be useful to auditors using nonstatistical sampling.

Considering the Qualitative Aspects of the Deviations

3.65 In addition to evaluating the frequency of deviations from pertinent controls, the auditor should consider the qualitative aspects of the deviations. These include (1) the nature and cause of the deviations, such as whether they result from fraud or errors, which may arise from misunderstanding of instructions or carelessness and (2) the possible relationship of the deviations to other phases of the audit. The discovery of fraud ordinarily requires a broader consideration of the possible implications than does the discovery of an error.

Reaching an Overall Conclusion

3.66 The auditor uses professional judgment to reach an overall conclusion about the effect that the evaluation of the results will have on his or her assessed level of control risk and thus on the nature, timing, and extent of planned substantive tests. If the sample results, along with other relevant evidential matter, support the planned assessed level of control risk, the auditor generally does not need to modify planned substantive tests. If the planned assessed level of control risk is not supported, the auditor would ordinarily either perform tests of other controls that could support the planned assessed level of control risk or increase the assessed level of control risk.

* * *

Appendix A to Audit Sampling Guide
Statistical Sampling Tables for Compliance Tests of Controls

* * *

Using the Tables

A.2 Chapter 3, "Sampling in Tests of Controls," discusses the factors that the auditor needs to consider when planning an audit sampling application for a test of controls. For statistical sampling, the auditor needs to specify explicitly (1) an acceptable level of the risk of assess-

ing control risk too high, (2) the tolerable rate, and (3) the expected population deviation rate. This appendix includes tables for 5 percent and 10 percent levels of risk of assessing control risk too low. Either a table in another reference on statistical sampling or a computer program is necessary if the auditor desires another level of risk of assessing control risk too low.

A.3 The auditor selects the table for the acceptable level of risk of assessing control risk too low and then reads down the expected population deviation rate column to find the appropriate rate. Next the auditor locates the column corresponding to the tolerable rate. The appropriate sample size is shown where the two factors meet.

A.4 In some circumstances, tables A.1 and A.2 can be used to evaluate the sample results. The parenthetical number shown next to each sample size is the expected number of deviations to be found in the sample. The expected number of deviations is the expected population deviation rate multiplied by the sample size. If the auditor finds that number of deviations or fewer in the sample, he or she can conclude that at the desired risk of assessing control risk too low, the projected deviation rate for the population plus an allowance for sampling risk is not more than the tolerable rate. In these circumstances the auditor need not use table A.3 or A.4 to evaluate the sample results.

A.5 If more than the expected number of deviations are found in the sample, the auditor cannot conclude that the population deviation rate is less than the tolerable rate. Accordingly, the test would not support his or her planned assessment of control risk. However, the sample might support some lesser assessment.

A.6 If the number of deviations found in the sample is not the expected number of deviations shown in the parentheses in tables A.1 or A.2, and the auditor wishes to calculate the maximum deviation rate in the population, he or she can evaluate the sample results using either table A.3 for a 5 percent acceptable risk of assessing control risk too low or table A.4 for a 10 percent acceptable risk of assessing control risk too low. Space limitations do not allow tables A.3 and A.4 to include evaluations for all possible sample sizes or for all possible numbers of deviations found. If the auditor is evaluating sample results for a sample size or number of deviations not shown in these tables, he or she can use either a table in another reference on statistical sampling or a computer program. Alternatively, the auditor might interpolate between sample sizes shown in these tables. Any error due to interpolation should not be significant to the auditor's evaluation. If the auditor wishes to be conservative, he or she can use the next smaller sample size shown in the table to evaluate the number of deviations found in the sample.

A.7 The auditor selects the table applicable to the acceptable level of risk of assessing control risk too low and then reads down the sample-size column to find the appropriate sample size. Next the auditor locates the column corresponding to the number of deviations found in the sample. The projection of the sample results to the population plus an allowance for sampling risk (that is, the maximum population deviation rate) is shown where the two factors meet. If this maximum population deviation rate is less than the tolerable rate, the test supports the planned assessment of control risk.

Applying Nonstatistical Sampling

A.8 The auditor using nonstatistical sampling for tests of controls uses his or her professional judgment to consider the factors described in chapter 3 in determining sample sizes.

The relative effect of each factor on the appropriate nonstatistical sample size is illustrated in chapter 3 and is summarized in exhibit A.1.

Exhibit A.1 Determining Sample Sizes

Factor	*General Effect on Sample Size*
Tolerable rate increase (decrease)	Smaller (larger)
Risk of assessing control risk too low increase (decrease)	Smaller (larger)
Expected population deviation rate increase (decrease)	Larger (smaller)
Population size	Virtually no effect

A.9 Neither SAS No. 39, *Audit Sampling* (AICPA, *Professional Standards*, vol. 1, AU sec. 350), nor this guide requires the auditor to compare the sample size for a nonstatistical sampling application with a corresponding sample size calculated using statistical theory. However, in applying professional judgment to determine an appropriate nonstatistical sample size for test of controls, an auditor might find it helpful to be familiar with the tables in this appendix. The auditor using these tables as an aid in understanding relative sample sizes for tests of controls will need to apply professional judgment in reviewing the risk levels and expected population deviation rates in relation to sample sizes. For example, an auditor designing a nonstatistical sampling application to test compliance with a prescribed control procedure might have assessed the tolerable rate as 8 percent. If the auditor were to consider selecting a sample size of sixty, these tables would imply that at approximately a 5 percent risk level the auditor expected no more than approximately 1.5 percent of the items in the population to be deviations from the prescribed control procedure. These tables also would imply that at approximately a 10 percent risk level the auditor expected no more than approximately 3 percent of the items in the population to be deviations.

Table A.1 Statistical Sample Sizes for Test of Controls—5 Percent Risk of Assessing Control Risk Too Low (with number of expected errors in parentheses)

Expected Population Deviation Rate	*Tolerable Rate*										
	2%	*3%*	*4%*	*5%*	*6%*	*7%*	*8%*	*9%*	*10%*	*15%*	*20%*
0.00%	149(0)	99(0)	74(0)	59(0)	49(0)	42(0)	36(0)	32(0)	29(0)	19(0)	14(0)
.25	236(1)	157(1)	117(1)	93(1)	78(1)	66(1)	58(1)	51(1)	46(1)	30(1)	22(1)
.50	*	157(1)	117(1)	93(1)	78(1)	66(1)	58(1)	51(1)	46(1)	30(1)	22(1)
.75	*	208(2)	117(1)	93(1)	78(1)	66(1)	58(1)	51(1)	46(1)	30(1)	22(1)
1.00	*	*	156(2)	93(1)	78(1)	66(1)	58(1)	51(1)	46(1)	30(1)	22(1)
1.25	*	*	156(2)	124(2)	78(1)	66(1)	58(1)	51(1)	46(1)	30(1)	22(1)
1.50	*	*	192(3)	124(2)	103(2)	66(1)	58(1)	51(1)	46(1)	30(1)	22(1)
1.75	*	*	227(4)	153(3)	103(2)	88(2)	77(2)	51(1)	46(1)	30(1)	22(1)
2.00	*	*	*	181(4)	127(3)	88(2)	77(2)	68(2)	46(1)	30(1)	22(1)
2.25	*	*	*	208(5)	127(3)	88(2)	77(2)	68(2)	61(2)	30(1)	22(1)
2.50	*	*	*	*	150(4)	109(3)	77(2)	68(2)	61(2)	30(1)	22(1)
2.75	*	*	*	*	173(5)	109(3)	95(3)	68(2)	61(2)	30(1)	22(1)
3.00	*	*	*	*	195(6)	129(4)	95(3)	84(3)	61(2)	30(1)	22(1)
3.25	*	*	*	*	*	148(5)	112(4)	84(3)	61(2)	30(1)	22(1)
3.50	*	*	*	*	*	167(6)	112(4)	84(3)	76(3)	40(2)	22(1)
3.75	*	*	*	*	*	185(7)	129(5)	100(4)	76(3)	40(2)	22(1)
4.00	*	*	*	*	*	*	146(6)	100(4)	89(4)	40(2)	22(1)
5.00	*	*	*	*	*	*	*	158(8)	116(6)	40(2)	30(2)
6.00	*	*	*	*	*	*	*	*	179(11)	50(3)	30(2)
7.00	*	*	*	*	*	*	*	*	*	68(5)	37(3)

* Sample size is too large to be cost-effective for most audit applications.

Note: This table assumes a large population. For discussion of the effect of population size on sample size, see chapter 3.

Table A.2 Statistical Sample Sizes for Test of Controls—10 Percent Risk of Assessing Control Risk Too Low (with number of expected errors in parentheses)

Expected Population Deviation Rate	*Tolerable Rate*										
	2%	*3%*	*4%*	*5%*	*6%*	*7%*	*8%*	*9%*	*10%*	*15%*	*20%*
0.00%	114(0)	76(0)	57(0)	45(0)	38(0)	32(0)	28(0)	25(0)	22(0)	15(0)	11(0)
.25	194(1)	129(1)	96(1)	77(1)	64(1)	55(1)	48(1)	42(1)	38(1)	25(1)	18(1)
.50	194(1)	129(1)	96(1)	77(1)	64(1)	55(1)	48(1)	42(1)	38(1)	25(1)	18(1)
.75	265(2)	129(1)	96(1)	77(1)	64(1)	55(1)	48(1)	42(1)	38(1)	25(1)	18(1)
1.00	*	176(2)	96(1)	77(1)	64(1)	55(1)	48(1)	42(1)	38(1)	25(1)	18(1)
1.25	*	221(3)	132(2)	77(1)	64(1)	55(1)	48(1)	42(1)	38(1)	25(1)	18(1)
1.50	*	*	132(2)	105(2)	64(1)	55(1)	48(1)	42(1)	38(1)	25(1)	18(1)
1.75	*	*	166(3)	105(2)	88(2)	55(1)	48(1)	42(1)	38(1)	25(1)	18(1)
2.00	*	*	198(4)	132(3)	88(2)	75(2)	48(1)	42(1)	38(1)	25(1)	18(1)
2.25	*	*	*	132(3)	88(2)	75(2)	65(2)	42(1)	38(2)	25(1)	18(1)
2.50	*	*	*	158(4)	110(3)	75(2)	65(2)	58(2)	38(2)	25(1)	18(1)
2.75	*	*	*	209(6)	132(4)	94(3)	65(2)	58(2)	52(2)	25(1)	18(1)
3.00	*	*	*	*	132(4)	94(3)	65(2)	58(2)	52(2)	25(1)	18(1)
3.25	*	*	*	*	153(5)	113(4)	82(3)	58(2)	52(2)	25(1)	18(1)
3.50	*	*	*	*	194(7)	113(4)	82(3)	73(3)	52(2)	25(1)	18(1)
3.75	*	*	*	*	*	131(5)	98(4)	73(3)	52(2)	25(1)	18(1)
4.00	*	*	*	*	*	19(6)	98(4)	73(3)	65(3)	25(1)	18(1)
5.00	*	*	*	*	*	*	160(8)	115(6)	78(4)	34(2)	18(1)
6.00	*	*	*	*	*	*	*	182(11)	116(7)	43(3)	25(2)
7.00	*	*	*	*	*	*	*	*	199(14)	52(4)	25(2)

* Sample size is too large to be cost-effective for most audit applications.

Note: This table assumes a large population. For discussion of the effect of population size on sample size, see chapter 3.

Table A.3 Statistical Sampling Results Evaluation Table for Tests of Controls—Upper Limits at 5 Percent Risk of Assessing Control Risk Too Low

Sample Size	*Actual Number of Deviations Found*										
	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
25	11.3	17.6	*	*	*	*	*	*	*	*	*
30	9.5	14.9	19.6	*	*	*	*	*	*	*	*
35	8.3	12.9	17.0	*	*	*	*	*	*	*	*
40	7.3	11.4	15.0	18.3	*	*	*	*	*	*	*
45	6.5	10.2	13.4	16.4	19.2	*	*	*	*	*	*
50	5.9	9.2	12.1	14.8	17.4	19.9	*	*	*	*	*
55	5.4	8.4	11.1	13.5	15.9	18.2	*	*	*	*	*
60	4.9	7.7	10.2	12.5	14.7	16.8	18.8	*	*	*	*
65	4.6	7.1	9.4	11.5	13.6	15.5	17.4	19.3	*	*	*
70	4.2	6.6	8.8	10.8	12.6	14.5	16.3	18.0	19.7	*	*
75	4.0	6.2	8.2	10.1	11.8	13.6	15.2	16.9	18.5	20.0	*
80	3.7	5.8	7.7	9.5	11.1	12.7	14.3	15.9	17.4	18.9	*
90	3.3	5.2	6.9	8.4	9.9	11.4	12.8	14.2	15.5	16.8	18.2
100	3.0	4.7	6.2	7.6	9.0	10.3	11.5	12.8	14.0	15.2	16.4
125	2.4	3.8	5.0	6.1	7.2	8.3	9.3	10.3	11.3	12.3	13.2
150	2.0	3.2	4.2	5.1	6.0	6.9	7.8	8.6	9.5	10.3	11.1
200	1.5	2.4	3.2	3.9	4.6	5.2	5.9	6.5	7.2	7.8	8.4

* Over 20 percent

Note: This table presents upper limits as percentages. This table assumes a large population.

Table A.4 Statistical Sampling Results Evaluation Table for Tests of Controls—Upper Limits at 10 Percent Risk of Assessing Control Risk Too Low

Sample	*Actual Number of Deviations Found*										
Size	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
20	10.9	18.1	*	*	*	*	*	*	*	*	*
25	8.8	14.7	19.9	*	*	*	*	*	*	*	*
30	7.4	12.4	16.8	*	*	*	*	*	*	*	*
35	6.4	10.7	14.5	18.1	*	*	*	*	*	*	*
40	5.6	9.4	12.8	16.0	19.0	*	*	*	*	*	*
45	5.0	8.4	11.4	14.3	17.0	19.7	*	*	*	*	*
50	4.6	7.6	10.3	12.9	15.4	17.8	*	*	*	*	*
55	4.1	6.9	9.4	11.8	14.1	16.3	18.4	*	*	*	*
60	3.8	6.4	8.7	10.8	12.9	15.0	16.9	18.9	*	*	*
70	3.3	5.5	7.5	9.3	11.1	12.9	14.6	16.3	17.9	19.6	*
80	2.9	4.8	6.6	8.2	9.8	11.3	12.8	14.3	15.8	17.2	18.6
90	2.6	4.3	5.9	7.3	8.7	10.1	11.5	12.8	14.1	15.4	16.6
100	2.3	3.9	5.3	6.6	7.9	9.1	10.3	11.5	12.7	13.9	15.0
120	2.0	3.3	4.4	5.5	6.6	7.6	8.7	9.7	10.7	11.6	12.6
160	1.5	2.5	3.3	4.2	5.0	5.8	6.5	7.3	8.0	8.8	9.5
200	1.2	2.0	2.7	3.4	4.0	4.6	5.3	5.9	6.5	7.1	7.6

* Over 20 percent

Note: This table presents upper limits as percentages. This table assumes a large population.

APPENDIX F: EXAMPLES OF EXTENT-OF-TESTING DECISIONS

This appendix reproduces Appendix B, paragraphs B30 and B31 (including Examples B-1 through B-4), of Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, PC sec. 140). The material provides examples of how to determine the extent of testing required to form a conclusion about internal control effectiveness. The material applies directly to auditors, not to company management, and it directly addresses auditors only. However, this material may also be helpful to management in applying the guidance in PCAOB Auditing Standard No. 2 that directly affects the planning and performance of the company's self-assessment of internal control effectiveness.

B30. As discussed throughout this standard, determining the effectiveness of a company's internal control over financial reporting includes evaluating the design and operating effectiveness of controls over all relevant assertions related to all significant accounts and disclosures in the financial statements. Paragraphs 88 through 107 provide the auditor with directions about the nature, timing, and extent of testing of the design and operating effectiveness of internal control over financial reporting.

B31. Examples B-1 through B-4 illustrate how to apply this information in various situations. These examples are for illustrative purposes only.

Example B-1—Daily Programmed Application Control and Daily Information Technology-Dependent Manual Control

The auditor has determined that cash and accounts receivable are significant accounts to the audit of XYZ Company's internal control over financial reporting. Based on discussions with company personnel and review of company documentation, the auditor learned that the company had the following procedures in place to account for cash received in the lockbox:

a. The company receives a download of cash receipts from the banks.
b. The information technology system applies cash received in the lockbox to individual customer accounts.
c. Any cash received in the lockbox and not applied to a customer's account is listed on an exception report (Unapplied Cash Exception Report).
    - Therefore, the application of cash to a customer's account is a programmed application control, while the review and follow-up of unapplied cash from the exception report is a manual control.

To determine whether misstatements in cash (existence assertion) and accounts receivable (existence, valuation, and completeness) would be prevented or detected on a timely basis, the auditor decided to test the controls provided by the system in the daily reconciliation of lock box receipts to customer accounts, as well as the control over reviewing and resolving unapplied cash in the Unapplied Cash Exception Report.

Nature, Timing, and Extent of Procedures. To test the programmed application control, the auditor:

- Identified, through discussion with company personnel, the software used to receive the download from the banks and to process the transactions and determined that the banks supply the download software.
  - — The company uses accounting software acquired from a third-party supplier. The software consists of a number of modules. The client modifies the software only for upgrades supplied by the supplier.
- Determined, through further discussion with company personnel, that the cash module operates the lockbox functionality and the posting of cash to the general ledger. The accounts receivable module posts the cash to individual customer accounts and produces the Unapplied Cash Exception Report, a standard report supplied with the package. The auditor agreed this information to the supplier's documentation.
- Identified, through discussions with company personnel and review of the supplier's documentation, the names, file sizes (in bytes), and locations of the executable files (programs) that operate the functionality under review. The auditor then identified the compilation dates of these programs and agreed them to the original installation date of the application.
- Identified the objectives of the programs to be tested. The auditor wanted to determine whether only appropriate cash items are posted to customers' accounts and matched to customer number, invoice number, amount, etc., and that there is a listing of inappropriate cash items (that is, any of the above items not matching) on the exception report.

In addition, the auditor had evaluated and tested general computer controls, including program changes (for example, confirmation that no unauthorized changes are undertaken) and logical access (for example, data file access to the file downloaded from the banks and user access to the cash and accounts receivable modules) and concluded that they were operating effectively.

To determine whether such programmed controls were operating effectively, the auditor performed a walkthrough in the month of July. The computer controls operate in a systematic manner, therefore, the auditor concluded that it was sufficient to perform a walkthrough for only the one item. During the walkthrough, the auditor performed and documented the following items:

a. Selected one customer and agreed the amount billed to the customer to the cash received in the lockbox.
b. Agreed the total of the lockbox report to the posting of cash receipts in the general ledger.
c. Agreed the total of the cash receipt download from the bank to the lockbox report and supporting documentation.
d. Selected one customer's remittance and agreed amount posted to the customer's account in the accounts receivable subsidiary ledger.

To test the detective control of review and follow up on the Daily Unapplied Cash Exception Report, the auditor:

a. Made inquiries of company personnel. To understand the procedures in place to ensure that all unapplied items are resolved, the time frame in which such resolution takes place,

and whether unapplied items are handled properly within the system, the auditor discussed these matters with the employee responsible for reviewing and resolving the Daily Unapplied Cash Exception Reports. The auditor learned that, when items appear on the Daily Unapplied Cash Exception Report, the employee must manually enter the correction into the system. The employee typically performs the resolution procedures the next business day. Items that typically appear on the Daily Unapplied Cash Exception Report relate to payments made by a customer without reference to an invoice number/purchase order number or to underpayments of an invoice due to quantity or pricing discrepancies.

b. Observed personnel performing the control. The auditor then observed the employee reviewing and resolving a Daily Unapplied Cash Exception Report. The day selected contained four exceptions—three related to payments made by a customer without an invoice number, and one related to an underpayment due to a pricing discrepancy.
   - For the pricing discrepancy, the employee determined, through discussions with a sales person, that the customer had been billed an incorrect price; a price break that the sales person had granted to the customer was not reflected on the customer's invoice. The employee resolved the pricing discrepancy, determined which invoices were being paid, and entered a correction into the system to properly apply cash to the customer's account and reduce accounts receivable and sales accounts for the amount of the price break.

c. Reperformed the control. Finally, the auditor selected 25 Daily Unapplied Cash Exception Reports from the period January to September. For the reports selected, the auditor reperformed the follow-up procedures that the employee performed. For instance, the auditor inspected the documents and sources of information used in the follow-up and determined that the transaction was properly corrected in the system. The auditor also scanned other Daily Unapplied Cash Exception Reports to determine that the control was performed throughout the period of intended reliance.

Because the tests of controls were performed at an interim date, the auditor had to determine whether there were any significant changes in the controls from interim to year-end. Therefore, the auditor asked company personnel about the procedures in place at year-end. Such procedures had not changed from the interim period, therefore, the auditor observed that the controls were still in place by scanning Daily Unapplied Cash Exception Reports to determine the control was performed on a timely basis during the period from September to year-end.

Based on the auditor's procedures, the auditor concluded that the employee was clearing exceptions in a timely manner and that the control was operating effectively as of year-end.

Example B-2—Monthly Manual Reconciliation

The auditor determined that accounts receivable is a significant account to the audit of XYZ Company's internal control over financial reporting. Through discussions with company personnel and review of company documentation, the auditor learned that company personnel reconcile the accounts receivable subsidiary ledger to the general ledger on a monthly basis. To determine whether misstatements in accounts receivable (existence, valuation, and completeness) would be detected on a timely basis, the auditor decided to test the control provided by the monthly reconciliation process.

Nature, Timing, and Extent of Procedures. The auditor tested the company's reconciliation control by selecting a sample of reconciliations based upon the number of accounts, the dollar value of the accounts, and the volume of transactions affecting the account. Because the auditor considered all other receivable accounts immaterial, and because such accounts had only minimal transactions flowing through them, the auditor decided to test only the reconciliation for the trade accounts receivable account. The auditor elected to perform the tests of controls over the reconciliation process in conjunction with the auditor's substantive procedures over the accounts receivable confirmation procedures, which were performed in July.

To test the reconciliation process, the auditor:

a. Made inquiries of personnel performing the control. The auditor asked the employee performing the reconciliation a number of questions, including the following:
   - What documentation describes the account reconciliation process?
   - How long have you been performing the reconciliation work?
   - What is the reconciliation process for resolving reconciling items?
   - How often are the reconciliations formally reviewed and signed off?
   - If significant issues or reconciliation problems are noticed, to whose attention do you bring them?
   - On average, how many reconciling items are there?
   - How are old reconciling items treated?
   - If need be, how is the system corrected for reconciling items?
   - What is the general nature of these reconciling items?
b. Observed the employee performing the control. The auditor observed the employee performing the reconciliation procedures. For nonrecurring reconciling items, the auditor observed whether each item included a clear explanation as to its nature, the action that had been taken to resolve it, and whether it had been resolved on a timely basis.
c. Reperformed the control. Finally, the auditor inspected the reconciliations and reperfomed the reconciliation procedures. For the May and July reconciliations, the auditor traced the reconciling amounts to the source documents on a test basis. The only reconciling item that appeared on these reconciliations was cash received in the lockbox the previous day that had not been applied yet to the customer's account. The auditor pursued the items in each month's reconciliation to determine that the reconciling item cleared the following business day. The auditor also scanned through the file of all reconciliations prepared during the year and noted that they had been performed on a timely basis. To determine that the company had not made significant changes in its reconciliation control procedures from interim to year-end, the auditor made inquiries of company personnel and determined that such procedures had not changed from interim to year-end. Therefore, the auditor verified that controls were still in place by scanning the monthly account reconciliations to determine that the control was performed on a timely basis during the interim to year-end period.

Based on the auditor's procedures, the auditor concluded that the reconciliation control was operating effectively as of year-end.

Example B-3—Daily Manual Preventive Control

The auditor determined that cash and accounts payable were significant accounts to the audit of the company's internal control over financial reporting. Through discussions with company personnel, the auditor learned that company personnel make a cash disbursement only after they have matched the vendor invoice to the receiver and purchase order. To determine whether misstatements in cash (existence) and accounts payable (existence, valuation, and completeness) would be prevented on a timely basis, the auditor tested the control over making a cash disbursement only after matching the invoice with the receiver and purchase.

Nature, Timing, and Extent of Procedures. On a haphazard basis, the auditor selected 25 disbursements from the cash disbursement registers from January through September. In this example, the auditor deemed a test of 25 cash disbursement transactions an appropriate sample size because the auditor was testing a manual control performed as part of the routine processing of cash disbursement transactions through the system. Furthermore, the auditor expected no errors based on the results of company-level tests performed earlier. [If, however, the auditor had encountered a control exception, the auditor would have attempted to identify the root cause of the exception and tested an additional number of items. If another control exception had been noted, the auditor would have decided that this control was not effective. As a result, the auditor would have decided to increase the extent of substantive procedures to be performed in connection with the financial statement audit of the cash and accounts payable accounts.]

a. After obtaining the related voucher package, the auditor examined the invoice to see if it included the signature or initials of the accounts payable clerk, evidencing the clerk's performance of the matching control. However, a signature on a voucher package to indicate signor approval does not necessarily mean that the person carefully reviewed it before signing. The voucher package may have been signed based on only a cursory review, or without any review.
b. The auditor decided that the quality of the evidence regarding the effective operation of the control evidenced by a signature or initials was not sufficiently persuasive to ensure that the control operated effectively during the test period. In order to obtain additional evidence, the auditor reperformed the matching control corresponding to the signature, which included examining the invoice to determine that (a) its items matched to the receiver and purchase order and (b) it was mathematically accurate.

Because the auditor performed the tests of controls at an interim date, the auditor updated the testing through the end of the year (initial tests are through September to December) by asking the accounts payable clerk whether the control was still in place and operating effectively. The auditor confirmed that understanding by performing a walkthrough of one transaction in December.

Based on the auditor's procedures, the auditor concluded that the control over making a cash disbursement only after matching the invoice with the receiver and purchase was operating effectively as of year-end.

Example B-4—Programmed Prevent Control and Weekly Information Technology-Dependent Manual Detective Control

The auditor determined that cash, accounts payable, and inventory were significant accounts to the audit of the company's internal control over financial reporting. Through discussions

with company personnel, the auditor learned that the company's computer system performs a three-way match of the receiver, purchase order, and invoice. If there are any exceptions, the system produces a list of unmatched items that employees review and follow up on weekly.

In this case, the computer match is a programmed application control, and the review and follow-up of the unmatched items report is a detective control. To determine whether misstatements in cash (existence) and accounts payable/inventory (existence, valuation, and completeness) would be prevented or detected on a timely basis, the auditor decided to test the programmed application control of matching the receiver, purchase order, and invoice as well as the review and follow-up control over unmatched items.

Nature, Timing, and Extent of Procedures. To test the programmed application control, the auditor:

a. Identified, through discussion with company personnel, the software used to process receipts and purchase invoices. The software used was a third-party package consisting of a number of modules.

b. Determined, through further discussion with company personnel, that they do not modify the core functionality of the software, but sometimes make personalized changes to reports to meet the changing needs of the business. From previous experience with the company's information technology environment, the auditor believes that such changes are infrequent and that information technology process controls are well established.

c. Established, through further discussion, that the inventory module operated the receiving functionality, including the matching of receipts to open purchase orders. Purchase invoices were processed in the accounts payable module, which matched them to an approved purchase order against which a valid receipt has been made. That module also produced the Unmatched Items Report, a standard report supplied with the package to which the company has not made any modifications. That information was agreed to the supplier's documentation and to documentation within the information technology department.

d. Identified, through discussions with the client and review of the supplier's documentation, the names, file sizes (in bytes), and locations of the executable files (programs) that operate the functionality under review. The auditor then identified the compilation dates of the programs and agreed them to the original installation date of the application. The compilation date of the report code was agreed to documentation held within the information technology department relating to the last change made to that report (a change in formatting).

e. Identified the objectives of the programs to be tested. The auditor wanted to determine whether appropriate items are received (for example, match a valid purchase order), appropriate purchase invoices are posted (for example, match a valid receipt and purchase order, non-duplicate reference numbers) and unmatched items (for example, receipts, orders or invoices) are listed on the exception report. The auditor then reperformed all those variations in the packages on a test-of-one basis to determine that the programs operated as described.

In addition, the auditor had evaluated and tested general computer controls, including program changes (for example, confirmation that no unauthorized changes are undertaken to the functionality and that changes to reports are appropriately authorized, tested, and approved before being applied) and logical access (for example, user access to the inventory

and accounts payable modules and access to the area on the system where report code is maintained), and concluded that they were operating effectively. (Since the computer is deemed to operate in a systematic manner, the auditor concluded that it was sufficient to perform a walkthrough for only the one item.)

To determine whether the programmed control was operating effectively, the auditor performed a walkthrough in the month of July. As a result of the walkthrough, the auditor performed and documented the following items:

a. Receiving cannot record the receipt of goods without matching the receipt to a purchase order on the system. The auditor tested that control by attempting to record the receipt of goods into the system without a purchase order. However, the system did not allow the auditor to do that. Rather, the system produced an error message stating that the goods could not be recorded as received without an active purchase order.

b. An invoice will not be paid unless the system can match the receipt and vendor invoice to an approved purchase order. The auditor tested that control by attempting to approve an invoice for payment in the system. The system did not allow the auditor to do that. Rather, it produced an error message indicating that invoices could not be paid without an active purchase order and receiver.

c. The system disallows the processing of invoices with identical vendor and identical invoice numbers. In addition, the system will not allow two invoices to be processed against the same purchase order unless the sum of the invoices is less than the amount approved on the purchase order. The auditor tested that control by attempting to process duplicate invoices. However, the system produced an error message indicating that the invoice had already been processed.

d. The system compares the invoice amounts to the purchase order. If there are differences in quantity/extended price, and such differences fall outside a preapproved tolerance, the system does not allow the invoice to be processed. The auditor tested that control by attempting to process an invoice that had quantity/price differences outside the tolerance level of 10 pieces, or $1,000. The system produced an error message indicating that the invoice could not be processed because of such differences.

e. The system processes payments only for vendors established in the vendor master file. The auditor tested that control by attempting to process an invoice for a vendor that was not established in the vendor master file. However, the system did not allow the payment to be processed.

f. The auditor tested user access to the vendor file and whether such users can make modifications to such file by attempting to access and make changes to the vendor tables. However, the system did not allow the auditor to perform that function and produced an error message stating that the user was not authorized to perform that function.

g. The auditor verified the completeness and accuracy of the Unmatched Items Report by verifying that one unmatched item was on the report and one matched item was not on the report.

   Note: It is inadvisable for the auditor to have uncontrolled access to the company's systems in his or her attempts described above to record the receipt of goods without a purchase order, approve an invoice for payment, process duplicate invoices, etc. These procedures ordinarily are performed in the presence of appropriate company personnel so that they can be notified immediately of any breach to their systems.

To test the detect control of review and follow up on the Unmatched Items Report, the auditor performed the following procedures in the month of July for the period January to July:

a. Made inquiries of company personnel. To gain an understanding of the procedures in place to ensure that all unmatched items are followed-up properly and that corrections are made on a timely basis, the auditor made inquiries of the employee who follows up on the weekly-unmatched items reports. On a weekly basis, the control required the employee to review the Unmatched Items Report to determine why items appear on it. The employee's review includes proper followup on items, including determining whether:
   - All open purchase orders are either closed or voided within an acceptable amount of time.
   - The requesting party is notified periodically of the status of the purchase order and the reason for its current status.
   - The reason the purchase order remains open is due to incomplete shipment of goods and, if so, whether the vendor has been notified.
   - There are quantity problems that should be discussed with purchasing.
b. Observed the performance of the control. The auditor observed the employee performing the control for the Unmatched Items Reports generated during the first week in July.
c. Reperformed the control. The auditor selected five weekly Unmatched Items Reports, selected several items from each, and reperformed the procedures that the employee performed. The auditor also scanned other Unmatched Items Reports to determine that the control was performed throughout the period of intended reliance.

To determine that the company had not made significant changes in their controls from interim to year-end, the auditor discussed with company personnel the procedures in place for making such changes. Since the procedures had not changed from interim to year-end, the auditor observed that the controls were still in place by scanning the weekly Unmatched Items Reports to determine that the control was performed on a timely basis during the interim to year-end period.

Based on the auditor's procedures, the auditor concluded that the employee was clearing exceptions in a timely manner and that the control was operating effectively as of year-end.

APPENDIX G: EXAMPLES OF SIGNIFICANT DEFICIENCIES AND MATERIAL WEAKNESSES

Understanding the definitions of significant deficiencies and material weaknesses is critical, not only to evaluate the magnitude of control deficiencies, but also for planning the assessment of internal control. This appendix reproduces Appendix D of Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, PC sec. 140). It provides examples of how to apply the guidance discussed in Chapter 5 of this Practice Aid. The material applies directly to auditors, not to company management, and it directly addresses auditors only. However, this material may also be helpful to management in applying the guidance in PCAOB Auditing Standard No. 2 that directly affects the planning and performance of the company's self-assessment of internal control effectiveness.

D1. Paragraph 8 of this standard defines a control deficiency. Paragraphs 9 and 10 go on to define a significant deficiency and a material weakness, respectively.

- Paragraphs 22 through 23 of this standard discuss materiality in an audit of internal control over financial reporting, and paragraphs 130 through 140 provide additional direction on evaluating deficiencies in internal control over financial reporting.
- The following examples illustrate how to evaluate the significance of internal control deficiencies in various situations. These examples are for illustrative purposes only.

Example D-1—Reconciliations of Intercompany Accounts Are Not Performed on a Timely Basis

Scenario A—Significant Deficiency.

The company processes a significant number of routine intercompany transactions on a monthly basis. Individual intercompany transactions are not material and primarily relate to balance sheet activity, for example, cash transfers between business units to finance normal operations.

A formal management policy requires monthly reconciliation of intercompany accounts and confirmation of balances between business units. However, there is not a process in place to ensure performance of these procedures. As a result, detailed reconciliations of intercompany accounts are not performed on a timely basis. Management does perform monthly procedures to investigate selected large-dollar intercompany account differences. In addition, management prepares a detailed monthly variance analysis of operating expenses to assess their reasonableness.

Based only on these facts, the auditor should determine that this deficiency represents a significant deficiency for the following reasons: The magnitude of a financial statement misstatement resulting from this deficiency would reasonably be expected to be more than inconsequential, but less than material, because individual intercompany transactions are not material, and the compensating controls operating monthly should detect a material mis-

statement. Furthermore, the transactions are primarily restricted to balance sheet accounts. However, the compensating detective controls are designed only to detect material misstatements. The controls do not address the detection of misstatements that are more than inconsequential but less than material. Therefore, the likelihood that a misstatement that was more than inconsequential, but less than material, could occur is more than remote.

Scenario B—Material Weakness

The company processes a significant number of intercompany transactions on a monthly basis. Intercompany transactions relate to a wide range of activities, including transfers of inventory with intercompany profit between business units, allocation of research and development costs to business units and corporate charges. Individual intercompany transactions are frequently material.

A formal management policy requires monthly reconciliation of intercompany accounts and confirmation of balances between business units. However, there is not a process in place to ensure that these procedures are performed on a consistent basis. As a result, reconciliations of intercompany accounts are not performed on a timely basis, and differences in intercompany accounts are frequent and significant. Management does not perform any alternative controls to investigate significant intercompany account differences.

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

Example D-2—Modifications to Standard Sales Contract Terms Not Reviewed To Evaluate Impact on Timing and Amount of Revenue Recognition

Scenario A—Significant Deficiency

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

Based only on these facts, the auditor should determine that this deficiency represents a significant deficiency for the following reasons: The magnitude of a financial statement misstatement resulting from this deficiency would reasonably be expected to be more than inconsequential, but less than material, because individual sales transactions are not material and the compensating detective controls operating monthly and at the end of each financial reporting period should reduce the likelihood of a material misstatement going undetected. Furthermore,

the risk of material misstatement is limited to revenue recognition errors related to shipping terms as opposed to broader sources of error in revenue recognition. However, the compensating detective controls are only designed to detect material misstatements. The controls do not effectively address the detection of misstatements that are more than inconsequential but less than material, as evidenced by situations in which transactions that were not material were improperly recorded. Therefore, there is a more than remote likelihood that a misstatement that is more than inconsequential but less than material could occur.

Scenario B—Material Weakness

The company has a standard sales contract, but sales personnel frequently modify the terms of the contract. The nature of the modifications can affect the timing and amount of revenue recognized. Individual sales transactions are frequently material to the entity, and the gross margin can vary significantly for each transaction.

The company does not have procedures in place for the accounting function to regularly review modifications to sales contract terms. Although management reviews gross margins on a monthly basis, the significant differences in gross margins on individual transactions make it difficult for management to identify potential misstatements. Improper revenue recognition has occurred, and the amounts have been material.

Based only on these facts, the auditor should determine that this deficiency represents a material weakness for the following reasons: The magnitude of a financial statement misstatement resulting from this deficiency would reasonably be expected to be material, because individual sales transactions are frequently material, and gross margin can vary significantly with each transaction (which would make compensating detective controls based on a reasonableness review ineffective). Additionally, improper revenue recognition has occurred, and the amounts have been material. Therefore, the likelihood of material misstatements occurring is more than remote. Taken together, the magnitude and likelihood of misstatement of the financial statements resulting from this internal control deficiency meet the definition of a material weakness.

Scenario C—Material Weakness

The company has a standard sales contract, but sales personnel frequently modify the terms of the contract. Sales personnel frequently grant unauthorized and unrecorded sales discounts to customers without the knowledge of the accounting department. These amounts are deducted by customers in paying their invoices and are recorded as outstanding balances on the accounts receivable aging. Although these amounts are individually insignificant, they are material in the aggregate and have occurred consistently over the past few years.

Based on only these facts, the auditor should determine that this deficiency represents a material weakness for the following reasons: The magnitude of a financial statement misstatement resulting from this deficiency would reasonably be expected to be material, because the frequency of occurrence allows insignificant amounts to become material in the aggregate. The likelihood of material misstatement of the financial statements resulting from this internal control deficiency is more than remote (even assuming that the amounts were fully reserved for in the company's allowance for uncollectible accounts) due to the likelihood of material misstatement of the gross accounts receivable balance. Therefore, this internal control deficiency meets the definition of a material weakness.

Example D-3—Identification of Several Deficiencies

Scenario A—Material Weakness

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

- Inadequate segregation of duties over certain information system access controls.
- Several instances of transactions that were not properly recorded in subsidiary ledgers; transactions were not material, either individually or in the aggregate.
- A lack of timely reconciliations of the account balances affected by the improperly recorded transactions.

Based only on these facts, the auditor should determine that the combination of these significant deficiencies represents a material weakness for the following reasons: Individually, these deficiencies were evaluated as representing a more than remote likelihood that a misstatement that is more than inconsequential, but less than material, could occur. However, each of these significant deficiencies affects the same set of accounts. Taken together, these significant deficiencies represent a more than remote likelihood that a material misstatement could occur and not be prevented or detected. Therefore, in combination, these significant deficiencies represent a material weakness.

Scenario B—Material Weakness

During its assessment of internal control over financial reporting, management of a financial institution identifies deficiencies in: the design of controls over the estimation of credit losses (a critical accounting estimate); the operating effectiveness of controls for initiating, processing, and reviewing adjustments to the allowance for credit losses; and the operating effectiveness of controls designed to prevent and detect the improper recognition of interest income. Management and the auditor agree that, in their overall context, each of these deficiencies individually represent a significant deficiency.

In addition, during the past year, the company experienced a significant level of growth in the loan balances that were subjected to the controls governing credit loss estimation and revenue recognition, and further growth is expected in the upcoming year.

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

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

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