Chapter 1

The Engagement Approach

Chapter Summary

Overview of the Securities and Exchange Commission (SEC) rules requiring
- Management's assessment of the effectiveness of the entity's internal control over financial reporting,
- Independent auditors' audit of management's report on internal control, and
- Management's required quarterly reporting on the effectiveness of the entity's disclosure controls and procedures

Summary of the relevant auditing standards relating to internal control.

Description of a structured approach for the evaluation of an entity's internal control.

Suggestions for outside consultants on structuring an engagement to assist management in evaluating the effectiveness of internal control and preparing for an independent auditor's audit of management's internal control report.

MANAGEMENT'S REQUIRED ASSESSMENT OF THE ENTITY'S INTERNAL CONTROL

The Sarbanes-Oxley Act of 2002 made significant changes to many aspects of the financial reporting process. One of those changes is a requirement that management provide a report, both quarterly and annually, on the effectiveness of certain aspects of the entity's internal control over financial reporting. This chapter summarizes these reporting requirements. Chapter 8 provides more detailed guidance and examples.

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

(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.

When considering the SEC's definition, you should note the following:

- 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 an entity's 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 their definition to be consistent with the definition of internal controls that pertain to financial reporting objectives that was provided in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Report. (See Chapter 2 for a detailed discussion of the COSO Report.)
- The rule makes explicit reference to the use or disposition of the entity's assets—that is, the safeguarding of assets.

This book, unless otherwise indicated, uses the term *internal control* to mean the same thing as "internal control over financial reporting," as defined by the SEC rules.

Annual Reporting

Section 404 of the Sarbanes-Oxley Act requires chief executive officers (CEOs) and chief financial officers (CFOs) to evaluate and report on the effectiveness of the entity's internal control over financial reporting. This report is contained in the company's Form 10K, which is filed annually with the SEC. The SEC has adopted rules for its registrants that effectively implement the requirements of the Sarbanes-Oxley Act, Section 404.

Under the SEC rules, the company's 10K 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) *Attestation Report of the Registered Public Accounting Firm*. Provide the registered public accounting firm's attestation 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.

The company's annual report filed with the SEC also should include management's fourth-quarter report on the effectiveness of the entity's disclosure controls and procedures, as described in the next section.[2]

Quarterly Reporting

Section 302 of the Sarbanes-Oxley Act requires quarterly reporting on the effectiveness of an entity's "disclosure controls and procedures." Item 307 of SEC Regulation S-K implements this requirement for the company's quarterly Form 10Q filings by requiring management to

> Disclose the conclusions of the company's principal executive and principal financial officers, or persons performing similar functions, regarding the effectiveness of the company's disclosure controls and procedures as of the end of the period covered by the report, based on the evaluation of these controls and procedures.

In addition to reporting on disclosure controls, the company's quarterly reports also must disclose material changes in the entity's internal control over financial reporting.

Note that for these quarterly filings

- Management is *not* required to evaluate or report on internal control over financial reporting. That evaluation is required on an *annual basis only*.

- The company's independent auditors are *not* required to attest to management's evaluation of disclosure controls.

Disclosure Controls and Procedures. With these rules, 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 those that are

> Designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits under the Act is
>
> - Recorded
> - Processed,
> - Summarized, and
> - Reported
>
> within the time periods specified in the Commission's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that *information required to be disclosed* by an issuer in the reports that it files or submits under the Act is *accumulated and communicated* to the issuer's management, including its principal executive and principal financial officers, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure.

Thus, "disclosure controls and procedures" would encompass the controls over all material financial and nonfinancial information in Exchange Act reports. Information that would fall under this definition that would *not* be part of an entity's internal control over financial reporting might include the signing of a significant contract, changes in a strategic relationship, management compensation, or legal proceedings. Chapter 2 of this book provides additional guidance on disclosure controls and procedures and the effect these might have on management's assessment of the effectiveness of internal control.

The Disclosure Committee. In relation to its rule requiring an assessment of 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, including the

- Review of 10Q, 10K, and other SEC filings; earnings releases; and other public information for the appropriateness of disclosure
- Determination of what constitutes a significant transaction or event that requires disclosure
- Determination and identification of significant deficiencies and material weaknesses in the design or operating effectiveness of disclosure controls and procedures

- Assessment of CEO and CFO awareness of material information that could affect disclosure

The existence and effective operation of an entity's disclosure committee can have a significant effect on the nature and scope of your work to evaluate the effectiveness of the entity's internal control. For example:

- The effective functioning of a disclosure committee may be viewed as an element that strengthens the entity's control environment.
- The work of the disclosure committee may create documentation that engagement teams can use to reduce the scope of their work.

Management Certifications

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 two certifications, which are included as exhibits to the entity's 10Q and 10K. These two certifications are required by the following sections of the Sarbanes-Oxley Act:

- Section 302, which requires a certification to accompany each quarterly and annual report filed with the SEC.
- Section 906, which added a new Section 1350 to Title 18 of the United States Code, and which contains a certification requirement subject to specific federal criminal provisions. This certification is separate and distinct from the Section 302 certification requirement.

Exhibit 1.1 provides the text of the Section 302 certification. This text is provided in SEC Rule 13a-14(a) and should be used exactly as set forth in the rule.

Exhibit 1.2 provides an example of the Section 906 certification. Note that some certifying officers may choose to include a "knowledge qualification," as indicated by the optional language in italics. Officers who choose to include this language should do so only after consulting with their SEC counsel. Unlike the Section 302 certification, which requires a separate certification for both the CEO and CFO, the company can provide only one 906 certification, which is then signed by both individuals.

Subcertification. A great deal of the information included in financial statements and other reports filed with the SEC 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, it is common for the CEO and CFO to 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 sign their certifications in good faith.

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.

Exhibit 1.2 Section 906 Certification, 18 U.S.C. Section 1350

In connection with the [annual/quarterly] report of [name of registrant] (the "Company") on Form (10K/10Q] for the period ended _____ (the "Report"), the undersigned in the capacities listed below, hereby certify, pursuant to 18 U.S.C. ss. 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that *to my knowledge*

(i) The Report fully complies with the requirements of Section 12(a) or 15(d) of the Securities Exchange Act of 1934; and

(ii) The information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of the Company.

Items that may be the subject of subcertification affidavits include:

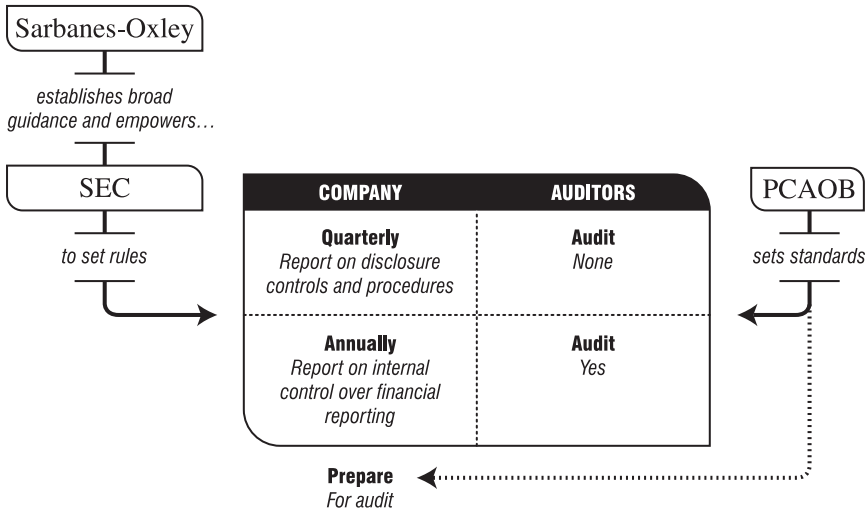
- Adequacy of specific disclosures in the financial statements or other reports filed with the SEC, such as *Management's Disclosure and Analysis* included in the entity's 10Q or 10K.
- Accuracy of specific account balances.
- Compliance with company policies and procedures, including the company's code 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.

THE INDEPENDENT AUDITOR'S REPORTING RESPONSIBILITIES

Exhibit 1.3 describes the relationship between the various rule-making bodies, companies, and their auditors regarding the reporting on internal control. As described previously, Sections 302 and 404 of the Sarbanes-Oxley Act require management of public companies to report on the effectiveness of the entity's internal control on an annual basis. The company's independent auditors are required to audit this report. The SEC is responsible for setting rules to implement the Sarbanes-Oxley Act requirements. Those rules include guidance for reporting by the CEO and CFO on the entity's internal control over financial reporting and disclosure controls, but they do not provide any guidance or set standards for the independent auditors. The Public Company Accounting Oversight Board (PCAOB) sets the auditing standards, which will have a direct effect on auditors and how they plan and perform their engagements.

In addition, the auditing standards will have an *indirect effect* on the company as it prepares for the audit of its internal control report. Just as in a financial statement audit, the company should be able to support its conclusions about internal control and provide documentation that is sufficient for the auditor to perform an

Exhibit 1.3 Relationship of the Rules, Regulations, and Standards



audit. Thus, in preparing for the audit of its internal control report, it is vital for management, and those who assist them, to have a good understanding of what the independent auditors will require.

The Auditing Standard

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*. 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.

AS No. 2 Affects Company Management. The Auditing Standard has 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 have released periodically 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 both 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. An important step in planning a SOX 404 compliance engagement is to make sure you have read the most current staff positions issued by the PCAOB and the SEC.

Overall Objective of the Auditor's Engagement

The auditor's objective in an audit of internal control is to express an opinion about management's assessment of the effectiveness of the company's internal control over financial reporting. This objective implies a two-step process:

1. Management must perform its own assessment and conclude on the effectiveness of the entity's internal controls.
2. The auditors will perform their own assessment and form an independent opinion as to whether management's assessment of the effectiveness of internal control is fairly stated.

Thus, internal control is assessed twice, first by management and then by the independent auditors. That the auditors will be auditing internal control—and in some cases, reperforming some of the tests performed by the entity—does not relieve management of its obligation to document, test and report on internal control.

To form his or her opinion, the auditor will:

- Evaluate the reliability of the process used by management to assess the entity's internal control
- Review and rely on the results of *some* of the tests performed by management, internal auditors, and others during their assessment process
- Perform his or her own tests

Evaluation of Management's Assessment Process

The 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, companies will commonly look to the Auditing Standard to help determine which business units or controls should be included in their assessment.

AS No. 2 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 and modify the "clean opinion" on internal control. As a practical matter, most companies take steps to ensure that their assessment process includes all the required elements listed in the auditing 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.
  - Anti-fraud 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).

- 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 reports (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 external auditor and to others, if applicable.
- Evaluating whether findings are reasonable and support management's assessment.

In reading these requirements note that the scope of management's assessment (as described in the first bullet point) 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
- Anti-fraud programs and controls
- The company's "tone at the top" and other elements of the control environment

Also consider that "inquiry alone is not adequate" to test operating effectiveness; that is, tests of controls should be robust and meaningful. The testing of controls is discussed in Chapters 6 and 7.

Documentation

The external auditors are required to 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.

Paragraph 42 of the standard provides the requirements for the 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.

Chapter 3 of this book provides additional guidance on the documentation of controls.

Use of Work of Internal Auditors and Others

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 participants 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: The company is *prohibited* in its self-assessment of internal control from relying on the work performed by the external auditors in their audit.

Keep in mind that the company is required to perform a thorough, detailed assessment of the company's 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.

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

Note that 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 anti-fraud programs and controls themselves.

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:

1. Evaluate the nature of the controls subjected to the work of others. In general, auditors will probably want to perform their own tests on the controls related to accounts that have a high risk of material misstatement. For the controls for less risky accounts they will be more inclined to rely on the work of the company.
2. Evaluate the competence and objectivity of the individuals who performed the work. The more competent and objective the company's project team, the more likely the external auditors will be to rely on their work.
3. Test some of the work performed by others to evaluate the quality and effectiveness of their work.

To allow the company's external auditors to make as much use as possible of the company's own assessment of internal control, company management should have a clear understanding of the conditions that must be met for the external auditor 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* of the auditing standard 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.

Determination of Material Weakness

The SEC reporting rules require entity management to disclose material weaknesses in internal control. Engagements to assess the effectiveness of internal control should be planned and performed in a way that will detect material misstatements. Thus, it is critical that you have a working definition of the term. PCAOB Auditing standard provides the following definitions:

- 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 *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: 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*.
- 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.

Chapter 8 provides additional guidance on determining the relative magnitude of internal control deficiencies.

Working with the Independent Auditors

To render an opinion on either the financial statements or the effectiveness of internal control, the company's independent auditors are required to maintain their

independence, in accordance with applicable SEC rules. These rules are guided by certain underlying principles, which include:

- The audit firm must not be in a position where it audits its own work.
- The auditor must not act as management or as an employee of the client.

The PCAOB Auditing Standard incorporates the SEC's principles in its auditing standard and then expands on these principles in important ways. Although maintaining independence is primarily the responsibility of the auditors, several of the independence requirements of AS No. 2 impose certain responsibilities on management and the audit committee. These requirements include:

- *Preapproval by the audit committee.* Each internal control-related service to be provided by the 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.
- *Active involvement of management.* Management must be "actively involved" in a "substantive and extensive" way in all internal control services the 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.

Determining How the Auditors May Assist Management. No matter how detailed the independence rules may become, they cannot possibly address every possible interaction between the company and its auditors. During the initial implementation of SOX 404 many situations arose that called into question whether the auditor could interact with the company in a particular way and still maintain its independence.

For example, if the company was unsure whether its documentation of internal control would be acceptable, could it approach its auditors for advice? If the auditors made recommendations on how to improve the documentation and the company then incorporated those recommendations, wouldn't that put the audit firm in the position of auditing its own work when it reviewed that documentation? The form and content of the company's documentation of its internal control is the responsibility of management. If the auditors become significantly involved in that decision, doesn't that imply that they are acting in the capacity of management?

In the initial implementation of SOX 404, it became common for auditors to provide as little advice as possible to their clients on internal control matters. Concerned about possibly violating the independence rules, they chose to largely remove themselves from their clients' efforts.

As a practical matter, both the SEC and the PCAOB understood that the public interest is not well-served if the independent auditors are completely uninvolved from the company's efforts to understand and assess its internal control. There must be some sharing of information between the company and its auditors, and the auditors must be able to provide help and advice on some matters.

In June 2004 the SEC and PCAOB issued some guidance in this area. Essentially that guidance allows the auditor to provide "limited assistance to management in documenting internal controls and making recommendations for changes to internal controls. However, management has the ultimate responsibility for the assessment, documentation and testing of the company's internal control."

The PCAOB provided more extensive guidance on how company management may solicit advice from and share advice with their auditors on internal control matters. The guidance from the staff was in answer to a question directed specifically to an auditor's review of the 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.

Thus, "some type of information-sharing on a timely basis between management and the auditor is necessary." However, when management seeks the assistance of the company's auditors to help with its internal control assessment, it should make it clear that management retains the ultimate responsibility for internal control. The PCAOB places the burden on management to clearly communicate with the auditors the nature of the advice they are seeking and the purpose for which the auditor is being involved.

The PCAOB Clarifies Its Guidance

As indicated previously, both the SEC and PCAOB periodically issue staff position papers to clarify how AS 2 applies in specific circumstances. On May 16, 2005, in response to information that was gathered about the first year of implementation, both the SEC and PCAOB issued guidance that addressed the most significant problems encountered with the implementation of AS 2. Of the five main areas addressed in the guidance, the following are the most relevant to company management.

- Use a risk-based, "top-down" approach. The PCAOB emphasized that auditors should use a "top-down" approach, and company management would be wise to use this same approach. In a top-down approach, you begin with an evaluation of entity-level controls and from there move to the testing of detailed activity-level controls.

  One of the key principles of the top-down approach is that the decision of which controls to document and test is based an assessment of risk. Controls that mitigate significant risks should be documented and assessed. Those that mitigate less significant risks would be subject to considerably less, if any testing and evaluation.

  The risk-based, top-down approach is described in more detail in the next section of this chapter.

- Auditors and company management should engage in direct and timely communication with each other. As described in the previous section of this chapter, during the first year of compliance, there was often a lack of communication between the two. With its May 16th guidance, the PCAOB makes it clear that auditors should be responsive to client requests for advice, provided that company management take final responsibility for internal control.
- Auditors should make as much use as possible of the work on internal control performed by the company. This guidance should help companies keep down the cost of compliance, but it also means that companies have to perform their assessment with qualified individuals in a way that is consistent with the requirements of AS 2.

A RISK-BASED, TOP-DOWN APPROACH FOR EVALUATING INTERNAL CONTROL

Principles of a Risk-Based, Top-Down Approach

As discussed in more detail in Chapter 2 of this book, controls operate at two levels within any organization. Entity-level controls are pervasive and can affect many different financial statement accounts. For example, a company's hiring and training policies will affect the way in which individual control procedures are performed. Companies that hire qualified people and train them properly will have much greater success when it comes time for those people to perform their jobs. The converse also is true. In that sense, hiring and training policies can have an effect on many different financial statement accounts.

Activity-level controls, on the other hand, are restricted to one transaction type. Controls over case disbursements will affect cash disbursements only and will have no impact on other accounts, such as the recording of goodwill or the depreciation of fixed assets.

In the year of implementation, many companies and their auditors adopted a bottom-up approach in which they started by identifying all of the companies' activity-level controls and then documenting and testing each of these to determine whether internal control as a whole was effective. As you can imagine, this approach was extremely time-consuming and costly. Moreover, not only is it not required, it is not even contemplated by AS 2.

The method described by the auditing standard is the exact opposite of this approach. In a top-down approach you begin at the top, at the entity-level. You then identify the most significant accounts and transaction types at the organization and the control objectives for those accounts and transactions. Once you determine the control objectives, you identify those controls that are in place to meet those objectives. Those controls, and only those controls, are then testetd and evaluated.

By using a top-down approach, the company

- Tests only those controls related to significant accounts and transactions, which eliminates the need to understand the process and assess controls in those areas

that do not affect the likelihood that the company's financial statements could be materially misstated.
- Tests the minimum number of controls necessary to meet the control objective. Redundant controls (and there are many of these) are not tested.

Implementing a top-down approach requires company management to exercise its judgment. How do you decide which accounts and transactions are "significant" and which are insignificant? If you are not going to test all the control activities for significant accounts and transactions, how do you determine which ones to test?

To make these and other decisions you should consider the related risk of material misstatement of the financial statements. As described in more detail in Chapter 2 of this book, control activities are designed to meet identified risks of misstatement. For example, one of the risks of misstatement is that the company may fail to record all of its accounts payable as of year-end. To mitigate this risk, management will design and implement procedures at the company to make sure that all payables get recorded.

Do these controls need to be documented and tested? It depends on the relative significance of the risk of failing to record all accounts payable. What is the likelihood that the failure to record all accounts payable would result in a material misstatement of the company's financial statements? The answer to this question will help you determine whether to document and test the controls over accounts payable.

Performing an assessment of internal control is not a "paint-by-numbers" exercise. It is a process that requires a great deal of judgment. The primary benchmark for making these judgments is risk, that is the risk that the financial statements would be materially misstated if the identified control was ineffective.

This book provides practical guidance for implementing a risk-based, top-down approach.

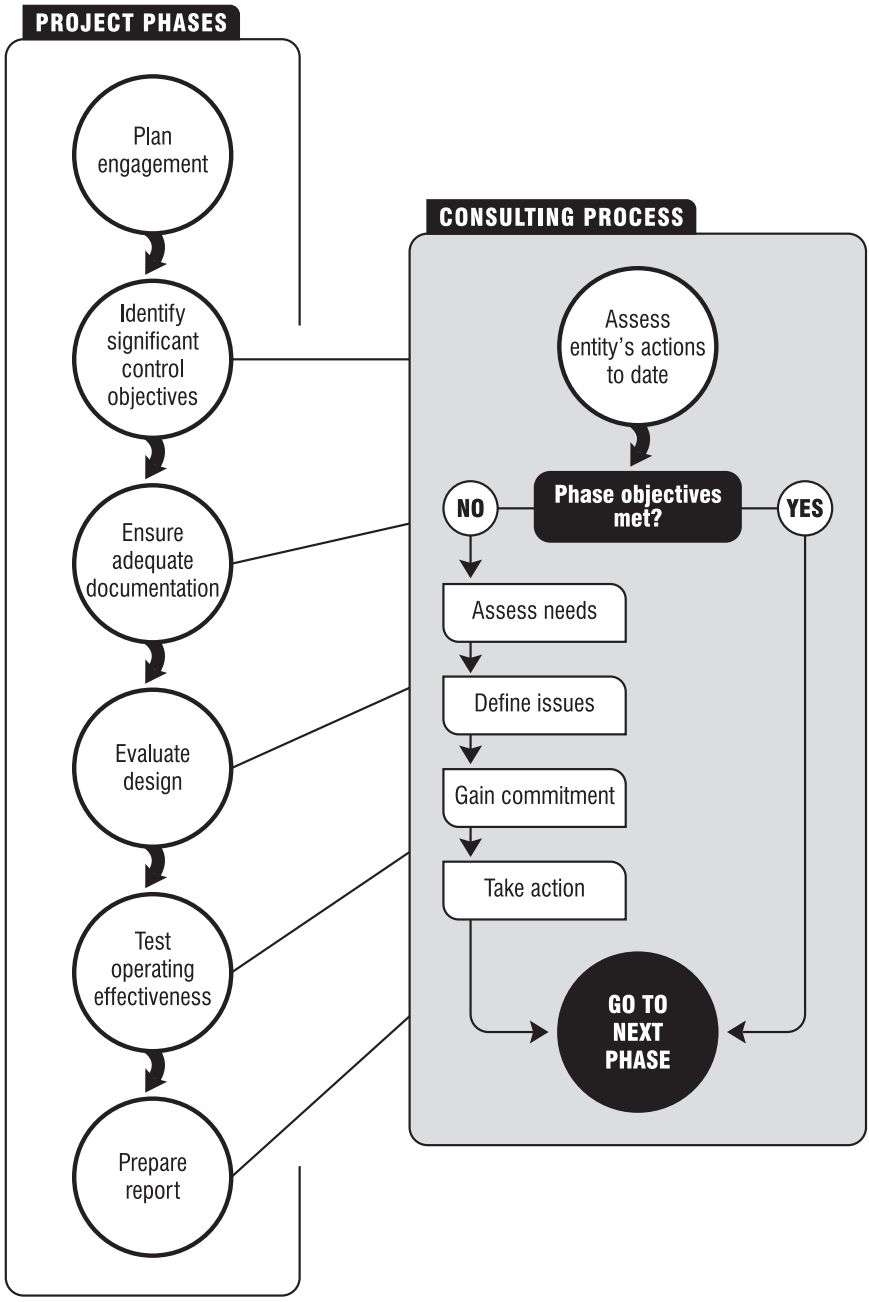
A Top-Down Approach

There is no one way to structure an engagement to achieve the above objectives. Exhibit 1.4 summarizes the approach followed in this book.

Distinct Phases and Their Objectives. The left-hand side of Exhibit 1.4 describes *what* should be done to issue and support management's report about the effectiveness of the entity's internal controls. The diagram depicts six sequential steps, which start with planning and end with reporting. The objective of each of these steps is as follows:

- *Engagement planning*. The primary objectives of the engagement planning phase are to
  - Assess information needs and identify sources of information required to effectively perform the assessment of internal control.

Exhibit 1.4 Process for Evaluating Effectiveness of Internal Control



  - Determine the overall scope of the engagement.
  - Establish the terms of the working relationship both within the project team and between the project team and the project owner.
  - Coordinate the efforts with the independent auditors.

- *Assess internal control effectiveness*. This phase represents the bulk of the engagement and can be broken down into four separate components.

  1. *Identify significant controls*.[3] Management's assessment is based on the effectiveness of internal control *taken as a whole*, not on the effectiveness of individual components of control or individual controls. This holistic approach to assessing effectiveness recognizes the interdependence of the control components. Implicit in this approach is the notion that some individual controls are more significant to the overall operating effectiveness of internal than other controls. For example, the effectiveness of an entity's control environment or computer general controls is a prerequisite for the effective operation of an individual control procedure for a specific transaction.

     Additionally, the term "internal control over financial reporting" incorporates the notions of materiality and risks. For example, the attestation standards state that evaluating the effectiveness of the design of a specific control is concerned with whether the control is suitably designed to prevent or detect *material* misstatements.

     For these reasons, the first step in evaluating the effectiveness of internal control *taken as a whole* is to identify significant individual controls, both at the entity level and next at the business process level. Your assessment of internal control effectiveness will focus on these significant controls.

     Note: Steps 2, 3, and 4 of the process should be performed first for the entity-level controls and then repeated for activity-level controls.

  2. *Ensure adequate documentation of significant controls*. The documentation of a control is an important design element of the internal control system. For example, it is difficult for control procedures to be reliable consistently if there is no formal means for communicating the requirements of the procedure. For this reason, management should review the entity's documentation of significant controls to ensure that it is adequate.
  3. *Evaluate the design effectiveness of significant controls*. To evaluate the design of controls requires that procedures be performed to determine whether the control is suitable to prevent or detect material misstatements. The nature of the procedures performed will vary according to the circumstances.
  4. *Evaluate the operating effectiveness of significant controls*. Tests of operating effectiveness are concerned with
     - How the control was applied
     - The consistency with which it was applied
     - By whom it was applied

- *Report*. The process ends when the CEO and CFO prepare their report on the effectiveness of the entity's internal control.

Subsequent chapters in this book provide more detailed guidance on each of these phases in the process.

A Consultative Approach to Achieving Project Objectives. The right side of Exhibit 1.4 describes a separate process that is repeated continuously for each of the steps required to evaluate the effectiveness of internal control. As you undertake your engagement, you should consider that the entity may have already taken steps to evaluate the effectiveness of its internal control. For example, the company may have accumulated evidence to support its assessment of internal control in conjunction with

- Ongoing SOX 404 compliance activities
- The quarterly disclosure control reporting requirements
- Internal control–related work performed by internal auditors and others
- Internal control reporting required by other regulations, such as the Federal Deposit Insurance Corporation Improvement Act (FDICIA), which applies to financial institutions

Thus, each step in the evaluation process begins with obtaining an understanding of the actions already taken by the entity to achieve the engagement objectives. If those steps are adequate and achieve the objective, then no further work is necessary. If those steps are not adequate, then you are in a position to assess the entity's needs, recommend solutions, gain commitment, and then implement them.

For example, suppose that as part of its quarterly reporting on internal control, ABC has formed a disclosure committee to oversee that process. Part of the committee's responsibilities is to identify significant disclosure control policies and procedures. However, ABC has not taken any steps to identify significant controls over financial reporting. In that situation, the first step in the evaluation process would be to review the work of the disclosure committee related to significant disclosure controls and to assist in the identification of significant internal controls over financial reporting.

CONSIDERATIONS FOR OUTSIDE CONSULTANTS

Some entities may lack the resources or expertise necessary to conduct a thorough, comprehensive assessment of their internal control. In order to comply with the SEC reporting requirements, these entities commonly engage outside consultants to provide them the necessary assistance. This section provides guidance to consul-

tants who have been engaged in such a capacity. Although the section is written for external consultants, employees and internal project leaders involved with the assessment process may find some of the guidance that follows to be useful.

Pre-Engagement Considerations

Before you begin your engagement to help management assess the effectiveness of internal control, you will need to gather information and come to a mutual understanding with the client on whether you will be engaged to perform the work, and if so, how the engagement will be structured. In this pre-engagement phase, your objectives are to

- Obtain a commitment from the client to move forward with the project.
- Understand the client's expectations for the conduct and results of the project.

Most likely, you will be required to meet with the prospective client in order to achieve these goals. Following are some suggestions for how to prepare for and conduct such a meeting.

Preparing to Meet the Prospective Client

Obtain a Basic Understanding of the Client. Your first step in preparing for a meeting prior to entering into the engagement should be to obtain a basic understanding of the prospective client. This understanding should be sufficient to enable you to

- Ask insightful questions about the entity and its operations.
- Understand the implications of answers that are provided.
- Identify the most significant issues that will affect engagement performance.

This preliminary understanding of the client should *not* be detailed enough for you to plan the engagement. Understanding the client at that level of detail will be the first phase of the engagement itself.

To obtain this understanding you may wish to

- Read the entity's most recent 10K to gain an understanding of its most significant business processes, the scope and complexity of its operations, and the results of its most recent assessment of internal controls. Chapter 3 provides suggestions for what to look for when reading an entity's 10K.
- Review information posted on the company's Web site, particularly in its investor relations section.
- Make inquiries of the entity's independent auditors, especially if you have an existing relationship with them or they were responsible for introducing you to the prospective client.

Identify Assumptions and Goals. Before meeting with the prospective client, it may be helpful for you to identify any assumptions you have about your proposed work together with the goals of your meeting. By articulating these assumptions and goals, you will be better able to quickly reach a mutual understanding of the nature of the work and the results that can be expected.

When preparing for the meeting, consider exploring answers to the following questions:

- What assumptions are you making about the prospective engagement? For example:
  - Management's understanding of the process that will be followed by the independent auditors during their audit of the internal control report
  - Management's understanding of the depth and quality of documentation required to support their assessment of internal control effectiveness
  - The entity's existing process for evaluating the effectiveness of internal control
  - The resources the entity has to commit to the project
  - The nature of the independent auditors' involvement with the assessment of internal control
- What are you basing your assumptions on? For example:
  - Conversations with the prospective client
  - Discussions with the prospective client's independent auditors
  - Information contained in public filings or the entity's own Web site
- What assumptions would it be appropriate for you to share with the prospective client if the opportunity arose?
- Under what assumptions is your client operating? For example:
  - Your and your firm's knowledge and expertise
  - The amount of work required to assess the effectiveness of internal control and prepare for an audit of that assessment
  - The urgency of the project
- What is the prospective client's goal for the interaction? For example, the prospective client may be considering several options for how they will conduct their assessment and who they will involve, and their goal for the meeting may be to assess your and your firm's qualifications.

Identify Key Players. Prior to meeting with the prospective client, you should consider who should be involved in the meeting. From the prospective client, you will want to be sure that the meeting includes the client's internal project leader and, if someone else, the person(s) who will make the decisions about whether to retain the services of you and your firm.

From your firm, in addition to yourself, you also should include individuals

with expertise that is particularly relevant to the prospective client's situation. For example, if your prospective client's business processes are heavily technology dependent, you should include an individual with information technology (IT) auditing experience in your meeting. Prospective clients that operate in industries with highly specialized business practices and needs will expect you and your firm to demonstrate a depth of expertise in those specialized practices.

Meeting with the Prospective Client

Your initial meeting(s) with a prospective client can be broken down into two phases:

1. Information gathering, in which your primary role is to ask questions, listen, and gather information
2. A second phase in which you describe your overall approach to the engagement as a means to help them decide whether to retain your services

During this meeting it is important to refrain from offering solutions, even if those solutions seem obvious. You need to thoroughly assess needs and understand the situation and the client before you offer a solution. To offer a solution prematurely is to risk proposing the wrong solution or the solution to a different problem.

Gather Information

Assess Client Understanding. The prospective client's understanding of their own needs can vary widely. On one end of the spectrum, the client may have already performed a significant amount of work to assess its internal controls, and as a result of that work, designated you and your firm to oversee the remainder of the process. At the other end of the spectrum, the prospective client may have made very little progress. You should seek to determine where the prospective client falls along that spectrum of understanding.

Assess Current Situation. During your meeting with the client, you should obtain information about the current situation. For example, you may wish to make inquiries about

- The experience of the company in its most recent assessment of internal control.
- Whether the prospective client has established a project team that has the overall responsibility for conducting the assessment of internal control. If so, then it would be helpful to know
  - The members of the project team
  - The progress the team has made to date

  - The role, if any, that the independent auditors will play in management's evaluation process
- Any known or suspected issues identified to date, including
  - Scope of work
  - Lack of adequate documentation
  - Means for assessing effectiveness
  - Identified or suspected control deficiencies
  - Other reporting issues
- How the prospective client will measure the success of the project

Your Role on the Project Team. It is important for you to clarify the prospective client's expectations regarding your role in assisting them in the project. They may be looking for someone to lead the project. Or they may simply wish to engage you to help in certain limited matters, such as performing tests of the operating effectiveness of specific controls. You should clarify your responsibilities and ensure that the working relationship (e.g., to whom you will report or the authority you have to make decisions) is aligned with that level of responsibility. Whatever your role you should make it clear to your client that senior management of the company, not you, have the responsibility for implementing and maintaining internal control and for forming an opinion on its effectiveness.

Additionally, you should try to determine the prospective client's understanding of *how you will add value* to the project. There are several ways in which you can add value, including

- *Technical expertise*. You can provide technical expertise in a number of areas, including internal control design, the design and evaluation of tests of internal controls, and the documentation and support required by the independent auditors to perform their attestation of the entity's report on internal control.
- *Problem solving*. The prospective client may look to you to provide solutions when problems are identified. For example, if internal control deficiencies arise, you may be asked to design new controls to address the deficiency.
- *Business strategy*. As you gain an understanding of the entity's internal control, you may find opportunities for improvement that fall outside of financial reporting and disclosure. The prospective client may expect you to identify these areas for improvement to internal control that will help the entity achieve operational goals and strategies.
- *Project administration*. The prospective client may expect you to take the lead in conducting the project, relying on you to take the initiative to form an effective project team, work within the time and budget constraints, provide regular project status reports to management, and coordinate the project with the independent auditors.

For each of your information-gathering objectives you should develop a questioning strategy for your meeting with the prospective client.

Describe an Overall Approach to the Engagement

Once you gain an understanding of the client's situation and their expectations, the meeting will invariably shift to you and how you will approach the engagement. This is natural, since the prospective client will want to alleviate some of the uncertainty they have about how the engagement will be performed. Again, it should not be necessary for you to provide a detailed plan for engagement performance—you have not gathered enough information at this point to provide such a plan in any meaningful way.

However, it is appropriate for you to discuss your overall approach to the engagement. In describing that approach, you should emphasize the following:

- *The project will be done in phases*. Depending on the needs of the client, the engagement will start with planning; proceed through an assessment of the documentation, design, and operating effectiveness of significant controls; include a provision for remedial action, if any; and conclude with the preparation of the report.

  This phased approach allows the client to maintain control of the project, how it proceeds, and whether you will continue in the role that was originally envisioned. At the conclusion of each phase, you will present the work product, and the client will determine whether and how to proceed to the next phase. Presenting your engagement in this fashion will alleviate a great deal of the uncertainty the prospective client has about the project.
- *The work builds on what the prospective client has already done.* Each phase of the project begins by understanding the steps the entity has already taken to achieve the objective of the work. Needs are evaluated and only the work that is necessary to achieve the stated objective is proposed. Work is not started until there is agreement on the scope of the work, the procedures that will be performed, and the deliverables and their timing. You will communicate with the independent auditors during each phase to ensure that the approach and resulting work product will meet their needs.

Clarifying the Work Arrangement

Once you have been engaged by management to help in their assessment of internal control, then your agreement should be documented in an engagement letter or contract. A written agreement between you and your client is the best way to make sure that the two parties have an understanding of the services you will provide.

For consulting services, a common structure to written agreements is one that includes

- The main agreement, which describes the general nature of the work and other matters such as fees, the limitations of the work, ownership of any resulting intellectual property, confidentiality, and so on.
- An exhibit to the agreement, which describes the work and the related deliverables in more detail. As described above, your work will be done in phases, with the client having the control to decide whether and when to move on to the next phase. As you and the client reach an agreement as to the nature and scope of each phase of the agreement, you would prepare an additional appendix to your engagement letter to document this agreement.

Main Agreement. The main agreement remains unchanged; as you and the client agree to additional phases in the process, you would draft and have the client sign additional appendixes.

Your firm most likely has a standard engagement letter that can serve as the basis for your main agreement. In modifying this standard letter for an engagement to help in the assessment of the effectiveness of internal control, consider the following:

- *Description of services*. The main agreement should refer to the attachment for a complete description of services.
- *Clarify responsibilities*. The CEO and CFO are responsible for establishing and maintaining adequate internal controls and procedures for financial reporting and for assessing the effectiveness of the company's internal controls. Working under the direction of the company's senior management, your responsibility is to assist them in making their assessment.
- *Guarantees and limitations*. Your agreement should clearly state that you do not guarantee any results (e.g., that the independent auditors will issue a "clean opinion" on management's report on internal control). You also should consider any limitations on what the client can expect from your work. For example, your engagement is not designed to detect occurrences of fraud.
- *Open-ended phrases*. Be careful not to give the impression that the scope of your work is open-ended and includes whatever is necessary to "get the job done." Phrases such as "other such services as necessary" should be avoided.
- *Separate engagement letters from proposals*. If you prepare a written proposal for a prospective client, it is generally good practice to *not* include an engagement letter or contract as an attachment. You do not want to give the client the impression that your engagement included all the services that you might have mentioned in a proposal or other marketing collateral.
- *Ownership of work product*. Typically, in a consulting engagement, the work product becomes property of the client. In some instances, you may wish to re-

tain the ownership or right to future use of certain by-products of your engagement, for example, training materials or process methodologies. In either case, be sure to clearly delineate ownership rights in your engagement letter.

Description of Services Exhibit. In general, you should consider including the following in your exhibit describing the services you will perform at each phase of the engagement.

- *Description of services/objective*. A brief description of the services to be performed and their objective; for example, "assist in the identification of significant internal controls, which will serve as the basis for testing and evaluating the entity's internal control over financial reporting and disclosure controls."
- *Process*. A summary of the process you will use to deliver the services.
- *Deliverables*. A description of what you will produce as a result of the work.
- *Fees*. Fees are not part of the main agreement but are determined separately for each phase of the work. Thus, the fees should be included in the exhibit.
- *Schedule and timing*. When the product will be delivered and, if appropriate, the timing of significant milestones.
- *Assumptions*. Summarize the assumptions upon which the agreement is based, for example, that the client will be providing certain resources.

APPENDIX 1A
Action Plan: Structuring the Engagement

The following action plan is intended to help you implement the suggestions contained in this chapter for structuring an engagement to assess the effectiveness of internal control.

1. Understand Rules and Standards

Become familiar with the relevant rules and standards pertaining to the assessment of internal control. For example:

- Consider the summary guidance on the following matters presented in this chapter:
  - SEC annual and quarterly reporting requirements
  - PCAOB internal control auditing standard
- If you have not done so already, read the relevant SEC rules and PCAOB Auditing Standard No. 2.

- Read all SEC Staff "Frequently Asked Questions" and PCAOB Staff "Questions and Answers" that were issued since the company's last internal report.

2. Clarify Your Approach

Develop a structured, comprehensive approach for assessing and reporting on the effectiveness of internal control. Possible action steps include

- Read and understand the Top Down Approach described in the PCAOB Staff's answer to Question 38, issued May 16, 2005.
- Become familiar with the engagement approach described in this chapter.
- Modify approach as necessary to meet the needs of the entity, expectations of management, qualifications of potential team members, and so on.

Additional considerations for outside consultants:

3. Assess Prospective Clients

Identify and gather information about prospective clients.

4. Meet Prospects

Meet with prospective clients and

- Gather information about client's needs.
- Assess their current situation.
- Clarify client's expectations about your role on the engagement team and the role of the company's senior management.

5. Reach Understanding

Obtain a written understanding of your work arrangement with the client.

APPENDIX 1B

Requirements for Management's Assessment Process: Cross Reference to Guidance

As indicated in this chapter, PCAOB Auditing Standard No. 2 related to the audit of internal control requires the independent auditor to evaluate management's process for assessing the effectiveness of the company's internal control. The standard then describes certain elements that should be present in management's process.

Exhibit 1.5 summarizes those required elements and provides a cross-reference

Exhibit 1.5 Auditing Standard Requirements

PCAOB Audit Standard Requirement.	Applicable Guidance
Determine which controls should be tested.	Chapter 4
Controls over initiating, recording, processing, and reporting significant accounts and disclosures and related assertions.	Chapter 7
Controls over the selection and application of accounting policies.	Chapters 4 and 6
Anti-fraud programs and controls.	Chapters 4 and 6
Controls on which other controls are dependent.	Chapters 4 and 6
Controls over significant nonroutine and nonsystematic transactions, such as accounts involving judgments and estimates.	Chapters 4 and 6
Company-level controls.	Chapters 4 and 6
Evaluate the likelihood that failure of controls could result in a misstatement.	Chapter 8
Determine the locations or business units to include in the evaluation for a company with multiple locations or business units.	Chapter 3
Evaluate the design effectiveness of controls.	Chapters 6 and 7
Evaluate the operating effectiveness of controls.	Chapters 6 and 7
Determine whether the deficiencies in internal control constitute significant deficiencies or material weaknesses.	Chapter 8
Communicate findings to the auditor and to others, if applicable.	Chapter 8
Evaluate whether findings are reasonable and support management's assessment.	Chapter 8

to the chapters in this book where you can find guidance to help you comply with these requirements.

Notes

1. See Regulation S-K, Item 308 (17 CFR §229.308).
2. At the time this manuscript was prepared, these reporting requirements were effective for all accelerated filers. Non-accelerated filers (both U.S. and foreign) are required to fully comply for their first fiscal year ending after July 15, 2007. Accelerated foreign private issuers are required to comply as of the first fiscal year ending after July 15, 2006.

3. As described more completely in Chapter 2, internal controls should be considered within the context of an entity's overall risk management strategy. In order to identify and understand an entity's significant controls, it is important to understand the significant risks facing the entity. You may wish to identify and assess these risks as a separate engagement step. However, the approach described in this book considers this risk assessment to be a component of this process step, the identification of significant controls. See Chapter 4 for additional details.