Part I

Authoritative and Nonauthoritative Guidance on the Auditor's Risk Assessment in a Financial Statement Audit

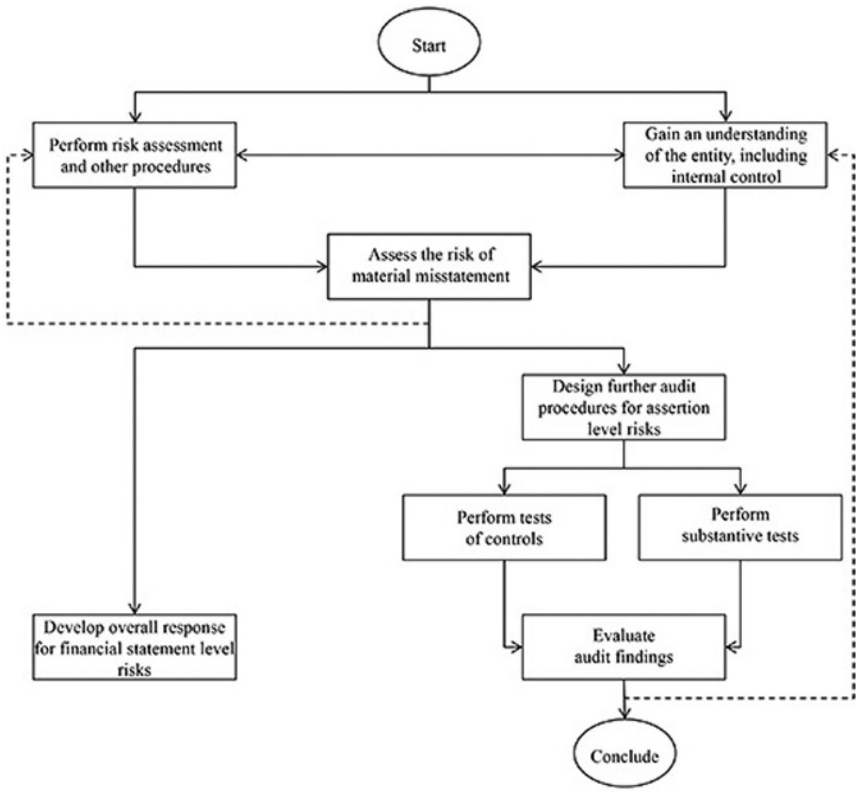
Chapter 1

Overview of Applying the Audit Risk Standards

TABLE OF CONTENTS

Observations and Suggestions

Illustration 1-1
Overview of Applying the Audit Risk Model



This illustration describes a high-level approach to the process that you follow to apply the audit risk standards to your audits by (1) assessing the risks of material misstatement, (2) using this risk assessment to plan and perform further audit procedures, and (3) evaluating the results of your procedures and reaching conclusions about the financial statements.

An Iterative Process. *Although the flowchart may indicate to some a linear audit process, an audit is, in fact, an iterative process in which you may repeat as the audit progresses the steps described in the flowchart as a result of new information obtained. In the flowchart, the dotted line connecting later steps in the process to earlier steps illustrates the potential iterative nature of the audit process.*

As indicated by the dotted line, the results of further audit procedures provide you with information that you use to confirm or modify your original risk assessment, which in turn, may lead to additional audit procedures or to a conclusion.

Perform Risk Assessment Procedures to Gain an Understanding of the Entity. *The first step in the process is to perform* risk assessment procedures *(for example, inquiry, observation, or inspection of documents) to gather information and gain an understanding of your client and its environment, including its internal control.*

Gain an Understanding of the Entity and Its Environment, Including Internal Control. *You should gain an understanding of the entity and its environment, including internal control, to identify and assess risks of material misstatement and to design further audit procedures. As you gather information about your client, you will begin to form an understanding of its business and the environment in which it operates. An important part of this understanding is your evaluation of the design of internal control and a determination of whether controls have been implemented (that is, placed in operation). This knowledge of the client, including the design of its internal control, may prompt you to seek additional information until you are satisfied with your level of understanding. Specifically, this knowledge and understanding of the client will enable you to assess whether there are risks of material misstatement in the financial statements that you are auditing. These risks should be expressed in terms of what can go wrong in specific classes of transactions, account balances, and disclosures and their relevant assertions.*

Materiality. *As you gather information and perform risk assessment procedures, you will want to have a materiality threshold in mind. Your risk assessment is responsive to judgments about financial statement materiality. Materiality is a critical judgment that affects all steps in the audit process. Because this judgment is not clearly associated with a specific phase and is responsive to some information you will be gathering before assessing the risks of material misstatement, it is not separately depicted in the illustration.*

Assess the Risks of Material Misstatement. *After identifying risks you will (1) relate them to what can go wrong in preparing the financial statements and (2) assess the likelihood and significance of the risk. When making these risk assessments, consider that*

- *the* risk of material misstatement (RMM) *is a combination of inherent and control risk. You are not required to perform a combined risk assessment, as you may choose to make separate assessments of inherent and control risk.*

- *risks of material misstatement can reside at either the financial statement level or the assertion level for classes of transactions, account balances, or disclosures. For example, a risk relating to the regulatory environment in which your client operates is a pervasive risk that affects many of the financial statement assertions in many accounts. On the other hand, a risk related to the valuation of inventory is restricted to that account and assertion and the related determination of cost of sales. Understanding the differences between the two types of risks is important because these differences drive your audit response. You will perform different procedures to understand and respond to financial statement level risks than you will need to understand and respond to assertion level risks.*

- *your assessment of risk at the assertion level should be specific to the unique circumstances of the entity. For example, assessing the* risk of material misstatement *relating to the existence assertion of an account as* "high" *in many cases would not be sufficient to design effective further audit procedures. Instead, in this example, your assessment of risk should describe how the existence assertion could contain a material misstatement, given the specific business processes, information processing, and controls in use at the particular client. It is common to use standard audit programs and example audit practice aids to complete your engagement. However, when using these standard programs and examples, it is important to consider carefully whether they appropriately reflect the unique circumstances of your client. To be effective, such programs are ordinarily tailored to each engagement.*

- *it is important that your risk assessments are supported by sufficient appropriate audit evidence. It is not appropriate to simply designate a risk to be at a given level without any support for the risk assessment. For example, why is the risk "low" and what supporting evidence do you have to support the assessment? This enumeration facilitates the review and communication value of the documentation.*

- *to the extent possible, even risks that reside at the financial statement level should be related to what can go wrong at the relevant assertion level for classes of transactions, account balances, or disclosures.*

Design Further Audit Procedures to Respond to Assessed Risks. *Once you have assessed the risks of material misstatement, you will design* further audit procedures *in response to these risks. There are two types of* further audit procedures*: tests of controls and substantive procedures. You may perform a combination of these two types of procedures. Of critical importance in performing an effective audit is to develop a clear link between the identified risks, the assessment of those risks, and the further audit procedures performed in response to the assessed risks. By relating risks of material misstatement to specific assertions, you will be able to establish this necessary linkage. Cross-references between assessed risks and further audit procedures facilitate the quality of the documentation and make working papers easier to review for quality assurance.*

Evaluate Audit Findings and Evidence. *At the conclusion of the audit, you are required to evaluate the results of your audit procedures and reach a conclusion concerning whether the financial statements are free of material misstatement. You also should determine whether you have obtained sufficient appropriate audit evidence to support your audit opinion at a high level of assurance. Finally, you are required to evaluate identified control deficiencies and determine whether these deficiencies, individually or in combination, are significant deficiencies or material weaknesses.*

On every audit you are required to assess the risks that individual financial statement assertions are materially misstated. Other AICPA Audit and Accounting Guides may provide useful suggested risk assessment procedures if an entity is in a specialized industry or has transactions addressed within the specialized industry guides. The assessment of risk then serves as the basis for the design of further audit procedures.

This chapter provides an overview of this process, beginning with the information about the client and its environment that is necessary for you to identify risks, how you use that information to assess risk at the assertion level, and how that risk assessment helps you determine further audit procedures.

Subsequent chapters provide additional detail, as well as examples and illustrations of how the general guidance described here might be applied.

Practice Considerations for Auditors of Entities Using the COSO Framework

In May 2013, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published the updated *Internal Control—Integrated Framework* (COSO framework). The update of the original 1992 *Internal Control—Integrated Framework* (original COSO framework) became necessary due to the increasing complexity of business, evolving technologies, and changing expectations of stakeholders. The COSO framework updated in 2013 supersedes the original COSO framework after December 15, 2014.

Although the auditing standards do not require the application of a specific internal control framework, the COSO framework is widely used by entities[1] for designing, implementing, and conducting internal control. The COSO framework provides guidance that is useful and relevant to auditors charged with evaluating the design and implementation of controls (for example, as part of their risk assessment procedures) during a financial statement audit. The discussion in the following chapters of this guide are reflective of the fact that auditing standards are written without reference to a specific controls framework.

The auditing standards recognize 5 components of internal control that, for purposes of generally accepted auditing standards, provide a useful framework for auditors when considering how different aspects of an entity's internal control may affect the audit. Chapter 2, "Key Concepts Underlying the Auditor's Risk Assessment Process," and appendix C, "Internal Control Components," of this guide further explain these 5 components and the elements of

[1] *Standards for Internal Control in the Federal Government*, known as the "Green Book," sets the standards for an effective internal control system for federal agencies and may also be used by state and local governments and quasigovernmental entities, as well as not-for-profit entities.

those components that are relevant to the audit. These components are consistent with the components recognized in the COSO framework. However, the COSO framework includes not only 5 separate components but also 17 principles representing the fundamental concepts associated with the components.

In order for an entity's system of internal control to be effective, the COSO framework states that each of the five components of internal control and relevant principles should be *present* (designed appropriately and placed in operation) and *functioning* (effectively operating) and that the five components be operating together in an integrated manner. A major deficiency exists in an entity's system of internal control when the entity's management has determined that a component and one or more principles are not present and functioning or that components are not operating together. A *major deficiency* according to the COSO framework is an internal control deficiency or combination of deficiencies that severely reduces the likelihood that the entity can achieve its objectives. As discussed in the COSO framework, when a major deficiency exists, an entity cannot conclude that it has an effective system of internal control.

Observations and Suggestions

The COSO framework uses the terms *component*, *principle*, *points of focus*,[2] *approaches*, and *examples* to assist users in applying the framework. The auditing literature in many cases uses the term *objective* to help users comprehend the controls assessment process. This audit guide follows the terminology in the Statements on Auditing Standards, but may clarify how certain terms relate to the COSO framework. For example, companies may set financial reporting "objectives" as part of Principle 6, which is different from the "objective" of having controls over the revenue account.

In addition, the COSO framework notes two deficiency assessment levels: deficiency and severe deficiency. However this guide uses the categorizations of deficiency, significant deficiency, and material weakness as set out in AU-C section 265, *Communicating Internal Control Related Matters Identified in an Audit* (AICPA, *Professional Standards*).

Chapter 7, "Evaluating Audit Findings, Audit Evidence, and Deficiencies in Internal Control," of this guide provides guidance on the evaluation and communication of control deficiencies in the context of the auditing standards.

Points of focus are also provided within the COSO framework. There is no requirement that an assessment be performed to determine whether all points of focus are present and functioning. Management may determine that some points of focus are not suitable or relevant to the entity. Similarly, management may identify other suitable and relevant points of focus in addition to those provided in the COSO framework.

The fundamental concepts of an effective control are the same whether the entity is large or small. The auditing standards do not set up a lower standard

[2] *Points of focus* are important characteristics of principles that assist management in designing, implementing, and conducting internal control and in assessing whether the relevant principles are, in fact, present and functioning.

for small businesses or separate standards for different industries. Additionally, the auditing standards have no measures for achieving effective internal control that apply only to certain businesses. Similarly, the COSO framework views the 5 components and 17 principles as suitable to all entities. The COSO framework presumes that principles are relevant because they have a significant bearing on the presence and functioning of an associated component. Accordingly, if a relevant principle is not present and functioning, the associated component cannot be present and functioning. Therefore, in the context of risk assessment for a financial statement audit of an entity using the COSO framework, the consideration of the COSO components and principles is applicable regardless of the size of the entity being audited.

Appendix C of this guide specifies the 5 COSO components of internal control and the 17 COSO principles representing the fundamental concepts associated with the components.

COSO has also published the following companion documents to the COSO framework:

- *Internal Control—Integrated Framework Illustrative Tools for Assessing Effectiveness of a System of Internal Control*
- *Internal Control—Integrated Framework Internal Control over External Financial Reporting: A Compendium of Approaches and Examples*

Although not authoritative, these resources may be useful to auditors charged with evaluating the design and implementation of controls (as well as the operating effectiveness thereof) in conjunction with a financial statement audit.

Entities that have adopted the COSO framework and their auditors may find the transition to it, or the first time adoption of it, challenging in some respects. For example, the auditing standards currently do not explicitly recognize the 17 principles that COSO introduced in the COSO framework, although the principles for the most part align with the elements of internal control outlined in AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* (AICPA, *Professional Standards*). This guide can help relate the framework to the auditing standards and acts as a bridge to help entities and their auditors transition from the original COSO framework.

The Purpose of This Audit Guide

1.01 You, as the auditor, are required to perform risk assessment procedures, which include gaining an understanding of systems of internal control, to provide a basis for the identification and assessment of risks of material misstatement at the financial statement and relevant assertion levels. (Throughout this guide the auditor is referred to as "you.") This risk assessment then serves as the basis for you to design the nature, timing, and extent of further audit procedures. (AU-C sec. 315 par. .05 and AU-C sec. 300 par. .09)

1.02 The further audit procedures you design and perform should be appropriate in the circumstances for the purpose of obtaining sufficient appropriate audit evidence to be able to draw a reasonable conclusion on which to base your opinion. (AU-C sec. 500 par. .01 and .06)

1.03 This guide provides guidance, primarily on performing risk assessment procedures referred to in paragraph 1.01 and obtaining sufficient appropriate audit evidence referred to in paragraph 1.02. As such, this guide illustrates how to gather information needed to assess risk, evaluate that information to assess risk at the assertion level, and design and perform further audit procedures based on that assessed risk, evaluate the results, and reach conclusions. In addition, guidance on evaluating and communicating findings is also included.

Observations and Suggestions

The preceding paragraph describes a process in which there is a link between information gathering, the identification and assessment of risk, and the design and performance of further audit procedures. Each step in this process serves as the basis for performing the subsequent step. For example, your determination of what can go wrong at the assertion level helps you determine the nature, timing, and extent of your substantive procedures.

This linkage between the various stages in the risk assessment process is vital to performing an effective and efficient audit.

Financial statement assertions allow you to develop this link between the various stages of the risk assessment process. For example, your substantive procedures and tests of controls are directed at what can go wrong in specific assertions. For those audit procedures to be clearly linked to risks of material misstatement, those risks also should be expressed at that same level of detail: what can go wrong in the financial statement assertions.

Your documentation of the risks and associated procedures should be clear, to enable an experienced auditor with no prior association with the audit to understand the intended linkage.

1.04 Understanding the entity and its environment includes obtaining an understanding of its internal control. (This guide uses the term *client* to refer to the entity being audited.) This understanding of internal control should be sufficient to allow you to evaluate the design of controls and to determine whether they have been implemented (placed in operation). (Unless otherwise indicated, this guide uses the term *internal control* to mean "internal control over financial reporting, including the relevant controls over safeguarding assets.")

Overview of the Risk Assessment Process

1.05 This chapter provides a summary of the risk assessment process followed in an audit. Even though some requirements and guidance are presented in a way that suggests a sequential process, risk assessment involves a continuous process of gathering, updating, and analyzing information throughout the audit. Accordingly, you may implement the requirements and guidance in a different sequence from that presented in this guide or you may revisit steps when updated information is available.

Observations and Suggestions

Auditing is a nonlinear process, and different auditors may have different judgments about which steps should be performed first. For example, some auditors may determine that it first is necessary to obtain an understanding of the client and its environment to develop an appropriate audit strategy. Other auditors may determine that it first is necessary to determine appropriate materiality levels, which then serve to guide them through the information gathering process.

Neither approach is inherently more effective or efficient than the other. Within the audit process, it is common for different steps to interact dynamically with one or more other steps. The determination of materiality drives audit procedures, which produce results, which in turn influence materiality levels.

In that sense, it may not matter where you start in the process as long as you continue to revisit the procedures you performed and confirm the judgments made earlier in your engagement as you discover new information. For example, a practical point at which to revisit the judgments made to date and their interactions is when assessing the *risks of material misstatement*. At that point, the materiality and risk assessment procedures come together in determining the further audit procedures, and the assessment of the risks of material misstatement is an important determinant of the procedures to be applied to the audit risks.

1.06 The following is an overview of the audit process described in this guide:

- Perform risk assessment procedures by *gathering information about the entity and its environment, including internal control*. You should gather information about those aspects of the client and its environment that will allow you to identify and assess *risks of material misstatements* of the client's financial statements. The client's internal control is an integral part of its operations, and your evaluation of the design of internal control is an important part of your understanding of the client.
- *Gain an understanding of the entity and its environment, including its internal control*. You need to develop an understanding of specific aspects of the entity, its environment, and internal control to identify and assess risk and design and perform further audit procedures. Based on the information gathered, you should be able to identify what can go wrong in specific classes of transactions, account balances, and disclosures and their relevant assertions.
- *Assess risks of material misstatement*. Next, you will use your understanding of the client and its environment to assess the risks of material misstatement that relate to relevant assertions. Paragraph .27 of AU-C section 315, states that, to assess RMM, you should
    - — identify risks through the process of obtaining an understanding of the entity and its environment, including relevant controls that relate to the risks, by considering the classes of transactions, account balances, and disclosures in the financial statements;
    - — assess the identified risks and evaluate whether they relate more pervasively to the financial statements as a whole and potentially affect many assertions;

  - relate the identified risks to what can go wrong at the relevant assertion level, taking account of relevant controls that the auditor intends to test; and
  - consider the likelihood of misstatement, including the possibility of multiple misstatements, and whether the potential misstatement is of a magnitude that could result in a material misstatement.

- *Design further audit procedures (an audit response)*. You should address the risks of material misstatement at both the financial statement level and the relevant assertion level. These risks are described subsequently. (The auditing standards use the term *relevant assertions* to describe the specific assertions that are related to a given account, class of transactions, or disclosure. This guide uses the term *assertions* in the same manner in which the auditing standards use the term *relevant assertions*.)
  - Risks of material misstatement at the financial statement level have a more pervasive effect on the financial statements and affect many accounts and assertions. In addition to developing assertion-specific responses, these types of risks may require you to develop an overall, audit-wide response, such as your choice of audit team members.
  - Assertion level risk pertains to specific accounts and assertions and should be considered when you design and subsequently perform further audit procedures. These further procedures often encompass a combined approach using both tests of activity-level controls (this guide uses the term *activity-level controls* to refer to the controls that pertain to assertion level risks) and substantive procedures directed at individual account balances, classes of transactions, and disclosures and their relevant assertions. It is important that auditors are mindful that some risks may relate to more than one assertion.
- *Perform further audit procedures*. Further audit procedures include tests of controls and substantive procedures. The nature, timing, and extent of these procedures should be designed in a way that is responsive to your assessed risks. Once designed, you will perform these procedures to gather sufficient appropriate audit evidence to support your opinion on the financial statements.
- *Evaluate audit findings*. You will evaluate the results of further audit procedures and the audit evidence obtained to reach a conclusion about whether the client's financial statements are free of material misstatement or whether such a conclusion can be reached.

Audit documentation is an important part of every audit, and each chapter in this guide summarizes the documentation requirements that pertain to each phase in the audit.

(AU-C sec. 230 par. 08, AU-C sec. 315 par. .03, and AU-C sec. 500 par. .06)

Information Gathering

Information Needed About the Client and Its Environment to Identify and Assess Risks of Material Misstatement

1.07 Obtaining an understanding of your client and its environment, including internal control, is a continuous, dynamic process of gathering, updating, and analyzing information throughout the audit. This understanding establishes a framework that allows you to plan the audit and exercise professional judgment throughout the audit when, for example, you are

- assessing risks of material misstatement of the financial statements;
- determining materiality;
- considering the appropriateness of the client's selection and application of accounting policies and adequacy of its financial statement disclosures;
- identifying areas where special audit consideration may be necessary (for example, related party transactions);
- developing expectations for performing analytical procedures;
- responding to the assessed risks of material misstatement, including designing and performing further audit procedures to obtain sufficient appropriate audit evidence; and
- evaluating the sufficiency and appropriateness of audit evidence obtained.

1.08 Not all information about a client or its environment is relevant for your audit. Often, the information you are required to gather about your client is that which allows you to assess the risk that specific assertions could be materially misstated. AU-C section 315 defines the aspects of the client for which you should gather information and obtain an understanding. Table 1-1 summarizes these aspects. Chapter 3, "Planning and Performing Risk Assessment Procedures," of this guide provides more detail and examples of the information you should gather.

Table 1-1
Understanding the Client and Its Environment, Including the Entity's Internal Control

On every audit you should gather (or update) information and obtain an understanding of the client and its environment including an understanding of the

- relevant industry, regulatory, and other external factors affecting the client;
- nature of the client;
- client's selection and application of accounting policies;
- client's objectives and strategies and those related business risks that may result in risks of material misstatement

(continued)

Understanding the Client and Its Environment, Including the Entity's Internal Control—*continued*

- measurement and review of the client's financial performance; and
- the client's internal control relevant to the audit.

(AU-C sec. 315 par. .12–.13)

Relevant industry factors may include the market and competition, supplier and customer relationships, energy supply and cost, and technological developments.

Regulatory factors may include relevant accounting pronouncements, the regulatory framework, laws, taxation, governmental policies, and environmental requirements that affect the industry and client.

Other external factors may include general economic conditions, interest rates, inflation, and availability of financing.

Understanding the nature of the client, may include, among other matters, its operations, ownership, governance, the types of investments it makes and plans to make, how it is financed, and how it is structured. Numerous other matters you may consider are included in paragraph .A31 of AU-C section 315.

The client's selection and application of accounting policies may encompass the methods used for significant and unusual transactions, changes in accounting policies, new accounting standards and their adoption, and the financial reporting competencies of personnel. You should evaluate whether the client's accounting policies are appropriate for its business and consistent with the applicable financial reporting framework and those used in the client's industry. (AU-C sec. 315 par. .12)

The client sets strategies in the context of its industry, regulatory, and other external factors. Those strategies are the approaches to achieving its business objectives. Objectives and strategies are related to business risks. An understanding of business risks increases the likelihood of identifying risks of material misstatement because most business risks eventually have financial consequences that in turn affect the client's financial statements. You are not responsible to identify or assess all business risks because not all of them give rise to risks of material misstatement. Paragraph .A39 of AU-C section 315 includes numerous examples of objectives, strategies, and business risks.

The metrics used by management to measure and review financial performance provide you with information about the aspects of the entity that management considers to be important.

Internal Control

1.09 Not all of the client's internal controls are relevant to your audit. When performing a financial statement audit, your consideration of internal control is limited to those controls that are deemed to be "relevant to the audit." Operational controls, for example, over production and other business functions, may affect but often are not directly related to financial reporting. Accordingly, early in the audit process, you will determine which controls are relevant to the audit. For example, production quality control issues may affect estimates of warranty costs. Paragraph .A69 of AU-C section 315 lists many factors that you might consider in making a professional judgment about whether a control, individually or in combination with others, is relevant to the audit. The factors include materiality, the size of the entity, the diversity and complexity of its operations, and how a specific control prevents, or detects and corrects, potential material misstatements.

1.10 There are some controls that are relevant to every audit. These controls relate to

a. elements of the five internal control components that chapter 2 of this guide describes. On each audit, you should gain an understanding of certain, specified elements relating to each of the five components.

b. antifraud programs and controls. AU-C section 240, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*), directs you to evaluate the design and implementation of antifraud programs and controls.

c. controls related to "significant risks." Some significant risks arise on most audits, and the controls related to these risks are relevant to your audit. Significant risks are discussed in paragraph 1.30.

d. controls related to circumstances when substantive procedures alone will not provide sufficient appropriate audit evidence.

e. other controls that you determine to be relevant to your audit.

In addition, when obtaining an understanding of the company and its environment, the design and implementation of controls over the most significant revenues and significant expenditures will, in many cases, be relevant. Chapters 3 and 4, "Understanding the Client, Its Environment, and Its Internal Control," further describe these categories of relevant controls in more detail.

Risk Assessment Procedures

1.11 You should perform risk assessment procedures to provide a basis for your identification and assessment of risks of material misstatement at the financial statement level and relevant assertion level. Risk assessment procedures include

a. inquiries of management, appropriate individuals within the internal audit function (if such function exists), and others at the client who, in the auditor's professional judgment, may have information that is likely to assist in identifying risks of material misstatement due to fraud or error,

b. analytical procedures, and

c. observation and inspection.

(AU-C sec. 315 par. .06)

Observations and Suggestions

You should perform risk assessment procedures to support your assessment of the risks of material misstatement. Your risk assessment procedures provide the audit evidence necessary to support your risk assessments, which, in turn, drive the nature, timing, and extent of further audit procedures. Thus, the results of your risk assessment procedures are an integral part of the audit evidence you obtain to support your opinion on the financial statements. It is not acceptable to simply deem risk to be "at the maximum" without evidence or support unless such an assessment is supported by the facts. By defaulting to maximum risk without adequate understanding of actual controls in place, you are not determining specifically what, exactly, the risks are, and which assertions they affect. For example, is it likely that all assertions of accounts payable are equally risky? If that were so, extensive tests of existence and valuation would be required as well as the common tests of completeness and accuracy, and this is unlikely to result in an efficient audit. You may also overlook conditions or weaknesses that indicate a fraud risk. Example or illustrative audit programs may not be sufficient to address all possible risks of material misstatement that might be specific to this entity.

Further, even at the assertion level, for example, an inventory existence risk could be high, but it could result from a number of different causes, not all of which may be applicable at your client (for example, theft, shrinkage, cut-off issues, short deliveries). Without understanding and documenting what, exactly, is the source of this risk, you are not necessarily able to design the appropriate nature, timing, and extent of procedures to address the risk. Procedures designed to address a risk of theft may be different from procedures designed to address a risk of short deliveries or cut-off, even though both could be described as high risk pertaining to existence of inventory.

A Mix of Procedures

1.12 You are not required to perform *all* the risk assessment procedures (for example, inquiries, analytical procedures, observations, and so on) for *each* aspect of the client's internal control and its environment listed in table 1-1. However, in the course of obtaining the required understanding about the client, including internal control, you should perform all the risk assessment procedures.

(AU-C sec. 315 par. .A5)

Procedures to Obtain an Understanding of Internal Control

1.13 Inquiry may allow you to gather information about internal control design, but inquiry alone is not sufficient to determine whether the control has been implemented (placed in operation). Thus, when inquiry is used to obtain information about the design of internal control, you should corroborate the responses to your inquiries by performing at least one other risk assessment procedure to determine that client personnel are using the control. That additional procedure may be further observations of the control operating, inspecting documents and reports, or tracing transactions through the information system relevant to financial reporting.

1.14 Although AU-C section 500, *Audit Evidence* (AICPA, *Professional Standards*), notes that corroboration of evidence obtained through inquiry is often of particular importance, in the case of inquiries about the control environment and "tone-at-the-top," the information available to support management's responses to inquiries may be limited. When better audit evidence is not available from any other sources, corroborative inquiries made of multiple sources may sometimes be a source of evidence available to determine whether a control has been implemented (that is, placed in operation). When no more effective procedures can be identified, corroborating inquiries of different knowledgeable persons can be an effective procedure when the results of the inquiries are consistent with observed behaviors or past actions. For example, making inquiries of an owner-manager about the implementation of the company's code of conduct will not, by itself, allow the auditor to obtain a sufficient understanding of that aspect of the control environment. However, corroborating the owner manager's response with additional inquiries or a survey of other company personnel, and observing consistent behaviors or other evidence with respect to the results of those inquiries, may provide the auditor with the requisite level of understanding. As another example, if it is represented to the auditor that no instances of ethics code violations were reported and evidence of that is not otherwise observable, corroborating inquiry and the lack of contradictory evidence or observations may be the only viable alternative evidence. The auditor may consider his or her experience in dealing with management in this area as well as other areas, and consider whether any results from applying audit procedures are consistent with or might contradict such evidence before accepting the inquiries.

Observations and Suggestions

As will be discussed later, inquiry is often the starting point for understanding controls but is supported by observation, examining documentary evidence, or a walkthrough. These are common audit procedures that provide evidence that a control is in place.

Other Procedures That Provide Relevant Information About the Client

1.15 *Assessing the risks of material misstatement due to fraud.* AU-C section 240 directs you to perform certain audit procedures to assess the risks of material misstatement due to fraud. Some of these procedures also may help gather information about the entity and its environment, particularly its internal control. For this reason, it may be helpful to

- coordinate the procedures you perform to assess the risks of material misstatement due to fraud (for example, brainstorming) with your other risk assessment procedures, and
- consider the results of your assessment of fraud risk when identifying the risks of material misstatement.

The COSO framework specifies, under the risk assessment component, principles and associated points of focus addressing the entity's consideration of the potential for fraud during risk assessment procedures (principle 8).

1.16 *Other information.* When relevant to the audit, you also should consider other knowledge you have of the client that can help you assess risk. This other information may include either or both of the following:

- Information obtained from prior audits or from your client acceptance or continuance process
- Experience gained on other engagements performed by the engagement partner for the client, for example, the audit of the client's pension plan.

(AU-C sec. 315 par. .07–.08)

Updating Information From Prior Periods

1.17 If you intend to use information about the client you obtained from previous experience with the client and from audit procedures performed in previous audits, you should determine whether changes have occurred since then that may affect the relevance of the information to the current audit. To make this determination, you may make inquiries and perform other appropriate audit procedures, such as walkthroughs of relevant systems. (AU-C sec. 315 par. .10)

Gaining an Understanding of the Client and Its Environment

1.18 The gathering of information, by itself, does not provide you with the understanding of the client that is necessary for you to assess risk. For you to assess the risks of material misstatement and design further audit procedures, you will want to assimilate and synthesize the information gathered to determine how it might affect the financial statements. For example,

- information about the client's industry may allow you to identify characteristics of the industry that could give rise to specific misstatements. For example, if your client is a construction contractor that uses long-term contract accounting, your understanding of the client should be sufficient to allow you to recognize that the significant estimates of revenues and costs create risk, and without proper controls, there would be risks of material misstatement.
- information about the ownership of your client, how it is structured, and other elements of its nature assists you to identify related-party transactions that, if not accounted for properly and adequately disclosed, could lead to a material misstatement.
- your identification and understanding of the business risks facing your client increase the chance that you will identify financial reporting risks. For example, your client may face an imminent risk that a new company has recently entered its market, and that new entrant could have certain business advantages (for example, economies of scale or greater brand recognition). The potential risk related to this business risk might be obsolescence or overproduction of inventory that could only be sold at a discount. Thus, you might need to understand how the client understands and controls the risk in order to assess the risks of material misstatement.
- information about the performance measures used by client management may lead you to identify differences in internal control or pressures or incentives that could motivate client personnel to misstate the financial statements.
- information about the design and implementation of internal control may lead you to identify a deficiency in control design. Such an improperly designed control may represent a significant deficiency or material weakness.
- appendix B, "Understanding the Entity and Its Environment," of this guide suggests factors that may be relevant in understanding

the entity and its environment, and is reproduced from paragraph .A156 of AU-C section 315.

Understanding Internal Control

Observations and Suggestions

The "extent" of your understanding of controls describes the level of knowledge you should obtain about the controls. There are two basic levels of knowledge:

a. The design (presence) of the controls and whether they have been implemented. You should obtain this level of understanding on all engagements.

b. The operational effectiveness (functioning) of those controls. You should obtain this level of understanding only when you plan to rely on internal control to modify the nature, timing, and extent of your substantive procedures or in the circumstance when substantive procedures alone do not provide sufficient audit evidence.

The second level, the operational effectiveness of controls, requires a more in-depth testing of internal control that addresses how well the control performed during the audit period. To determine operational effectiveness, you first need to understand how the controls are designed and assess whether they appear to have been implemented (that is, placed in operation). In other words, any knowledge of operational effectiveness builds upon your evaluation of control design and implementation.

1.19 At a minimum, your understanding of internal control allows you to do the following:

a. *Evaluate control design*. Evaluating the design of a control involves determining whether the control is capable of either

  i. effectively preventing material misstatements, or

  ii. effectively detecting and correcting material misstatements.

b. *Determine whether a control has been implemented*. Implementation of a control means that the control exists and that the entity is using it.

(AU-C sec. 315 par. .14)

Procedures Related to Controls at a Service Organization

1.20 When your client uses a service organization to process some of its transactions, you may need to obtain an understanding of the information system and related controls that reside at the service organization. To help obtain that understanding, you may wish to obtain a report on the service organization's controls, prepared by the service organization's auditors.

Service organizations (including sub-servicers, if applicable) play an increasing role in the financial accounting and reporting of many entities. Relevant services that are performed by these organizations may be applicable regarding the *risks of material misstatement* of the entity they serve. The COSO framework contains a pervasive discussion of service organizations and the effect thereof on the considerations that may be made relevant to certain principles.

1.21 Just because your client uses a service organization to process some of its transactions does not, in itself, require you to obtain a service auditor's report. If certain conditions are met, such as sufficient company input and output controls on the information processed by the service organization, you may meet the requirements for understanding internal control without obtaining a service auditor's report on controls at a service organization. Paragraphs 3.78–.85 of this guide provide additional guidance on this matter.

Discussion Among the Audit Team

1.22 The engagement partner and other key members of the audit engagement team should discuss the susceptibility of the client's financial statements to material misstatement. The engagement partner should determine which matters are to be communicated to the engagement team members not involved in the discussion. (AU-C sec. 315 par. .11)

This discussion

- provides an opportunity for more experienced team members to share their insights;
- allows team members to exchange information about the client's business risks;
- assists team members to gain a better understanding of the potential for material misstatement resulting from fraud or error in areas assigned to them; and
- provides a basis upon which the team members communicate and share new information obtained throughout the audit that may affect the assessment of risks of material misstatement or the audit procedures to address those risks.

1.23 This discussion among the audit team could be held at the same time as the discussion among the team related to fraud, as described by AU-C section 240. In many cases this discussion may be held after the auditor obtains the understanding of the entity and its controls. If held earlier, the brainstorming might need to be repeated or updated.

Observations and Suggestions

The discussion among the engagement team about the susceptibility of the entity's financial statements to material misstatement and the annual brainstorming session specific to fraud can become stale over time. To keep the sessions thoughtful and effective, auditors may vary the format and focus of discussions. In some cases, fraud specialists or firm owners may be invited to participate in the engagement discussion to provide a fresh perspective.

Assessing the Risks of Material Misstatement

Observations and Suggestions

To assess the risk of "material" misstatement, you will need to determine an appropriate materiality level. Over the course of your audit, as you perform audit procedures and evaluate the results, you may revise your determination of materiality. If your judgments of materiality do change, you also may want to reevaluate your assessment of the risks of material misstatement. For example, if your audit procedures result in you lowering your materiality level for a particular assertion, certain conditions that you previously did not consider to result in a risk of a material misstatement could be reassessed as risks of material misstatement.

1.24 The *risk of material misstatement* of the financial statements prior to the audit consists of the following two components:

- *Inherent risk* is the susceptibility of an assertion about a class of transaction, account balance, or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls (that is, assuming that there are no related controls). For example, the inherent risk of uncollectible accounts receivable might be high but such risk might be mitigated with effective controls over the granting of credit and the collection of outstanding accounts receivable.
- *Control risk* is the risk that a misstatement that could occur in an assertion about a class of transaction, account balance, or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented or detected and corrected on a timely basis by the entity's internal control.

(AU-C sec. 200 par. .14)

1.25 Inherent risk and control risk are the client's risks; that is, they exist independently of your audit. Thus, your risk assessment procedures help you better assess these client risks, but they do not alter the client's existing inherent or control risks. This guide refers to the *risk of material misstatement* as your combined assessment of inherent risk and control risk; however, you may make separate assessments of inherent risk and control risk.

Observations and Suggestions—Assessing Versus Testing Controls

There is a difference between assessing and testing controls. For example, say that you have assessed the controls as effective based on your review of their design and an observation that they have been implemented (that is, placed in operation). Based solely on that assessment, you would not necessarily have an adequate basis for considering control risk is low (or even moderate) as part of your audit strategy, as you would need further evidence of the effective operation of the controls through sufficient tests of controls to reach that conclusion.

Observations and Suggestions—The Audit Risk Model

Chapter 2 of this guide provides a model of audit risk (AR) in which:

$$AR = RMM \times DR$$

where RMM is the risk of material misstatement and DR is detection risk.

The risk of material misstatement is described as "the client's risk," which means that it is independent of your audit. You can control detection risk by changing the nature, timing, and extent of your substantive procedures. For example, to decrease the planned level of detection risk, you could perform more extensive and detailed analytical procedures and detailed substantive procedures, such as increasing sample sizes. Illustrations of how these risks can be managed to achieve a low overall audit risk can also be noted in table 4-2 in chapter 4, "Nonstatistical and Statistical Audit Sampling for Substantive Tests of Details," of the AICPA Audit Guide *Audit Sampling*.

You cannot control the risk of material misstatement as you can detection risk. The risk of material misstatement exists separately from your audit procedures. However, to properly control detection risk, you are required to assess the risk of material misstatement. The risk assessment process described in this guide is designed to allow you to gather information to assess the risk of material misstatement so you can design further audit procedures.

The Risk Assessment Process

1.26 You use your understanding of the client and its environment—which includes your evaluation of the design and implementation of internal control—to identify and assess the risks of material misstatement at the financial statement level and the relevant assertion level for classes of transactions, account balances, and disclosures. (AU-C sec. 315 par. .26) To make this assessment, you should

a. identify risk throughout the process of obtaining an understanding of the entity and its environment, including relevant controls that relate to the risks, by considering the classes of transactions, account balances, and disclosures in the financial statements;

b. assess the identified risks and evaluate whether they relate more pervasively to the financial statements as a whole and potentially to many assertions;

c. relate the identified risks to what could go wrong at the assertion level, considering relevant controls that you intend to test; and

d. consider the likelihood of misstatement and whether the potential misstatement is of a magnitude that could result in a material misstatement.

(AU-C sec. 315 par. .27)

Financial Statement Level and Assertion Level Risks

1.27 You should identify and assess the risks of material misstatement at both the financial statement level and the relevant assertion level for classes of transactions, account balances, and disclosures. (AU-C sec. 315 par. .26)

a. *Financial statement level risks and controls*. Some risks of material misstatement relate pervasively to the financial statements as a whole and potentially affect many relevant accounts and assertions. The risks at the financial statement level may be identifiable with specific assertions at the class of transaction, account balance or disclosure level. In this guide, we use the term *entity-level* *controls* to describe those controls that pertain to financial statement level risks.

b. *Relevant assertion level risks and controls*. Other risks of material misstatement relate to specific classes of transactions, account balances, and disclosures at the assertion level, for example, the valuation of a long-term unconditional promise to give in a not-for-profit organization. Your assessment of risk at the assertion level provides a basis for considering the appropriate audit approach for designing and performing further audit procedures, which include substantive procedures and may also include tests of controls. This guide uses the term *activity-level controls* to refer to the controls that pertain to assertion level risks.

Observations and Suggestions

You express an audit opinion on the financial statements *as a whole*, and the audit risk model describes audit risk for the overall financial statements (and for assertions). However, in executing the audit, you apply the audit risk model and assess risk at a more granular level, namely the assertion level. To accomplish this detailed level of risk assessment, you will consider what can be misstated in specific accounts, classes of transactions, and disclosures and their relevant assertions.

Risk that exists at the financial statement level, for example, those that pertain to a weak control environment or to management's process for making significant accounting estimates, should be related to specific assertions, if possible. For example, risk related to the client's process for making accounting estimates would affect those assertions where an accounting estimate was necessary (for example, the valuation of assets).

In other instances, it may not be possible for you to relate your financial statement level risk to a particular assertion or group of assertions. For example, it may not be possible for you to determine which assertions will or will not be affected by an overall weak control environment. Financial statement level risk such as a weak control environment that cannot be related to specific assertions often will require you to make an overall engagement response, such as the way in which the audit is staffed or supervised, or the timing of further audit procedures. It might also mean that risk might be assessed as high for many or all accounts and assertions.

Careful consideration of potential financial statement level risk during the brainstorming may indicate that there are cost-effective ways to limit your response to the risk. For example, a weak accounting function may only be a significant risk for unusual or new transactions or when new accounting standards are implemented. Effective accounting for routine transactions may be well evidenced. By focusing audit procedures on the points in the accounting process where these issues can create risk, a more cost- and risk-effective audit can be designed.

How to Consider Internal Control When Assessing Risks

1.28 Your evaluation of internal control design and the determination of whether controls have been implemented are integral components of the risk assessment process. When making risk assessments, you should identify the controls that are likely to either prevent, or detect and correct material misstatements in specific assertions. For example, procedures relating to the client's physical inventory count may relate specifically to the existence or completeness of inventory.

1.29 Individual controls often do not address a risk completely by themselves. Often, only multiple control activities, together with other components of internal control (for example, the control environment, risk assessment, information and communication, or monitoring), will be sufficient to address a risk. For this reason, when determining whether identified controls are likely to prevent or detect and correct material misstatements, you may organize your risk assessment procedures according to significant transactions and business processes, rather than general ledger accounts.

Identification of Significant Risks

1.30 Paragraph .04 of AU-C section 315 defines *significant risk* as follows: "A significant risk is an identified and assessed risk of material misstatement that, in the auditor's professional judgment, requires special audit consideration." (The defined term *significant risk* is italicized in this guide to remind readers of its definition and limited application.) As part of your risk assessment, you should determine whether any risks identified are, in your professional judgment, a *significant risk*. In making this judgment you exclude the effects of identified related controls (that is, assume there are no related controls). *Significant risks* are those that require special audit consideration. For example, because of the nature of your client and the industry in which it operates, you might determine that revenue recognition requires special audit consideration. For other clients, the valuation of intangible assets or the identification and required disclosure of related party transactions may be considered *significant risks*. Significant risk often arises with unusual transactions. Moreover, one or more *significant risks* arise on most audits. (Note: In practice, auditors may confuse significant risk with high risk. Not all high risks are *significant risks*. For example, the collectability of accounts receivable may be a high risk but not a *significant risk*; that is, no special audit consideration is required beyond extensive but customary substantive procedures of collectability.) (AU-C sec. 315 par. .28)

1.31 Special audit consideration for *significant risks* means you should

a. obtain an understanding of your client's controls relevant to that risk and, based on that understanding, evaluate the design of related controls, including relevant control activities, and determine whether they have been implemented. (AU-C sec. 315 par. .30)

b. perform other appropriate procedures that are linked clearly and responsive to the risk. Moreover, when your approach to *significant risks* consists *only* of substantive procedures, you should include tests of details.

   Substantive procedures related to *significant risks* should not be limited solely to analytical procedures. For other risks, effective analytical procedures alone may sometimes provide sufficient evidence.

   Note that if you *are* testing controls over *significant risks*, you may be able to limit your substantive procedures to only analytical procedures.

   (AU-C sec. 330 par. .22)

c. If you intend to rely on controls related to a *significant risk*, you should test the operating effectiveness of those controls in the current period. Reliance on tests of controls performed in a prior period is not appropriate for a *significant risk*. (AU-C sec. 330 par. .15)

d. Document those risks you have identified as *significant risks* (AU-C sec. 315 par. 33*d*).

1.32 The determination of *significant risks* is a matter for your professional judgment. In exercising that judgment, you should first consider only inherent risk and not control risk. Paragraphs 5.30–.37 of this guide provide more guidance on how to determine *significant risks*. (AU-C sec. 315 par. .29)

Responding to Assessed Risks

1.33 The risk assessment process culminates with your articulation of the account balances, classes of transactions, or disclosures where material misstatements are most likely to occur and how those misstatements may occur, given the unique circumstances of your client. This assessment of the risk of material misstatement, which relates identified risks to what can go wrong at the assertion level, provides a basis for designing and performing further audit procedures.

1.34 You perform further audit procedures to obtain the audit evidence necessary to support your audit opinion. Further audit procedures are defined as tests of controls and substantive procedures. Often, a combined approach using both tests of controls and substantive procedures is an effective approach.

1.35 In determining the nature, timing, and extent of further audit procedures, you should design and perform further audit procedures whose nature, timing, and extent are responsive to the assessed risks of material misstatement at the assertion level. You should provide a clear linkage between the risk assessments and the nature, timing, and extent of the further audit procedures. (AU-C sec. 330 par. .06)

1.36 Audit procedures performed in previous audits and suggested procedures provided by illustrative audit programs may help you understand the types of further audit procedures it is possible for you to perform. However, prior year procedures and example audit programs do not provide a sufficient basis for determining the nature, timing, and extent of audit procedures to perform in the current audit. Your assessment of the risks of material misstatement in the current period is the primary basis for designing further audit procedures in the current period.

Identification and Communication of Internal Control Matters

1.37 Your objective in an audit is to form an opinion on the client's financial statements as a whole. Your audit objective is not to identify all deficiencies in internal control, and you are not required to perform procedures to identify all deficiencies in internal control. Nevertheless, your application of audit procedures or communications with management or others may make you aware of deficiencies in the client's internal control. (AU-C sec. 265 par. .02)

1.38 A deficiency in internal control over financial reporting 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 and correct misstatements on a timely basis. (AU-C sec. 265 par. .07) You should evaluate the deficiencies in internal control you identify during the course of your audit and determine whether these deficiencies, individually or in combination, are significant deficiencies or material weaknesses. (AU-C sec. 265 par. .09) You are required to communicate in writing to management and those charged with governance those deficiencies in internal control that, in your judgment, constitute significant deficiencies or material weaknesses. (AU-C sec. 265 par. .11) Chapter 7 of this guide provides guidance on the evaluation and communication of deficiencies.

Audit Documentation

1.39 AU-C section 230, *Audit Documentation* (AICPA, *Professional Standards*), provides requirements that apply to the risk assessment process. Your audit documentation should be sufficient to enable an experienced auditor, having no previous connection to the audit, to understand

- the nature, timing, and extent of the audit procedures performed,
- the results of the audit procedures performed, and the evidence obtained, and
- the significant findings or issues, and conclusions reached, and professional judgments made.

Subsequent chapters of this guide illustrate the application of the audit documentation requirements.

(AU-C sec. 230 par. .08)

1.40 The form and extent of audit documentation is for you to determine using professional judgment. AU-C section 230 provides general guidance regarding the purpose, content, and ownership and confidentiality of audit documentation. Examples of common documentation techniques include narrative descriptions, questionnaires, checklists, and flowcharts. These techniques may be used alone or in combination.

1.41 The form and extent of your documentation are influenced by the following:

- The nature, size, and complexity of the entity, its controls, and its environment
- The availability of information from the entity
- The specific audit methodology and technology used in the course of the audit

Observations and Suggestions

For example, documentation of the understanding of a complex information system in which a large volume of transactions are electronically initiated, recorded, processed, or reported may include flowcharts, questionnaires, or decision tables. For an information system for which few transactions are processed (for example, long-term debt), documentation of the system in the form of a memorandum may be sufficient. In many cases, the more complex the entity and its environment, and the more extensive the audit procedures performed by the auditor, the more extensive your documentation should be.

The existence of good client documentation can also help reduce the extent of required audit documentation as you document your understanding of the controls. Where the client has good documentation, it can minimize the cost of producing audit documentation about entity processes through leveraging the existing documentation using references and focusing auditor documentation on the assessment of the controls over those processes.

You may relate your client's controls to objectives (for example, principles) and assertions for the most significant processes of an entity, regardless of the way control processes are documented by the client. By documenting your evaluation of controls using the concepts in the controls framework, you will more easily identify important gaps in control that are not fully addressed by the client's system of internal control. When your client directly relates their documentation to the terms and structure of an appropriate framework (for example, components, principles, and points of focus), savings in audit time can be achieved.

The specific audit methodology and technology used in the course of the audit will also affect the form and extent of documentation. For example, a firm may require the use of a risk matrix (for example, by account and by assertion) to summarize the elements of the risks of material misstatement. That may simplify the documentation and linkage process. Also, firms may require the use of electronic working papers and the use of active electronic links, which may facilitate the documentation process and navigation between working papers.

Summary

1.42 Illustration 1-2 summarizes the guidance provided in this chapter.

Chapters 3–6 of this guide provide more detailed guidance, examples, and illustrations of the overview material described in this chapter. To apply this guidance on your audit, you will need to have a working knowledge of key risk assessments and terms. The next chapter of this guide provides you with this knowledge.

Illustration 1-2
Summary of the Risk Assessment Process