

Statement on Auditing Standards No. 109

Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement

(Together with Statement on Auditing Standards No. 110, supersedes Statement on Auditing Standards No. 55, Consideration of Internal Control in a Financial Statement Audit, as amended, AICPA, Professional Standards.)

Contents of Statement

	<i>Paragraph</i>
Introduction	1-4
Risk Assessment Procedures and Sources of Information About the Entity and Its Environment, Including Its Internal Control	5-20
Risk Assessment Procedures	6-13
Discussion Among the Audit Team	14-20
Understanding the Entity and Its Environment, Including Its Internal Control	21-101
Industry, Regulatory, and Other External Factors	24-25
Nature of the Entity	26-28
Objectives and Strategies and Related Business Risks	29-33
Measurement and Review of the Entity's Financial Performance	34-39
Internal Control	40-101
Assessing the Risks of Material Misstatement	102-121
Significant Risks That Require Special Audit Consideration	110-116
Risks for Which Substantive Procedures Alone Do Not Provide Sufficient Appropriate Audit Evidence	117-120
Revision of Risk Assessment	121
Documentation	122-123
Effective Date	124
Appendix A: Understanding the Entity and Its Environment	
Appendix B: Internal Control Components	
Appendix C: Conditions and Events That May Indicate Risks of Material Misstatement	

1612 Risk Assessment Standards: SAS No. 104–SAS No. 111

Introduction

1. This Statement establishes standards and provides guidance about implementing the second standard of field work, as follows:

The auditor must obtain a sufficient understanding of the entity and its environment, including its internal control, to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures.

The importance of the auditor's risk assessment as a basis for further audit procedures is discussed in the explanation of audit risk in Statement on Auditing Standards (SAS) No. 107, *Audit Risk and Materiality in Conducting an Audit*. See SAS No. 106, *Audit Evidence*, for guidance on how the auditor uses relevant assertions¹ in sufficient detail to form a basis for the assessment of risks of material misstatement and to design and perform further audit procedures. The auditor should make risk assessments at the financial statement and relevant assertion levels based on an appropriate understanding of the entity and its environment, including its internal control. SAS No. 110, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*, discusses the auditor's responsibility to determine overall responses and to design and perform further audit procedures whose nature, timing, and extent are responsive to the risk assessments. This standard should be applied in conjunction with the standards and guidance provided in other SASs. In particular, the auditor's responsibility to consider fraud in an audit of financial statements is discussed in SAS No. 99, *Consideration of Fraud in a Financial Statement Audit*.

2. The following is an overview of this standard:

- *Risk assessment procedures and sources of information about the entity and its environment, including its internal control.* This section explains the audit procedures that the auditor should perform to obtain the understanding of the entity and its environment, including its internal control (risk assessment procedures). The audit team should discuss the susceptibility of the entity's financial statements to material misstatement.
- *Understanding the entity and its environment, including its internal control.* This section provides guidance to the auditor in understanding specified aspects of the entity and its environment, and components of its internal control, in order to identify and assess risks of material misstatement, and in designing and performing further audit procedures.
- *Assessing the risks of material misstatement.* This section provides guidance to the auditor in assessing the risks of material misstatement

¹ *Relevant assertions* are assertions that have a meaningful bearing on whether the account is fairly stated. For example, valuation may not be relevant to the cash account unless currency translation is involved; however, existence and completeness are always relevant. Similarly, valuation may not be relevant to the gross amount of the accounts receivable balance, but is relevant to the related allowance accounts. Additionally, the auditor might, in some circumstances, focus on the presentation and disclosure assertions separately in connection with the period-end financial reporting process.

Statement on Auditing Standards No. 109

1613

at the financial statement and relevant assertion levels. The auditor should:

- Identify risks by considering the entity and its environment, including relevant controls, and by considering the classes of transactions, account balances, and disclosures in the financial statements.
- Relate the identified risks to what could go wrong at the relevant assertion level.
- Consider the significance and the likelihood of material misstatement for each identified risk.

This section also provides guidance to the auditor in determining whether any of the assessed risks are significant risks that require special audit consideration or risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. The auditor should evaluate the design of the entity's controls, including relevant control activities, over such risks and determine whether they are adequate and have been implemented.

- *Documentation.* This section provides related documentation guidance.

3. Obtaining an understanding of the entity and its environment is an essential aspect of performing an audit in accordance with generally accepted auditing standards. In particular, that understanding establishes a frame of reference within which the auditor plans the audit and exercises professional judgment about assessing risks of material misstatement of the financial statements and responding to those risks throughout the audit, for example when:

- Establishing materiality for planning purposes and evaluating whether that judgment remains appropriate as the audit progresses.
- Considering the appropriateness of the selection and application of accounting policies and the adequacy of financial statement disclosures.
- Identifying areas where special audit consideration may be necessary, for example, related-party transactions, the appropriateness of management's use of the going-concern assumption, complex or unusual transactions, or considering the business purpose of transactions.
- Developing expectations for use when performing analytical procedures.
- Designing and performing further audit procedures to reduce audit risk to an appropriately low level.
- Evaluating the sufficiency and appropriateness of audit evidence obtained, such as evidence related to the reasonableness of management's assumptions and of management's oral and written representations.

4. The auditor should use professional judgment to determine the extent of the understanding required of the entity and its environment, including its internal control. The auditor's primary consideration is whether the understanding that has been obtained is sufficient to assess risks of material misstatement of the financial statements and to design and perform further audit procedures. The depth of the overall understanding that the auditor obtains in performing the audit is less than that possessed by management in managing the entity.

AU §RAS

1614 Risk Assessment Standards: SAS No. 104–SAS No. 111**Risk Assessment Procedures and Sources of Information About the Entity and Its Environment, Including Its Internal Control**

5. Obtaining an understanding of the entity and its environment, including its internal control, is a continuous, dynamic process of gathering, updating, and analyzing information throughout the audit. Throughout this process, the auditor should also follow the guidance in SAS No. 99. As described in SAS No. 106, audit procedures to obtain the understanding are referred to as *risk assessment procedures* because some of the information obtained by performing such procedures may be used by the auditor as audit evidence to support assessments of the risks of material misstatement. In addition, in performing risk assessment procedures, the auditor may obtain audit evidence about the relevant assertions related to classes of transactions, account balances, or disclosures and about the operating effectiveness of controls, even though such audit procedures were not specifically planned as substantive procedures or as tests of controls. The auditor also may choose to perform substantive procedures or tests of controls concurrently with risk assessment procedures because it is efficient to do so.

Risk Assessment Procedures

6. The auditor should perform the following risk assessment procedures to obtain an understanding of the entity and its environment, including its internal control:

- a. Inquiries of management and others within the entity
- b. Analytical procedures
- c. Observation and inspection

The auditor is not required to perform all the risk assessment procedures described above for each aspect of the understanding described in paragraph 21. However, all the risk assessment procedures should be performed by the auditor in the course of obtaining the required understanding.

7. In addition, the auditor might perform other procedures where the information obtained may be helpful in identifying risks of material misstatement. For example, in cooperation with the entity, the auditor may consider making inquiries of others outside the entity such as the entity's external legal counsel or of valuation experts that the entity has used. Reviewing information obtained from external sources such as reports by analysts, banks, or rating agencies; trade and economic journals; or regulatory or financial publications may also be useful in obtaining information about the entity.

8. Although much of the information the auditor obtains by inquiries can be obtained from management and those responsible for financial reporting, inquiries of others within the entity, such as production and internal audit personnel, and other employees with different levels of authority, may be useful in providing the auditor with a different perspective in identifying risks of material misstatement. In determining others within the entity to whom inquiries may be directed, or the extent of those inquiries, the auditor should

AU §RAS

Statement on Auditing Standards No. 109

1615

consider what information may be obtained that might help the auditor in identifying risks of material misstatement. For example:

- Inquiries directed toward those charged with governance² may help the auditor understand the environment in which the financial statements are prepared.
- Inquiries directed toward internal audit personnel may relate to their activities concerning the design and effectiveness of the entity's internal control and whether management has satisfactorily responded to any findings from these activities.
- Inquiries of employees involved in initiating, authorizing, processing, or recording complex or unusual transactions may help the auditor in evaluating the appropriateness of the selection and application of certain accounting policies.
- Inquiries directed toward in-house legal counsel may relate to such matters as litigation, compliance with laws and regulations, knowledge of fraud or suspected fraud affecting the entity, warranties, post-sales obligations, arrangements (such as joint ventures) with business partners, and the meaning of contract terms.
- Inquiries directed toward marketing, sales, or production personnel may relate to changes in the entity's marketing strategies, sales trends, production strategies, or contractual arrangements with its customers.

9. Paragraphs 4 and 6 of SAS No. 56, *Analytical Procedures*, specify that the auditor should apply analytical procedures in planning the audit to assist in understanding the entity and its environment and to identify areas that may represent specific risks relevant to the audit. For example, analytical procedures may be helpful in identifying the existence of unusual transactions or events, and amounts, ratios, and trends that might indicate matters that have financial statement and audit implications. In performing analytical procedures as risk assessment procedures, the auditor should develop expectations about plausible relationships that are reasonably expected to exist. When comparison of those expectations with recorded amounts or ratios developed from recorded amounts yields unusual or unexpected relationships, the auditor should consider those results in identifying risks of material misstatement. However, when such analytical procedures use data aggregated at a high level (which is often the situation), the results of those analytical procedures provide only a broad initial indication about whether a material misstatement may exist. Accordingly, the auditor should consider the results of such analytical procedures along with other information gathered in identifying the risks of material misstatement.

10. Observation and inspection may support inquiries of management and others, and also provide information about the entity and its environment. Such audit procedures ordinarily include:

- Observation of entity activities and operations
- Inspection of documents (such as business plans and strategies), records, and internal control manuals

² See footnote 4 of Statement on Auditing Standards (SAS) No. 108, *Planning and Supervision*, for the definition of and discussion about those charged with governance.

1616 Risk Assessment Standards: SAS No. 104–SAS No. 111

- Reading reports prepared by management (such as quarterly management reports and interim financial statements), those charged with governance (such as minutes of board of directors' meetings), and internal audit
- Visits to the entity's premises and plant facilities
- Tracing transactions through the information system relevant to financial reporting, which may be performed as part of a walk-through

11. When the auditor intends to use information about the entity and its environment obtained in prior periods, the auditor should determine whether changes have occurred that may affect the relevance of such information in the current audit. For continuing engagements, the auditor's previous experience with the entity contributes to the understanding of the entity. For example, audit procedures performed in previous audits ordinarily provide audit evidence about the entity's organizational structure, business, and controls, as well as information about past misstatements and whether or not they were corrected on a timely basis, which assists the auditor in assessing risks of material misstatement in the current audit. However, such information may have been rendered irrelevant by changes in the entity or its environment. The auditor should make inquiries and perform other appropriate audit procedures, such as walk-throughs of systems, to determine whether changes have occurred that may affect the relevance of such information.

12. SAS No. 99 specifies that the auditor should specifically assess the risk of material misstatement³ of the financial statements due to fraud and states that the auditor should consider that assessment in designing audit procedures to be performed. In making this assessment, the auditor should also consider fraud risk factors that relate to either material misstatements arising from fraudulent financial reporting or misstatements arising from misappropriation of assets. Fraud risk factors that relate to fraudulent financial reporting are (a) management's characteristics and influence over the control environment, (b) industry conditions, and (c) operating characteristics and financial stability. Fraud risk factors that relate to misappropriation of assets are (a) susceptibility of assets to misappropriations and (b) absence of controls. The auditor's response to the assessment of the risk of material misstatement due to fraud is influenced by the nature and significance of the risk factors identified as being present. In some circumstances, the auditor may conclude that the conditions indicate a need to modify audit procedures. In these circumstances, the auditor should consider whether the assessment of the risk of material misstatement due to fraud calls for an overall response, one that is specific to a particular account balance, class of transactions, or disclosures at the relevant assertion level, or both. However, since such risk factors do not necessarily indicate the existence of fraud, the results of the assessment of the risk of material misstatement due to fraud provide only a broad initial indication about whether a material misstatement due to fraud may exist. Accordingly, the auditor should consider the results of the assessment of the risk of material misstatement due to fraud performed during planning along with other information gathered in identifying the risks of material misstatements.

13. When relevant to the audit, the auditor also should consider other information such as that obtained from the auditor's client acceptance or

³ Risk of material misstatement is described as the auditor's combined assessment of inherent risk and control risk. See paragraph 22 of SAS No. 107, *Audit Risk and Materiality in Conducting an Audit*, for the definition of and further discussion about risk of material misstatement.

Statement on Auditing Standards No. 109

1617

continuance process or, where practicable, experience gained on other engagements performed for the entity, for example, engagements to review interim financial information.

Discussion Among the Audit Team

14. The members of the audit team, including the auditor with final responsibility for the audit, should discuss the susceptibility of the entity's financial statements to material misstatements. This discussion could be held concurrently with the discussion among the audit team that is specified by SAS No. 99 to discuss the susceptibility of the entity's financial statements to fraud. When the entire engagement is performed by a single auditor, the auditor should consider and document the susceptibility of the entity's financial statements to material misstatements. In these circumstances, the auditor should consider other factors that may be necessary in the engagement, such as personnel possessing specialized skills.

15. Professional judgment should be used to determine which members of the audit team should be included in the discussion, how and when it should occur, and the extent of the discussion. Key members of the audit team, including the auditor with final responsibility, should be involved in the discussion; however, it is not necessary for all team members to have a comprehensive knowledge of all aspects of the audit. The extent of the discussion is influenced by the roles, experience, and information needs of the audit team members. An additional consideration is whether to include specialists assigned to the audit team. For example, the auditor may determine that a professional possessing information technology (IT)⁴ or other specialized skills is needed on the audit team and therefore include that individual in the discussion.

16. The auditor with final responsibility should consider which matters are to be communicated to members of the engagement not involved in the discussion. In a multilocation audit, for example, there may be multiple discussions that involve the key members of the audit team in each significant location.

17. The objective of this discussion⁵ is for members of the audit team to gain a better understanding of the potential for material misstatements of the financial statements resulting from fraud or error in the specific areas assigned to them, and to understand how the results of the audit procedures that they perform may affect other aspects of the audit, including the decisions about the nature, timing, and extent of further audit procedures.

18. The discussion provides an opportunity for more experienced team members, including the auditor with final responsibility for the audit, to share their insights based on their knowledge of the entity and for the team members to exchange information about the business risks⁶ to which the entity is subject and about how and where the financial statements might be susceptible to material misstatement. As specified in SAS No. 99, particular emphasis should be given to the susceptibility of the entity's financial statements to material

⁴ Information technology (IT) encompasses automated means of originating, processing, storing, and communicating information, and includes recording devices, communication systems, computer systems (including hardware and software components and data), and other electronic devices. An entity's use of IT may be extensive; however, the auditor is primarily interested in the entity's use of IT to initiate, authorize, record, process, and report transactions or other financial data.

⁵ There may be one or more discussions, depending on the circumstances of the engagement.

⁶ See paragraphs 29 through 33.

1618 Risk Assessment Standards: SAS No. 104–SAS No. 111

misstatement due to fraud. In addition, the audit team should discuss critical issues, such as areas of significant audit risk; areas susceptible to management override of controls; unusual accounting procedures used by the client; important control systems; materiality at the financial statement level and at the account level; and how materiality will be used to determine the extent of testing. The discussion should also address application of generally accepted accounting principles to the entity's facts and circumstances and in light of the entity's accounting policies.

19. The auditor should plan and perform the audit with an attitude of professional skepticism. The discussion among the audit team members should emphasize the need to exercise professional skepticism throughout the engagement, to be alert for information or other conditions that indicate that a material misstatement due to fraud or error may have occurred, and to be rigorous in following up on such indications.

20. Depending on the circumstances of the audit, there may be multiple discussions in order to facilitate the ongoing exchange of information between audit team members regarding the susceptibility of the entity's financial statements to material misstatements. The purpose is for audit team members to communicate and share information obtained throughout the audit that may affect the assessment of the risks of material misstatement due to fraud or error or the audit procedures performed to address the risks.

Understanding the Entity and Its Environment, Including Its Internal Control

21. The auditor's understanding of the entity and its environment consists of an understanding of the following aspects:

- a. Industry, regulatory, and other external factors
- b. Nature of the entity
- c. Objectives and strategies and the related business risks that may result in a material misstatement of the financial statements
- d. Measurement and review of the entity's financial performance
- e. Internal control, which includes the selection and application of accounting policies

22. Appendix A contains examples of matters that the auditor may consider in obtaining an understanding of the entity and its environment relating to categories (a) through (d) above. Appendix B contains a detailed explanation of the internal control components.

23. The nature, timing, and extent of the risk assessment procedures performed depend on the circumstances of the engagement, such as the size and complexity of the entity and the auditor's experience with it. In addition, identifying significant changes in any of the above aspects of the entity from prior periods is particularly important in gaining a sufficient understanding of the entity to identify and assess risks of material misstatement.

Industry, Regulatory, and Other External Factors

24. The auditor should obtain an understanding of relevant industry, regulatory, and other external factors. These factors include industry conditions, such as the competitive environment, supplier and customer relationships, and technological developments; the regulatory environment encompassing, among other matters, relevant accounting pronouncements, the legal and political

AU §RAS

Statement on Auditing Standards No. 109**1619**

environment, and environmental requirements affecting the industry and the entity; and other external factors, such as general economic conditions.⁷

25. The industry in which the entity operates may be subject to specific risks of material misstatement arising from the nature of the business, the degree of regulation, or other external forces (such as political, economic, social, technical, and competitive). For example, long-term contracts may involve significant estimates of revenues and costs that give rise to risks of material misstatement of the financial statements. Similarly, regulations may specify certain financial reporting requirements for the industry in which the entity operates. In such cases, the auditor should consider whether the audit team includes members with sufficient relevant knowledge and experience. If management fails to comply with such regulations, its financial statements may be materially misstated.

Nature of the Entity

26. The auditor should obtain an understanding of the nature of the entity. The nature of an entity refers to the entity's operations, its ownership, governance, the types of investments that it is making and plans to make, the way that the entity is structured, and how it is financed. An understanding of the nature of an entity enables the auditor to understand the classes of transactions, account balances, and disclosures to be expected in the financial statements.

27. The entity may have a complex structure with subsidiaries or other components in multiple locations. In addition to the difficulties of consolidation in such cases, other issues with complex structures that may give rise to risks of material misstatement include the allocation of goodwill to subsidiaries, and its impairment; whether investments are joint ventures, subsidiaries, or investments accounted for using the equity method; and whether special-purpose entities are accounted for appropriately.

28. An understanding of the ownership, management, and other key personnel and their relations between owners and other people or entities is also important in determining whether related-party transactions have been identified and accounted for appropriately. SAS No. 45, *Related Parties*, provides additional guidance on the auditor's considerations relevant to related parties.

Objectives and Strategies and Related Business Risks

29. The auditor should obtain an understanding of the entity's objectives and strategies, and the related business risks that may result in material misstatement of the financial statements. The entity conducts its business in the context of industry, regulatory, and other internal and external factors. To respond to these factors, the entity's management or those charged with governance define objectives, which are the overall plans for the entity. Strategies are the operational approaches by which management intends to achieve its objectives. Business risks result from significant conditions, events, circumstances, actions, or inactions that could adversely affect the entity's ability to achieve its objectives and execute its strategies, or through the setting of inappropriate objectives and strategies. Just as the external environment changes, the conduct of the entity's business is also dynamic and the entity's strategies and objectives change over time.

⁷ See SAS No. 54, *Illegal Acts by Clients*, for additional requirements related to the legal and regulatory framework applicable to the entity and the industry.

1620 Risk Assessment Standards: SAS No. 104–SAS No. 111

30. Business risk is broader than the risk of material misstatement of the financial statements, although it includes the latter. For example, a new entrant to the marketplace with the competitive advantage of brand recognition and economies of scale may represent a business risk to a manufacturer's ability to garner as much shelf space at retailers and compete on price. The potential risk of material misstatement of the financial statements related to such business risk might be obsolescence or overproduction of inventory that could only be sold at discounted amounts. Business risk particularly may arise from change or complexity, although a failure to recognize the need for change may also give rise to risk. Change may arise, for example, from the development of new products that may fail; from an inadequate market, even if successfully developed; or from flaws that may result in liabilities and reputation risk. As an example of complexity, the conduct and management of long-term engineering projects (such as ship construction or the building of a suspension bridge) give rise to risks in the areas of percentage of completion, pricing, costing, design, and performance control. An understanding of business risks increases the likelihood of identifying risks of material misstatement. However, the auditor does not have a responsibility to identify or assess all business risks.

31. Most business risks will eventually have financial consequences and, therefore, an effect on the financial statements. However, not all business risks give rise to risks of material misstatement. A business risk may have an immediate consequence for the risk of misstatement for classes of transactions, account balances, or disclosures at the relevant assertion level or for the financial statements taken as a whole. For example, the business risk arising from a contracting customer base due to industry consolidation may increase the risk of misstatement associated with the valuation of accounts receivable. Similarly, a business risk may have an immediate consequence for the risk of misstatement of the financial statements taken as a whole. For example, the business risk of significant transactions with related parties may increase the risk of misstatement of a range of significant account balances and relevant assertions. Furthermore, a business objective and related risks may also have a longer-term consequence that the auditor may need to consider when assessing the appropriateness of the going concern assumption. For example, the business risk of a decline in the industry in which the entity operates may affect the entity's ability to continue as a going concern. The auditor's consideration of whether a business risk may result in material misstatement is, therefore, made in light of the entity's circumstances. Examples of conditions and events that may indicate risks of material misstatement are given in Appendix C.

32. Usually management identifies business risks and develops approaches to address them. Such a risk assessment process is part of internal control and is discussed in paragraphs 76 to 80.

33. Smaller entities often do not set their objectives and strategies, or manage the related business risks, through formal plans or processes. In many cases there may be no documentation of such matters. In such entities, the auditor's understanding may be obtained through inquiries of management and observation of how the entity responds to such matters.

Measurement and Review of the Entity's Financial Performance

34. The auditor should obtain an understanding of the measurement and review of the entity's financial performance. Performance measures and their review indicate to the auditor aspects of the entity's performance that

AU §RAS

Statement on Auditing Standards No. 109

1621

management and others consider to be important. Performance measures, whether external or internal, create pressures on the entity that, in turn, may motivate management to take action to improve the business performance or to misstate the financial statements. Obtaining an understanding of the entity's performance measures assists the auditor in considering whether such pressures result in management actions that may have increased the risks of material misstatement.

35. Management's measurement and review of the entity's financial performance is to be distinguished from the monitoring of controls (discussed as a component of internal control in paragraphs 97 through 101), although their purposes may overlap. Monitoring of controls, however, is specifically concerned with the effective operation of internal control through consideration of information about the controls. The measurement and review of performance is directed at whether business performance is meeting the objectives set by management (or third parties), but it may be that performance indicators also provide information that enables management to identify deficiencies in internal control.

36. Internally generated information used by management for this purpose may include key performance indicators (financial and nonfinancial); budgets; variance analysis; subsidiary information and divisional, departmental, or other level performance reports; and comparisons of an entity's performance with that of competitors. External parties may also measure and review the entity's financial performance. For example, external information, such as analysts' reports and credit rating agency reports, may provide information useful to the auditor's understanding of the entity and its environment. Such reports may be obtained from the entity being audited or from Web sites.

37. Internal measures may highlight unexpected results or trends requiring management's inquiry of others in order to determine their cause and take corrective action (including, in some cases, the detection and correction of misstatements on a timely basis). Performance measures may also indicate to the auditor a risk of misstatement of related financial statement information. For example, performance measures may indicate that the entity has unusually rapid growth or profitability when compared to that of other entities in the same industry. Such information, particularly if combined with other factors such as performance-based bonus or incentive remuneration, may indicate the potential risk of management bias in the preparation of the financial statements.

38. Much of the information used in performance measurement may be produced by the entity's information system. If management assumes that data used for reviewing the entity's performance is accurate without having a basis for that assumption, errors may exist in the information, potentially leading management to incorrect conclusions about performance. When the auditor intends to make use of the performance measures for the purpose of the audit (for example, for analytical procedures), the auditor should consider whether the information related to management's review of the entity's performance provides a reliable basis and is sufficiently precise for such a purpose. If making use of performance measures, the auditor should consider whether they are precise enough to detect material misstatements.

39. Smaller entities ordinarily do not have formal processes to measure and review the entity's financial performance. Management nevertheless often relies on certain key indicators that knowledge and experience of the business suggest are reliable bases for evaluating financial performance and taking appropriate action.

AU §RAS

1622 Risk Assessment Standards: SAS No. 104–SAS No. 111**Internal Control⁸**

40. The auditor should obtain an understanding of the five components of internal control sufficient to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures. The auditor should obtain a sufficient understanding by performing risk assessment procedures to evaluate the design of controls relevant to an audit of financial statements and to determine whether they have been implemented. The auditor should use such knowledge to:

- Identify types of potential misstatements.
- Consider factors that affect the risks of material misstatement.
- Design tests of controls, when applicable, and substantive procedures.

41. Internal control⁹ is a process—effected by those charged with governance, management, and other personnel—designed to provide reasonable assurance about the achievement of the entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations.¹⁰ Internal control over safeguarding of assets against unauthorized acquisition, use, or disposition may include controls relating to financial reporting and operations objectives. Internal control consists of five interrelated components:

- a. *Control environment* sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- b. Entity's *risk assessment* is the entity's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.
- c. *Information and communication systems* support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- d. *Control activities* are the policies and procedures that help ensure that management directives are carried out.
- e. *Monitoring* is a process that assesses the quality of internal control performance over time.

Appendix B contains a detailed discussion of the internal control components.

42. The division of internal control into the five components provides a useful framework for auditors to consider how different aspects of an entity's internal control may affect the audit. The division does not necessarily reflect how an entity considers and implements internal control. Also, the auditor's primary consideration is whether, and how, a specific control prevents, or detects and corrects, material misstatements in relevant assertions related to classes of transactions, account balances, or disclosures, rather than its classification into any particular component. Accordingly, auditors may use different terminology or frameworks to describe the various aspects of internal control,

⁸ This section recognizes the definition and description of internal control contained in *Internal Control—Integrated Framework*, published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO Report).

⁹ Internal control also may be referred to as internal control structure.

¹⁰ It follows that internal control is designed and effected to address business risks that threaten the achievement of any of these objectives.

Statement on Auditing Standards No. 109

1623

and their effect on the audit, than those used in this Statement, provided all the components described in this Statement are addressed.

43. The way in which internal control is designed and implemented varies with an entity's size and complexity. Specifically, smaller entities may use less formal means and simpler processes and procedures to achieve their objectives. For example, smaller entities with active management involvement in the financial reporting process may not have extensive descriptions of accounting procedures or detailed written policies. For some entities, in particular very small entities, the owner-manager¹¹ may perform functions that in a larger entity would be regarded as belonging to several of the components of internal control. Therefore, the components of internal control may not be clearly distinguished within smaller entities, but their underlying purposes are equally valid.

44. The auditor should obtain an understanding of the entity's selection and application of accounting policies and should consider whether they are appropriate for its business and consistent with generally accepted accounting principles and accounting policies used in the relevant industry,¹² or with a comprehensive basis of accounting other than generally accepted accounting principles.¹³ The understanding encompasses the methods the entity uses to account for significant and unusual transactions; the effect of significant accounting policies in controversial or emerging areas for which there is a lack of authoritative guidance or consensus; and changes in the entity's accounting policies. The auditor should also identify financial reporting standards and regulations that are new to the entity and consider when and how the entity will adopt such requirements. Where the entity has changed its selection of or method of applying a significant accounting policy, the auditor should consider the reasons for the change and whether it is appropriate and consistent with generally accepted accounting principles.

45. The presentation of financial statements in conformity with generally accepted accounting principles should include adequate disclosure of material matters. These matters relate to the form, arrangement, and content of the financial statements and their appended notes, including, for example, the terminology used, the amount of detail given, the classification of items in the statements, and the bases of amounts set forth. The auditor should consider whether the entity has disclosed a particular matter appropriately in light of the circumstances and facts of which the auditor is aware at the time.

46. For the purposes of this Statement, the term *internal control* encompasses all five components of internal control stated above. In addition, the term *controls* refers to one or more of the components, or any aspect thereof.

Controls Relevant to Reliable Financial Reporting and to the Audit

47. There is a direct relationship between an entity's objectives and the internal control components it implements to provide reasonable assurance about their achievement. In addition, internal control is relevant to the entire

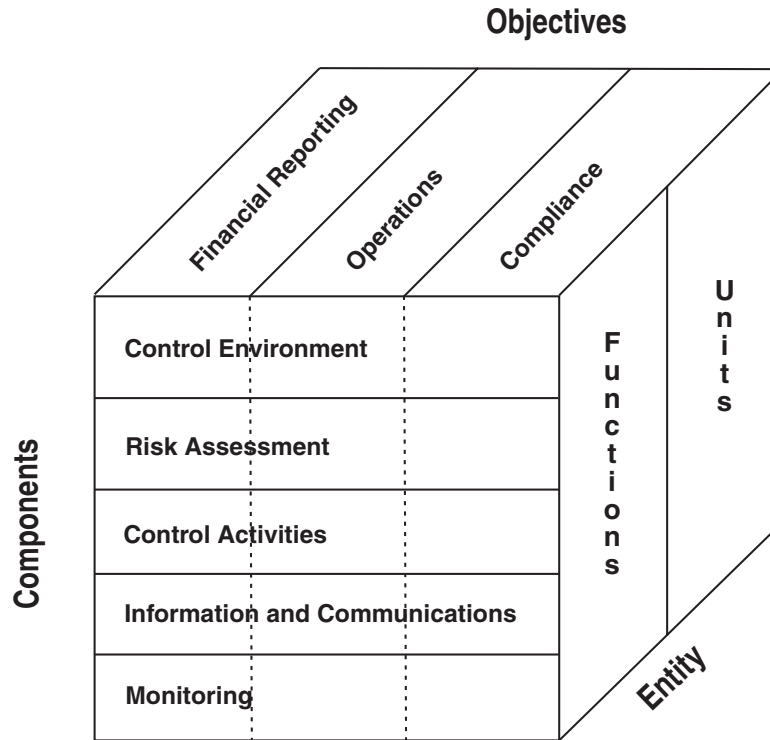
¹¹ This Statement uses the term *owner-manager* to indicate proprietors of entities who are involved in the running of the entity on a day-to-day basis.

¹² See SAS No. 69, *The Meaning of Present Fairly in Conformity With Generally Accepted Accounting Principles*, as amended.

¹³ The term *comprehensive basis of accounting other than generally accepted accounting principles* is defined in SAS No. 62, *Special Reports*, as amended. Hereafter, reference to generally accepted accounting principles in this Statement includes, where applicable, an other comprehensive basis of accounting.

1624 Risk Assessment Standards: SAS No. 104–SAS No. 111

entity, or to any of its operating units or business functions. This relationship is depicted as follows:



Although the entity's objectives, and therefore controls, relate to financial reporting, operations, and compliance, as referred to in paragraph 41, not all of these objectives and controls are relevant to the audit. Further, although internal control applies to the entire entity, or to any of its operating units or business functions, an understanding of internal control relating to each of the entity's operating units and business functions may not be necessary to the performance of the audit.

48. Ordinarily, controls that are relevant to an audit pertain to the entity's objective of preparing financial statements that are fairly presented in conformity with generally accepted accounting principles, including the management of risk that may give rise to a risk of material misstatement in those financial statements. However, it is not necessary to assess all controls in connection with assessing the risks of material misstatement and designing and performing further audit procedures in response to assessed risks. It is a matter of the auditor's professional judgment, as to the controls or combination of controls that should be assessed. However, as stated in paragraph 115, for significant risks, to the extent the auditor has not already done so, the auditor should evaluate the design of the entity's related controls, including relevant control activities, and determine whether they have been implemented. In exercising that judgment, the auditor should consider the circumstances, the applicable component, and factors such as the following:

- Materiality.
- The size of the entity.

AU §RAS

Statement on Auditing Standards No. 109

1625

- The nature of the entity's business, including its organization and ownership characteristics.
- The diversity and complexity of the entity's operations.
- Applicable legal and regulatory requirements.
- The nature and complexity of the systems that are part of the entity's internal control, including the use of service organizations.

49. Controls over the completeness and accuracy of information produced by the entity may also be relevant to the audit if the auditor intends to make use of the information in designing and performing further audit procedures. The auditor's previous experience with the entity and information obtained in understanding the entity and its environment and throughout the audit assist the auditor in identifying controls relevant to the audit.

50. Controls relating to operations and compliance¹⁴ objectives may, however, be relevant to an audit if they pertain to information or data the auditor may evaluate or use in applying audit procedures. For example, controls pertaining to nonfinancial data that the auditor may use in analytical procedures, such as production statistics, or controls pertaining to detecting noncompliance with laws and regulations that may have a direct and material effect on the financial statements, such as controls over compliance with income tax laws and regulations used to determine the income tax provision, may be relevant to an audit.

51. An entity generally has controls relating to objectives that are not relevant to an audit and therefore need not be considered. For example, an entity may rely on a sophisticated system of automated controls to provide efficient and effective operations (such as a manufacturing plant's computerized production scheduling system), but these controls ordinarily would not be relevant to the audit.

52. Internal control over safeguarding of assets against unauthorized acquisition, use, or disposition may include controls relating to financial reporting and operations objectives. In obtaining an understanding of each of the components of internal control, the auditor's consideration of safeguarding controls is generally limited to those relevant to the reliability of financial reporting. For example, use of access controls, such as passwords, that limit access to the data and programs that process cash disbursements may be relevant to a financial statement audit. Conversely, safeguarding controls relating to operations objectives, such as controls to prevent the excessive use of materials in production, generally are not relevant to a financial statement audit.

53. Controls relevant to the audit may exist in any of the components of internal control and a further discussion of controls relevant to the audit is included under the heading of each internal control component below (see paragraphs 67 through 101). In addition, paragraphs 115 and 117 discuss certain risks for which the auditor should evaluate the design of the entity's controls over such risks and determine whether they have been implemented.

Depth of Understanding of Internal Control

54. Obtaining an understanding of internal control involves evaluating the design of a control and determining whether it has been implemented.

¹⁴ An auditor may need to consider controls relevant to compliance objectives when performing an audit in accordance with SAS No. 74, *Compliance Auditing Considerations in Audits of Governmental Entities and Recipients of Governmental Financial Assistance*.

1626 Risk Assessment Standards: SAS No. 104–SAS No. 111

Evaluating the design of a control involves considering whether the control, individually or in combination with other controls, is capable of effectively preventing or detecting and correcting material misstatements. Further explanation is contained in the discussion of each internal control component below (see paragraphs 67 through 101). Implementation of a control means that the control exists and that the entity is using it. The auditor should consider the design of a control in determining whether to consider its implementation. An improperly designed control may represent a material weakness¹⁵ in the entity's internal control and the auditor should consider whether to communicate this to those charged with governance and management.

55. As stated in paragraph 6, the auditor should perform risk assessment procedures to obtain an understanding of internal control. Procedures to obtain audit evidence about the design and implementation of relevant controls may include inquiring of entity personnel, observing the application of specific controls, inspecting documents and reports, and tracing transactions through the information system relevant to financial reporting. Inquiry alone is not sufficient to evaluate the design of a control relevant to an audit and to determine whether it has been implemented.

56. Obtaining an understanding of an entity's controls is not sufficient to serve as testing the operating effectiveness of controls, unless there is some automation¹⁶ that provides for the consistent application of the operation of the control (manual and automated elements of internal control relevant to the audit are further described below). For example, obtaining audit evidence about the implementation of a manually operated control at a point in time does not provide audit evidence about the operating effectiveness of the control at other times during the period under audit. However, IT enables an entity to process large volumes of data consistently and enhances the entity's ability to monitor the performance of control activities and to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems. Therefore, because generally, IT processing is inherently consistent, performing audit procedures to determine whether an automated control has been implemented may serve as a test of that control's operating effectiveness, depending on the auditor's assessment and testing of IT general controls, including computer security and program change control. Tests of the operating effectiveness of controls are further described in SAS No. 110.

Characteristics of Manual and Automated Elements of Internal Control Relevant to the Auditor's Risk Assessment

57. *Effect of information technology on internal control.* An entity's use of IT may affect any of the five components of internal control relevant to the achievement of the entity's financial reporting, operations, or compliance objectives, and its operating units or business functions. For example, an entity may use IT as part of discrete systems that support only particular business units, functions, or activities, such as a unique accounts receivable system for a particular business unit or a system that controls the operation of factory equipment. Alternatively, an entity may have complex, highly integrated systems that share data and that are used to support all aspects of the entity's financial reporting, operations, and compliance objectives.

¹⁵ 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.

¹⁶ This is assuming effective IT general controls.

Statement on Auditing Standards No. 109

1627

58. The use of IT also affects the fundamental manner in which transactions are initiated, authorized, recorded, processed, and reported.¹⁷ In a manual system, an entity uses manual procedures and records in paper format (for example, individuals may manually record sales orders on paper forms or journals, authorize credit, prepare shipping reports and invoices, and maintain accounts receivable records). Controls in such a system also are manual and may include such procedures as approvals and reviews of activities, and reconciliations and follow-up of reconciling items. Alternatively, an entity may have information systems that use automated procedures to initiate, authorize, record, process, and report transactions, in which case records in electronic format replace such paper documents as purchase orders, invoices, shipping documents, and related accounting records. Controls in systems that use IT consist of a combination of automated controls (for example, controls embedded in computer programs) and manual controls. Further, manual controls may be independent of IT, may use information produced by IT, or may be limited to monitoring the effective functioning of IT and of automated controls, and to handling exceptions. When IT is used to initiate, authorize, record, process, or report transactions, or other financial data for inclusion in financial statements, the systems and programs may include controls related to the corresponding assertions for material accounts or may be critical to the effective functioning of manual controls that depend on IT. An entity's mix of manual and automated controls varies with the nature and complexity of the entity's use of IT.

59. Generally, IT provides potential benefits of effectiveness and efficiency for an entity's internal control because it enables an entity to:

- Consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data.
- Enhance the timeliness, availability, and accuracy of information.
- Facilitate the additional analysis of information.
- Enhance the ability to monitor the performance of the entity's activities and its policies and procedures.
- Reduce the risk that controls will be circumvented.
- Enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems.

60. IT also poses specific risks to an entity's internal control, including:

- Reliance on systems or programs that are processing data inaccurately, processing inaccurate data, or both.
- Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions or inaccurate recording of transactions.
- Unauthorized changes to data in master files.
- Unauthorized changes to systems or programs.
- Failure to make necessary changes to systems or programs.
- Inappropriate manual intervention.
- Potential loss of data or inability to access data as required.

¹⁷ Paragraph 9 of Appendix B defines *initiation, authorizing, recording, processing, and reporting* as used throughout this Statement.

1628 Risk Assessment Standards: SAS No. 104–SAS No. 111

61. The extent and nature of these risks to internal control vary depending on the nature and characteristics of the entity's information system. For example, multiple users, either external or internal, may access a common database of information that affects financial reporting. In such circumstances, a lack of control at a single user entry point might compromise the security of the entire database, potentially resulting in improper changes to or destruction of data. When IT personnel or users are given, or can gain, access privileges beyond those necessary to perform their assigned duties, a breakdown in segregation of duties can occur. This could result in unauthorized transactions or changes to programs or data that affect the financial statements. Therefore, the nature and characteristics of an entity's use of IT in its information system affect the entity's internal control.

62. Manual controls of systems may be more suitable where judgment and discretion are required, such as for the following circumstances:

- Large, unusual, or nonrecurring transactions.
- Circumstances where misstatements are difficult to define, anticipate, or predict.
- In changing circumstances that require a control response outside the scope of an existing automated control.
- In monitoring the effectiveness of automated controls.

63. Manual controls are performed by people, and therefore pose specific risks to the entity's internal control. Manual controls may be less reliable than automated controls because they can be more easily bypassed, ignored, or overridden and they are also more prone to errors and mistakes. Consistency of application of a manual control element cannot therefore be assumed. Manual systems may be less suitable for the following:

- High volume or recurring transactions, or in situations where errors that can be anticipated or predicted can be prevented or detected by control parameters that are automated.
- Control activities where the specific ways to perform the control can be adequately designed and automated.

Limitations of Internal Control

64. Internal control, no matter how well designed and operated, can provide an entity with reasonable, but not absolute, assurance about achieving an entity's objectives. The likelihood of achievement is affected by limitations inherent to internal control. These include the realities that human judgment in decision making can be faulty and that breakdowns in internal control can occur because of human failures such as simple errors or mistakes. For example, if an entity's information system personnel do not sufficiently understand how an order entry system processes sales transactions, they may design changes to the system that will erroneously process sales for a new line of products. On the other hand, such changes may be correctly designed but misunderstood by individuals who translate the design into program code. Errors also may occur in the use of information produced by IT. For example, automated controls may be designed to report transactions over a specified amount for management review, but individuals responsible for conducting the review may not understand the purpose of such reports and, accordingly, may fail to review them or investigate unusual items.

65. Additionally, controls, whether manual or automated, can be circumvented by the collusion of two or more people or inappropriate management override of internal control. For example, management may enter into

AU §RAS

Statement on Auditing Standards No. 109

1629

undisclosed agreements with customers that alter the terms and conditions of the entity's standard sales contracts, which may result in improper revenue recognition. Also, edit checks in a software program that are designed to identify and report transactions that exceed specified credit limits may be overridden or disabled.

66. Smaller entities often have fewer employees, which may limit the extent to which segregation of duties is practicable. However, for key areas, even in a very small entity, it can be practicable to implement some degree of segregation of duties or other form of unsophisticated but effective controls. The potential for override of controls by the owner-manager depends to a great extent on the control environment and, in particular, the owner-manager's attitudes about the importance of internal control.

Internal Control Components

67. Control environment. The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

68. The primary responsibility for the prevention and detection of fraud and error rests with those charged with governance and the management of the entity. In obtaining an understanding of the control environment, the auditor should consider the design and implementation of entity programs and controls to address the risk of fraud as discussed in SAS No. 99. The absence or inadequacy of such programs and controls may constitute a significant deficiency or a material weakness. An example of such programs is a "hotline process" for employees to report on a confidential basis any known or suspected fraudulent activity.

69. In evaluating the design of the entity's control environment, the auditor should consider the following elements and how they have been incorporated into the entity's processes:

- a. *Communication and enforcement of integrity and ethical values.* Essential elements that influence the effectiveness of the design, administration, and monitoring of controls.
- b. *Commitment to competence.* Management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.
- c. *Participation of those charged with governance.* Independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the information it receives, the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors.
- d. *Management's philosophy and operating style.* Management's approach to taking and managing business risks, and management's attitudes and actions toward financial reporting, information processing and accounting functions, and personnel.
- e. *Organizational structure.* The framework within which an entity's activities for achieving its objectives are planned, executed, controlled, and reviewed.
- f. *Assignment of authority and responsibility.* How authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established.

AU §RAS

1630 Risk Assessment Standards: SAS No. 104–SAS No. 111

- g. Human resource policies and practices.* Recruitment, orientation, training, evaluating, counseling, promoting, compensating, and remedial actions.

For example, management's response to internal control deficiencies communicated in prior periods may relate to one or more of the aforementioned elements, such as commitment to competence or management's philosophy and operating style.

70. The auditor should obtain sufficient knowledge of the control environment to understand the attitudes, awareness, and actions of those charged with governance concerning the entity's internal control and its importance in achieving reliable financial reporting. In understanding the control environment, the auditor should concentrate on the implementation of controls because controls may be established but not acted upon.

71. The responsibilities of those charged with governance are of considerable importance. This is recognized in codes of practice and other regulations or guidance produced for the benefit of those charged with governance. The basis for management remuneration, especially executive performance-related compensation, places stress on management arising from the conflicting demands of fair reporting and the perceived benefits to shareholders of improved results. It is one, but not the only, role of those charged with governance to counterbalance such pressures. In understanding the control environment, the auditor should consider such matters as the independence of the directors and their ability to evaluate the actions of management. The auditor also should consider whether there is a group of those charged with governance that understands the entity's business transactions and evaluates whether the financial statements are presented fairly in conformity with generally accepted accounting principles.

72. In understanding the control environment elements, the auditor should consider whether they have been implemented. The auditor should obtain sufficient appropriate audit evidence through a combination of inquiries and other risk assessment procedures, for example, corroborating inquiries through observation or inspection of documents. For example, through inquiries of management and employees, the auditor may obtain an understanding of how management communicates to employees its views on business practices and ethical behavior. The auditor should determine whether controls have been implemented by considering, for example, whether management has established a formal code of conduct and whether it acts in a manner that supports or condones violations of or authorizes exceptions to the code.

73. Audit evidence for elements of the control environment may not be available in documentary form, in particular for smaller entities where communication between management and other personnel may be informal, yet effective. For example, management's commitment to ethical values and competence are often implemented through the behavior and attitude they demonstrate in managing the entity's business instead of in a written code of conduct. Consequently, management's attitudes, awareness, and actions are of particular importance in the design of a smaller entity's control environment. In addition, the role of those charged with governance is often undertaken by the owner-manager where there are no other owners.

74. When obtaining an understanding of the control environment, the auditor also should consider the collective effect on the control environment of strengths and weaknesses in various control environment elements. Management's strengths and weaknesses may have a pervasive effect on internal control. For example, owner-manager controls may mitigate a lack of segregation of duties in a small business, or an active and independent board of directors may

AU §RAS

Statement on Auditing Standards No. 109

1631

influence the philosophy and operating style of senior management in larger entities. Alternatively, management's failure to commit sufficient resources to address security risks presented by IT may adversely affect internal control by allowing improper changes to be made to computer programs or to data, or by allowing unauthorized transactions to be processed. Similarly, human resource policies and practices directed toward hiring competent financial, accounting, and IT personnel may not mitigate a strong bias by top management to overstate earnings.

75. The existence of a satisfactory control environment is a positive factor when the auditor assesses the risks of material misstatement of the financial statements. Although an effective control environment is not an absolute deterrent to fraud because of the limitations of internal control, it may help reduce the risks of fraud. Because of the pervasive effect of the control environment on assessing the risks of material misstatement, the auditor's preliminary judgment about its effectiveness often influences the nature, timing, and extent of the further audit procedures to be performed. For example, weaknesses in the control environment may lead the auditor to perform more substantive procedures as of the date of the balance sheet rather than at an interim date, modify the nature of the tests of controls or substantive procedures to obtain more persuasive evidence, or increase the number of locations to be included in the scope of the audit. Conversely, an effective control environment may allow the auditor to have some degree of increased confidence in internal control and the reliability of evidence generated internally within the entity and thus, for example, allow the auditor to perform tests of controls and substantive procedures at an interim date rather than at the balance sheet date. However, the control environment ordinarily is not specific enough to prevent or detect material misstatements in account balances, classes of transactions, or disclosures and related assertions. The auditor, therefore, should consider the effect of other components of internal control in conjunction with the control environment when assessing the risks of material misstatement, for example, the monitoring of controls and the operation of specific control activities.

76. *The entity's risk assessment process.* An entity's risk assessment process for financial reporting purposes is its identification, analysis, and management of risks relevant to the preparation of financial statements that are presented fairly in conformity with generally accepted accounting principles. For example, risk assessment may address how the entity considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements. Risks relevant to reliable financial reporting also relate to specific events or transactions.

77. Risks relevant to financial reporting include external and internal events and circumstances that may occur and adversely affect an entity's ability to initiate, authorize, record, process, and report financial data consistent with the assertions of management in the financial statements.¹⁸ Risks can arise or change due to circumstances such as the following:

- Changes in operating environment
- New personnel
- New or revamped information systems
- Rapid growth

¹⁸ These assertions are discussed in SAS No. 106, *Audit Evidence*.

1632 Risk Assessment Standards: SAS No. 104–SAS No. 111

- New technology
- New business models, products, or activities
- Corporate restructurings
- Expanded foreign operations
- New accounting pronouncements

78. The auditor should obtain sufficient knowledge of the entity's risk assessment process to understand how management considers risks relevant to financial reporting objectives and decides about actions to address those risks. In evaluating the design and implementation of the entity's risk assessment process, the auditor should consider how management identifies business risks relevant to financial reporting, estimates the significance of the risks, assesses the likelihood of their occurrence, and decides upon actions to manage them. An entity's risk assessment process for financial reporting that encompasses the elements of internal control herein might be part of an entity's risk management framework. As such, auditors should focus on aspects of the framework that affect risks of material misstatements in financial reporting. If the entity's risk assessment process is appropriate to the circumstances, it assists the auditor in identifying risks of material misstatement.

79. The auditor should inquire about business risks that management has identified and should consider whether they may result in material misstatement of the financial statements. An entity's risk assessment process differs from the auditor's consideration of audit risk in a financial statement audit. The purpose of an entity's risk assessment process is to identify, analyze, and manage risks that affect the entity's objectives. In a financial statement audit, the auditor assesses risks to evaluate the likelihood that material misstatements could occur in the financial statements. Not all of the entity's risks are necessarily audit risks. However, the entity's risk assessment process may affect the auditor's consideration of audit risk. During the audit, the auditor may identify business risks or risks of material misstatement in the financial statements that management failed to identify. In such cases, the auditor should consider why the entity's risk assessment process failed to identify those risks and whether the process is appropriate to its circumstances.

80. In a smaller entity, management may not have a formal risk assessment process as described in paragraph 76. For such entities, the auditor should discuss with management how risks to the business are identified by management and how they are addressed.

81. *Information system, including the related business processes relevant to financial reporting, and communication.* The information system relevant to financial reporting objectives, which includes the accounting system, consists of the procedures, whether automated or manual, and records established to initiate, authorize, record, process, and report entity transactions (as well as events and conditions) and to maintain accountability for the related assets, liabilities, and equity. The quality of system-generated information affects management's ability to make appropriate decisions in controlling the entity's activities and to prepare reliable financial reports.

82. Communication involves providing an understanding of individual roles and responsibilities pertaining to internal control over financial reporting.

83. The auditor should obtain sufficient knowledge of the information system, including the related business processes relevant to financial reporting, to understand:

AU §RAS

Statement on Auditing Standards No. 109

1633

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

84. When IT is used to initiate, authorize, record, process, or report transactions or other financial data for inclusion in financial statements, the systems and programs may include controls related to the corresponding assertions for significant accounts or may be critical to the effective functioning of manual controls that depend on IT.

85. The auditor also should obtain an understanding of how the incorrect processing of transactions is resolved. For example, such understanding might include whether there is an automated suspense file, how it is used by the entity to ensure that suspense items are cleared out on a timely basis, and how system overrides or bypasses to controls are processed and accounted for.

86. In obtaining an understanding of the financial reporting process (including the closing process), the auditor should obtain an understanding of the automated and manual procedures an entity uses to prepare financial statements and related disclosures, and how misstatements may occur. Such procedures include those used to:

- *Enter transaction totals into the general ledger (or equivalent record).* In some information systems, IT may be used to transfer such information automatically from transaction processing systems to general ledger or financial reporting systems. The automated processes and controls in such systems may reduce the risk of inadvertent error but do not overcome the risk that individuals may inappropriately override such automated processes, for example, by changing the amounts being automatically passed to the general ledger or financial reporting system. Furthermore, in planning the audit, the auditor should be aware that when IT is used to transfer information automatically there may be little or no visible evidence of such intervention in the information systems.
- *Initiate, authorize, record, and process journal entries in the general ledger:* An entity's financial reporting process used to prepare the financial statements typically includes the use of standard journal entries that are required on a recurring basis to record transactions such as sales, purchases, and cash disbursements, or to record accounting estimates that are periodically made by management such as changes in the estimate of uncollectible accounts receivable. An entity's financial

AU §RAS

1634 Risk Assessment Standards: SAS No. 104–SAS No. 111

reporting process also includes the use of nonstandard journal entries to record nonrecurring or unusual transactions or adjustments such as a business combination or disposal, or a nonrecurring estimate such as an asset impairment. In manual, paper-based general ledger systems, such journal entries may be identified through inspection of ledgers, journals, and supporting documentation. However, when IT is used to maintain the general ledger and prepare financial statements, such entries may exist only in electronic form and may be more easily identified through the use of computer-assisted audit techniques.

- *Initiate and record recurring and nonrecurring adjustments to the financial statements.* These are procedures relating to adjustments and reclassifications that are not reflected in formal journal entries.
- *Combine and consolidate general ledger data.* This includes procedures to combine detailed general ledger accounts, prepare the trial balance, and prepare consolidated financial data (for example, transferring general ledger data and adjusting journals into a consolidation system or spreadsheet; performing consolidation routines; and reconciling and reviewing consolidated financial data, including footnote data).
- *Prepare financial statements and disclosures.* These are procedures designed to ensure that information required to be presented and disclosed is accumulated, recorded, processed, summarized, and appropriately reported in the financial statements.

87. The auditor should obtain an understanding of the entity's information system relevant to financial reporting in a manner that is appropriate to the entity's circumstances. This includes obtaining an understanding of how transactions originate within the entity's business processes. An entity's business processes are the activities designed to develop, purchase, produce, sell, and distribute an entity's products and services; ensure compliance with laws and regulations; and record information, including accounting and financial reporting information.

88. The auditor should obtain sufficient knowledge of the communication component to understand how the entity communicates financial reporting roles and responsibilities and significant matters relating to financial reporting. Communication involves providing an understanding of individual roles and responsibilities pertaining to internal control over financial reporting and may take such forms as policy manuals and financial reporting manuals. It includes the extent to which personnel understand how their activities in the financial reporting information system relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity. Open communication channels help ensure that exceptions are reported and acted on. The auditor's understanding of communication pertaining to financial reporting matters also includes communications between management and those charged with governance, particularly the audit committee, as well as external communications, such as those with regulatory authorities.

89. Control activities. The auditor should obtain an understanding of those control activities relevant to the audit. Control activities are the policies and procedures that help ensure that management directives are carried out; for example, that necessary actions are taken to address risks that threaten the achievement of the entity's objectives. Control activities, whether automated or manual, have various objectives and are applied at various organizational and functional levels. Examples of specific control activities include the following:

AU §RAS

Statement on Auditing Standards No. 109

1635

- *Authorization.* Control activities related to the initiation of derivatives and other off-balance sheet transactions may be relevant to the auditor's design of audit procedures related to the completeness assertion.
- *Segregation of duties.* Whether the personnel responsible for recording estimates for uncollectible accounts receivables are independent of personnel authorizing sales transactions may be relevant to the auditor's design of audit procedures related to the valuation assertion.
- *Safeguarding.* Control activities related to whether inventory is securely stored and the movement and access to inventory is limited to authorized individuals may be relevant to the auditor's design of audit procedures related to the existence assertion, in particular, the auditor's consideration as to the number of locations to visit.
- *Asset accountability.* Control activities related to reconciliations of the detailed records to the general ledger are ordinarily necessary to design and perform audit procedures for material classes of transactions and account balances.

90. The auditor should consider the knowledge about the presence or absence of control activities obtained from the understanding of the other components of internal control in determining whether it is necessary to devote additional attention to obtaining an understanding of control activities. An audit does not require an understanding of all the control activities related to each class of transactions, account balance, and disclosure in the financial statements or to every relevant assertion. Ordinarily, control activities that may be relevant to an audit include those relating to authorization, segregation of duties, safeguarding of assets, and asset accountability, including, for example, reconciliations of the general ledger to the detailed records. The auditor should obtain an understanding of the process of reconciling detail to the general ledger for significant accounts. Also, control activities are relevant to the audit if the auditor is required to evaluate them as discussed in paragraphs 115 through 117.

91. In obtaining an understanding of control activities, the auditor's primary consideration is whether, and how, a specific control activity, individually or in combination with others, prevents, or detects and corrects, material misstatements in classes of transactions, account balances, or disclosures. Control activities relevant to the audit are those for which the auditor considers it necessary to obtain an understanding in order to assess risks of material misstatement at the assertion level and to design and perform further audit procedures responsive to the assessed risks. The auditor's emphasis is on identifying and obtaining an understanding of control activities that address the areas where the auditor considers that material misstatements are more likely to occur. When multiple control activities achieve the same objective, it is unnecessary to obtain an understanding of each of the control activities related to such objective.

92. The auditor should obtain an understanding of how IT affects control activities that are relevant to planning the audit. Some entities and auditors may view the IT control activities in terms of application controls and general controls. Application controls apply to the processing of individual applications. Accordingly, application controls relate to the use of IT to initiate, authorize, record, process, and report transactions or other financial data. These controls help ensure that transactions occurred, are authorized, and are completely and accurately recorded and processed. Examples include edit checks of input data, numerical sequence checks, and manual follow-up of exception reports.

AU §RAS

1636 Risk Assessment Standards: SAS No. 104–SAS No. 111

93. Application controls may be performed by IT (for example, automated reconciliation of subsystems) or by individuals. When application controls are performed by people interacting with IT, they may be referred to as user controls. The effectiveness of user controls, such as reviews of computer-produced exception reports or other information produced by IT, may depend on the accuracy of the information produced. For example, a user may review an exception report to identify credit sales over a customer's authorized credit limit without performing procedures to verify its accuracy. In such cases, the effectiveness of the user control (that is, the review of the exception report) depends on both the effectiveness of the user review and the accuracy of the information in the report produced by IT.

94. General controls are policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. General controls commonly include controls over data center and network operations; system software acquisition, change, and maintenance; access security; and application system acquisition, development, and maintenance. While ineffective general controls do not, by themselves, cause misstatements, they may permit application controls to operate improperly and allow misstatements to occur and not be detected. For example, if there are weaknesses in the general controls over access security, and applications are relying on these general controls to prevent unauthorized transactions from being processed, such a general control weakness may have a more severe effect on the effective design and operation of the application control. General controls should be assessed in relation to their effect on applications and data that become part of the financial statements. For example, if no new systems are implemented during the period of the financial statements, weaknesses in the general controls over "systems development" may not be relevant to the financial statements being audited.

95. The use of IT affects the way that control activities are implemented. For example, when IT is used in an information system, segregation of duties often is achieved by implementing security controls.

96. The auditor should consider whether the entity has responded adequately to the risks arising from IT by establishing effective controls, including effective general controls upon which application controls depend. From the auditor's perspective, controls over IT systems are effective when they maintain the integrity of information and the security of the data such systems process.

97. *Monitoring of controls.* The auditor should obtain an understanding of the major types of activities that the entity uses to monitor internal control over financial reporting, including the sources of the information related to those activities, and how those activities are used to initiate corrective actions to its controls.

98. An important management responsibility is to establish and maintain internal control on an ongoing basis. Management's monitoring of controls includes whether they are operating as intended and that they are modified as appropriate for changes in conditions. Monitoring of controls may include activities such as management's review of whether bank reconciliations are being prepared on a timely basis, internal auditors' evaluation of sales personnel's compliance with the entity's policies on terms of sales contracts, and legal department's oversight of compliance with the entity's ethical or business practice policies.

99. Monitoring of controls is a process to assess the quality of internal control performance over time. It involves assessing the design and operation of controls on a timely basis and taking necessary corrective actions. Monitoring is

AU §RAS

Statement on Auditing Standards No. 109

1637

done to ensure that controls continue to operate effectively. For example, if the timeliness and accuracy of bank reconciliations are not monitored, personnel are likely to stop preparing them. Management accomplishes monitoring of controls through ongoing activities, separate evaluations, or a combination of the two. In many entities, internal auditors or personnel performing similar functions contribute to the monitoring of an entity's activities. When obtaining an understanding of the internal audit function, the auditor should follow the guidance in paragraphs 4 through 8 of SAS No. 65, *The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements*. Management's monitoring activities may include using information from communications from external parties such as customer complaints and regulator comments that may indicate problems or highlight areas in need of improvement.

100. In many entities, much of the information used in monitoring may be produced by the entity's information system. If management assumes that data used for monitoring is accurate without having a basis for that assumption, errors may exist in the information, potentially leading management to incorrect conclusions from its monitoring activities. The auditor should obtain an understanding of the sources of the information related to the entity's monitoring activities, and the basis upon which management considers the information to be sufficiently reliable for the purpose.

101. The auditor's understanding of management's monitoring of controls may assist the auditor in identifying the existence of more detailed controls or other activities that the auditor may consider in making risk assessments.

Assessing the Risks of Material Misstatement

102. The auditor should identify and assess the risks of material misstatement at the financial statement level and at the relevant assertion level related to classes of transactions, account balances, and disclosures. For this purpose, the auditor should:

- Identify risks throughout the process of obtaining an understanding of the entity and its environment, including relevant controls that relate to the risks, and considering the classes of transactions, account balances, and disclosures in the financial statements.
- Relate the identified risks to what can go wrong at the relevant assertion level.
- Consider whether the risks are of a magnitude that could result in a material misstatement of the financial statements.
- Consider the likelihood that the risks could result in a material misstatement of the financial statements.

103. The auditor should use information gathered by performing risk assessment procedures, including the audit evidence obtained in evaluating the design of controls and determining whether they have been implemented, as audit evidence to support the risk assessment. The auditor should use the risk assessment to determine the nature, timing, and extent of further audit procedures to be performed. When the risk assessment is based on an expectation that controls are operating effectively to prevent or detect material misstatement, individually or when aggregated, at the relevant assertion level, the auditor should perform tests of the controls that the auditor has determined to be suitably designed to prevent or detect a material misstatement in the relevant assertion to obtain audit evidence that the controls are operating effectively, as described in SAS No. 110.

1638 Risk Assessment Standards: SAS No. 104–SAS No. 111

104. The auditor should determine whether the identified risks of material misstatement relate to specific relevant assertions related to classes of transactions, account balances, and disclosures, or whether they relate more pervasively to the financial statements taken as a whole and potentially affect many relevant assertions. The latter risks (risks at the financial statement level) may derive in particular from a weak control environment.

105. The nature of the risks arising from a weak control environment is such that they are not likely to be confined to specific individual risks of material misstatement in particular classes of transactions, account balances, and disclosures. Rather, weaknesses such as management's lack of competence may have a more pervasive effect on the financial statements and may require an overall response by the auditor.

106. In making risk assessments, the auditor should identify the controls that are likely to prevent or detect and correct material misstatements in specific relevant assertions. Generally, the auditor gains an understanding of controls and relates them to relevant assertions in the context of processes and systems in which they exist. Doing so is useful because individual control activities often do not in themselves address a risk. Often only multiple control activities, together with other elements of internal control, will be sufficient to address a risk.

107. Conversely, some control activities may have a specific effect on an individual relevant assertion embodied in a particular class of transaction or account balance. For example, the control activities that an entity established to ensure that its personnel are properly counting and recording the annual physical inventory relate directly to the existence and completeness assertions for the inventory account balance.

108. Controls can be either directly or indirectly related to an assertion. The more indirect the relationship, the less effective that control may be in preventing or detecting and correcting misstatements in that assertion. For example, a sales manager's review of a summary of sales activity for specific stores by region ordinarily is only indirectly related to the completeness assertion for sales revenue. Accordingly, it may be less effective in reducing risk for that assertion than controls more directly related to that assertion, such as matching shipping documents with billing documents.

109. In assessing risks, deficiencies in an entity's internal control may come to the auditor's attention that are significant enough that they are, in the auditor's judgment, significant deficiencies that should be communicated to those charged with governance as required by SAS No. 60, *Communication of Internal Control Related Matters Noted in an Audit*, as amended. Furthermore, the auditor's understanding of internal control may raise doubts about the auditability of an entity's financial statements. Concerns about the integrity of the entity's management may be so serious as to cause the auditor to conclude that the risk of management misrepresentation in the financial statements is such that an audit cannot be conducted. Also, concerns about the condition and reliability of an entity's records may cause the auditor to conclude that it is unlikely that sufficient appropriate audit evidence will be available to support an unqualified opinion on the financial statements. In such circumstances, the auditor should consider a qualification or disclaimer of opinion, but in some cases the auditor's only recourse may be to withdraw from the engagement.

Significant Risks That Require Special Audit Consideration

110. As part of the risk assessment described in paragraph 102, the auditor should determine which of the risks identified are, in the auditor's judgment,

AU §RAS

Statement on Auditing Standards No. 109

1639

risks that require special audit consideration (such risks are defined as "significant risks"). Paragraphs 45 and 53 of SAS No. 110 describe the consequences for further audit procedures of identifying a risk as significant.

111. The determination of significant risks, which arise on most audits, is a matter for the auditor's professional judgment. In exercising this judgment, the auditor should consider inherent risk¹⁹ to determine whether the nature of the risk, the likely magnitude of the potential misstatement including the possibility that the risk may give rise to multiple misstatements, and the likelihood of the risk occurring are such that they require special audit consideration. Routine, noncomplex transactions that are subject to systematic processing are less likely to give rise to significant risks because they have lower inherent risks. On the other hand, significant risks are often derived from business risks that may result in a material misstatement. In considering the nature of the risks, the auditor should consider a number of matters, including the following:

- Whether the risk is a risk of fraud
- Whether the risk is related to recent significant economic, accounting, or other developments and, therefore, requires specific attention
- The complexity of transactions
- Whether the risk involves significant transactions with related parties
- The degree of subjectivity in the measurement of financial information related to the risks, especially those involving a wide range of measurement uncertainty
- Whether the risk involves significant nonroutine transactions that are outside the normal course of business for the entity, or that otherwise appear to be unusual

112. Significant risks often relate to significant nonroutine transactions and judgmental matters. Nonroutine transactions are transactions that are unusual, either due to size or nature, and that therefore occur infrequently. Judgmental matters may include the development of accounting estimates for which there is significant measurement uncertainty.

113. Risks of material misstatement may be greater for risks relating to significant nonroutine transactions arising from matters such as the following:

- Greater management intervention to specify the accounting treatment
- Greater manual intervention for data collection and processing
- Complex calculations or accounting principles
- The nature of nonroutine transactions, which may make it difficult for the entity to implement effective controls over the risks
- Significant related-party transactions

114. Risks of material misstatement may be greater for risks relating to significant judgmental matters that require the development of accounting estimates arising from matters such as the following:

- Accounting principles for accounting estimates or revenue recognition may be subject to differing interpretation.
- Required judgment may be subjective or complex, or may require assumptions about the effects of future events, for example, judgment about fair value.

¹⁹ The auditor does this before considering the effect of identified controls related to the risk.

1640 Risk Assessment Standards: SAS No. 104–SAS No. 111

115. For significant risks, to the extent the auditor has not already done so, the auditor should evaluate the design of the entity's related controls, including relevant control activities, and determine whether they have been implemented. An understanding of the entity's controls related to significant risks should provide the auditor with adequate information to develop an effective audit approach. Management ought to be aware of significant risks; however, risks relating to significant nonroutine or judgmental matters are often less likely to be subject to routine controls. Therefore, the auditor's understanding of whether the entity has designed and implemented controls for such significant risks includes whether and how management responds to the risks and whether control activities such as a review of assumptions by senior management or experts, formal processes for estimations, or approval by those charged with governance have been implemented to address the risks. For example, where there are nonrecurring events such as the receipt of notice of a significant lawsuit, consideration of the entity's response will include such matters as whether it has been referred to appropriate experts (such as internal or external legal counsel), whether an assessment has been made of the potential effect, and how it is proposed that the circumstances are to be disclosed in the financial statements.

116. If management has not appropriately responded by implementing controls over significant risks and if, as a result, the auditor judges that there is a significant deficiency or material weakness in the entity's internal control over financial reporting, the auditor should communicate this matter to those charged with governance. In these circumstances, the auditor also should consider the implications for the auditor's risk assessment.

Risks for Which Substantive Procedures Alone Do Not Provide Sufficient Appropriate Audit Evidence

117. As part of the risk assessment described in paragraph 102, the auditor should evaluate the design and determine the implementation of the entity's controls, including relevant control activities, over those risks for which, in the auditor's judgment, it is not possible or practicable to reduce detection risk at the relevant assertion level to an acceptably low level with audit evidence obtained only from substantive procedures. The consequences for further audit procedures of identifying such risks are described in paragraph 24 of SAS No. 110.

118. The understanding of the entity's information system relevant to financial reporting enables the auditor to identify risks of material misstatement that relate directly to the recording of routine classes of transactions or account balances and the preparation of reliable financial statements; these include risks of inaccurate or incomplete processing. Ordinarily, such risks relate to significant classes of transactions, such as an entity's revenue, purchases, and cash receipts or cash payments.

119. The characteristics of routine day-to-day business transactions often permit highly automated processing with little or no manual intervention. In such circumstances, it may not be possible to perform only substantive procedures in relation to the risk. For example, in circumstances where a significant amount of an entity's information is initiated, authorized, recorded, processed, or reported electronically, such as in an integrated system, the auditor may determine that it is not possible to design effective substantive procedures that by themselves would provide sufficient appropriate audit evidence that relevant classes of transactions or account balances are not materially misstated. In such cases, audit evidence may be available only in electronic form, and its

AU §RAS

Statement on Auditing Standards No. 109**1641**

appropriateness and sufficiency usually depend on the effectiveness of controls over its accuracy and completeness. Furthermore, the potential for improper initiation or alteration of information to occur and not be detected may be greater if information is initiated, authorized, recorded, processed, or reported only in electronic form and appropriate controls are not operating effectively.

120. Examples of situations in which the auditor may find it impossible to design effective substantive procedures that by themselves provide sufficient appropriate audit evidence that certain relevant assertions are not materially misstated include the following:

- An entity that conducts its business using IT to initiate orders for the purchase and delivery of goods based on predetermined rules of what to order and in what quantities and to pay the related accounts payable based on system-generated decisions initiated upon the confirmed receipt of goods and terms of payment. No other documentation of orders placed or goods received is produced or maintained, other than through the IT system.
- An entity that provides services to customers via electronic media (for example, an Internet service provider or a telecommunications company) and uses IT to create a log of the services provided to its customers, to initiate and process its billings for the services, and to automatically record such amounts in electronic accounting records that are part of the system used to produce the entity's financial statements.

Revision of Risk Assessment

121. The auditor's assessment of the risks of material misstatement at the relevant assertion level is based on available audit evidence and may change during the course of the audit as additional audit evidence is obtained. In particular, the risk assessment may be based on an expectation that controls are operating effectively to prevent or detect and correct a material misstatement at the relevant assertion level. In performing tests of controls to obtain audit evidence about their operating effectiveness, the auditor may obtain audit evidence that controls are not operating effectively at relevant times during the audit. Similarly, in performing substantive procedures, the auditor may detect misstatements in amounts or frequency that is greater than is consistent with the auditor's risk assessment. When the auditor obtains audit evidence from performing further audit procedures that tends to contradict the audit evidence on which the auditor originally based the assessment, the auditor should revise the assessment and should further modify planned audit procedures accordingly. See paragraphs 70 and 74 of SAS No. 110 for further guidance.

Documentation

122. The auditor should document:

- a. The discussion among the audit team regarding the susceptibility of the entity's financial statements to material misstatement due to error or fraud, including how and when the discussion occurred, the subject matter discussed, the audit team members who participated, and significant decisions reached concerning planned responses at the financial statement and relevant assertion levels.
- b. Key elements of the understanding obtained regarding each of the aspects of the entity and its environment identified in paragraph 21, including each of the components of internal control identified in paragraph 41, to assess the risks of material misstatement of the financial

AU §RAS

1642 Risk Assessment Standards: SAS No. 104–SAS No. 111

statements; the sources of information from which the understanding was obtained; and the risk assessment procedures.

- c. The assessment of the risks of material misstatement both at the financial statement level and at the relevant assertion level as required by paragraph 102 and the basis for the assessment.
- d. The risks identified and related controls evaluated as a result of the requirements in paragraphs 110 and 117.

123. The manner in which these matters are documented is for the auditor to determine using professional judgment. SAS No. 103, *Audit Documentation*, provides general guidance regarding the purpose, content, and ownership and confidentiality of audit documentation. Examples of common techniques used alone or in combination include narrative descriptions, questionnaires, checklists, and flowcharts. Such techniques may also be useful in documenting the auditor's assessment of the risks of material misstatement at the overall financial statement and relevant assertions level. The form and extent of this documentation are influenced by the nature, size, and complexity of the entity and its environment, including its internal control, and the availability of information from the entity and the specific audit methodology and technology used in the course of the audit. For example, documentation of the understanding of a complex information system in which a large volume of transactions are electronically initiated, authorized, recorded, processed, or reported may include flowcharts, questionnaires, or decision tables. For an information system making limited or no use of IT or for which few transactions are processed (for example, long-term debt), documentation in the form of a memorandum may be sufficient. Generally, the more complex the entity and its environment, including its internal control, and the more extensive the audit procedures performed by the auditor, the more extensively the auditor should document his or her work. The specific audit methodology and technology used in the course of the audit will also affect the form and extent of documentation.

Effective Date

124. This SAS is effective for audits of financial statements for periods beginning on or after December 15, 2006. Earlier application is permitted.

Appendix A

Understanding the Entity and Its Environment

A1. This appendix provides additional guidance on matters the auditor may consider when obtaining an understanding of the industry, regulatory, and other external factors that affect the entity; the nature of the entity; objectives and strategies and related business risks; and measurement and review of the entity's financial performance. The examples provided cover a broad range of matters applicable to many engagements; however, not all matters are relevant to every engagement and the list of examples is not necessarily complete. Additional guidance on internal control is contained in Appendix B.

Industry, Regulatory, and Other External Factors

A2. Examples of matters an auditor may consider include the following:

- Industry conditions
 - The market and competition, including demand, capacity, and price competition
 - Cyclical or seasonal activity
 - Product technology relating to the entity's products
 - Supply availability and cost
- Regulatory environment
 - Accounting principles and industry-specific practices
 - Regulatory framework for a regulated industry
 - Legislation and regulation that significantly affect the entity's operations
 - Regulatory requirements
 - Direct supervisory activities
 - Taxation (corporate and other)
 - Government policies currently affecting the conduct of the entity's business
 - Monetary, including foreign exchange controls
 - Fiscal
 - Financial incentives (for example, government aid programs)
 - Tariffs and trade restrictions
 - Environmental requirements affecting the industry and the entity's business
- Other external factors currently affecting the entity's business
 - General level of economic activity (for example, recession, growth)
 - Interest rates and availability of financing
 - Inflation and currency revaluation

1644 Risk Assessment Standards: SAS No. 104–SAS No. 111**Nature of the Entity**

A3. Examples of matters an auditor may consider include the following:

- **Business operations**
 - Nature of revenue sources (for example, manufacturer; wholesaler; banking, insurance, or other financial services; import-export trading, utility, transportation, and technology products and services)
 - Products or services and markets (for example, major customers and contracts, terms of payment, profit margins, market share, competitors, exports, pricing policies, reputation of products, warranties, backlog, trends, marketing strategy and objectives, and manufacturing processes)
 - Conduct of operations (for example, stages and methods of production, subsidiaries or divisions, delivery of products and services, and details of declining or expanding operations)
 - Alliances, joint ventures, and outsourcing activities
 - Involvement in e-commerce, including Internet sales and marketing activities
 - Geographic dispersion and industry segmentation
 - Location of production facilities, warehouses, and offices
 - Key customers
 - Important suppliers of goods and services (for example, long-term contracts, stability of supply, terms of payment, imports, and methods of delivery, such as "just-in-time")
 - Employment (for example, by location, supply, wage levels, union contracts, pension and other postemployment benefits, stock option or incentive bonus arrangements, and government regulation related to employment matters)
 - Research and development activities and expenditures
 - Transactions with related parties
- **Investments**
 - Acquisitions, mergers, or disposals of business activities (planned or recently executed)
 - Investments and dispositions of securities and loans
 - Capital investment activities, including investments in plant and equipment and technology, and any recent or planned changes
 - Investments in nonconsolidated entities, including partnerships, joint ventures, and special-purpose entities
 - Life cycle stage of enterprise (start-up, growing, mature, declining)
- **Financing**
 - Group structure—major subsidiaries and associated entities, including consolidated and nonconsolidated structures
 - Debt structure, including covenants, restrictions, guarantees, and off-balance-sheet financing arrangements
 - Leasing of property, plant, or equipment for use in the business

AU §RAS

Statement on Auditing Standards No. 109**1645**

- Beneficial owners (local and foreign business reputation and experience)
- Related parties
- Use of derivative financial instruments
- Financial reporting
 - Accounting principles and industry-specific practices
 - Revenue recognition practices
 - Accounting for fair values
 - Inventories (for example, locations and quantities)
 - Foreign currency assets, liabilities, and transactions
 - Industry-specific significant categories (for example, loans and investments for banks, accounts receivable and inventory for manufacturers, research and development for pharmaceuticals)
 - Accounting for unusual or complex transactions including those in controversial or emerging areas (for example, accounting for stock-based compensation)
 - Financial statement presentation and disclosure

Objectives and Strategies and Related Business Risks**A4.** Examples of matters an auditor may consider include the following:

- Existence of objectives (that is, how the entity addresses industry, regulatory, and other external factors) relating to, for example, the following:
 - Industry developments (a potential related business risk might be, for example, that the entity does not have the personnel or expertise to deal with the changes in the industry)
 - New products and services (a potential related business risk might be, for example, that there is increased product liability)
 - Expansion of the business (a potential related business risk might be, for example, that the demand has not been accurately estimated)
 - New accounting requirements (a potential related business risk might be, for example, incomplete or improper implementation, or increased costs)
 - Regulatory requirements (a potential related business risk might be, for example, that there is increased legal exposure)
 - Current and prospective financing requirements (a potential related business risk might be, for example, the loss of financing due to the entity's inability to meet requirements)
 - Use of information technology (IT) (a potential related business risk might be, for example, that systems and processes are not compatible)
 - Risk appetite of managers and stakeholders
- Effects of implementing a strategy, particularly any effects that will lead to new accounting requirements (a potential related business risk might be, for example, incomplete or improper implementation)

AU §RAS

1646 Risk Assessment Standards: SAS No. 104–SAS No. 111

Measurement and Review of the Entity's Financial Performance

A5. Examples of matters an auditor may consider include:

- Key ratios and operating statistics
- Key performance indicators
- Employee performance measures and incentive compensation policies
- Trends
- Use of forecasts, budgets, and variance analysis
- Analyst reports and credit rating reports
- Competitor analysis
- Period-on-period financial performance (revenue growth, profitability, and leverage)

Appendix B

Internal Control Components

B1. As set forth in paragraph 41 and described in paragraphs 67 through 101, internal control consists of the following components:

- a. Control environment
- b. Risk assessment
- c. Information and communication systems
- d. Control activities
- e. Monitoring

This appendix further explains these components as they relate to the financial statement audit.

Control Environment

B2. The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for effective internal control, providing discipline and structure.

B3. The control environment encompasses the following elements:

- a. *Communication and enforcement of integrity and ethical values.* The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment that influence the effectiveness of the design, administration, and monitoring of other components of internal control. Integrity and ethical behavior are the product of the entity's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct and by example.
- b. *Commitment to competence.* Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.
- c. *Participation of those charged with governance.* An entity's control consciousness is significantly influenced by those charged with governance. Attributes include those charged with governance's independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the information it receives, the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors. The importance of responsibilities of those charged with governance is recognized in codes of practice and other regulations or guidance produced for the benefit of those charged with governance. Other responsibilities of those charged with governance include oversight of the design and effective operation of whistle-blower procedures and of the process for reviewing the effectiveness of the entity's internal control.

1648 Risk Assessment Standards: SAS No. 104–SAS No. 111

- d. *Management's philosophy and operating style.* Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the following: management's approach to taking and monitoring business risks; management's attitudes and actions toward financial reporting (conservative or aggressive selection from available alternative accounting principles, and conscientiousness and conservatism with which accounting estimates are developed); and management's attitudes toward information processing and accounting functions and personnel.
- e. *Organizational structure.* An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and reviewed. Establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. An entity develops an organizational structure suited to its needs. The appropriateness of an entity's organizational structure depends in part on its size and the nature of its activities.
- f. *Assignment of authority and responsibility.* This factor includes how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that all personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.
- g. *Human resource policies and practices.* Human resource policies and practices relate to recruitment, orientation, training, evaluating, counseling, promoting, compensating, and remedial actions. For example, standards for recruiting the most qualified individuals—with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior—demonstrate an entity's commitment to competent and trustworthy people. Training policies that communicate prospective roles and responsibilities and include practices such as training schools and seminars illustrate expected levels of performance and behavior. Promotions driven by periodic performance appraisals demonstrate the entity's commitment to the advancement of qualified personnel to higher levels of responsibility.

Application to Small and Midsized Entities

B4. Small and midsized entities may implement the control environment elements differently than larger entities. For example, smaller entities might not have a written code of conduct but, instead, develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication and by management example. Similarly, those charged with governance in smaller entities may not include independent or outside members.

Entity's Risk Assessment Process

B5. An entity's risk assessment process is its process for identifying and responding to business risks and the results thereof. For financial reporting purposes, the entity's risk assessment process includes how management identifies risks relevant to the preparation of financial statements that are presented fairly in conformity with generally accepted accounting principles,

AU §RAS

Statement on Auditing Standards No. 109

1649

estimates their significance, assesses the likelihood of their occurrence, and decides upon actions to manage them. For example, the entity's risk assessment process may address how the entity considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements. Risks relevant to reliable financial reporting also relate to specific events or transactions.

B6. Risks relevant to financial reporting include external and internal events and circumstances that may occur and adversely affect an entity's ability to initiate, authorize, record, process, and report financial data consistent with the assertions of management in the financial statements. Once risks are identified, management considers their significance, the likelihood of their occurrence, and how they should be managed. Management may initiate plans, programs, or actions to address specific risks, or it may decide to accept a risk because of cost or other considerations. Risks can arise or change due to such circumstances as the following:

- *Changes in operating environment.* Changes in the regulatory or operating environment can result in changes in competitive pressures and significantly different risks.
- *New personnel.* New personnel may have a different focus on or understanding of internal control.
- *New or revamped information systems.* Significant and rapid changes in information systems can change the risk relating to internal control.
- *Rapid growth.* Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls.
- *New technology.* Incorporating new technologies into production processes or information systems may change the risk associated with internal control.
- *New business models, products, or activities.* Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with internal control.
- *Corporate restructurings.* Restructurings may be accompanied by staff reductions and changes in supervision and segregation of duties that may change the risk associated with internal control.
- *Expanded foreign operations.* The expansion or acquisition of foreign operations carries new and often unique risks that may affect internal control, for example, additional or changed risks from foreign currency transactions.
- *New accounting pronouncements.* Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.

Application to Small and Midsized Entities

B7. The basic concepts of the entity's risk assessment process are relevant to every entity, regardless of size, but the risk assessment process is likely to be less formal and less structured in small and midsized entities than in larger ones. All entities should have established financial reporting objectives, but they may be recognized implicitly rather than explicitly in smaller entities. Management may be able to learn about risks related to these objectives through direct personal involvement with employees and outside parties.

AU §RAS

1650 Risk Assessment Standards: SAS No. 104–SAS No. 111**Information System, Including the Related Business Processes Relevant to Financial Reporting, and Communication**

B8. An information system consists of infrastructure (physical and hardware components), software, people, procedures (manual and information technology [IT]), and data. Infrastructure and software will be absent, or have less significance, in systems that are exclusively or primarily manual. Many information systems rely extensively on IT.

B9. The information system relevant to financial reporting objectives, which includes the accounting system, consists of the procedures, whether IT or manual, and records established to initiate, authorize, record, process, and report entity transactions (as well as events and conditions) and to maintain accountability for the related assets, liabilities, and equity. Transactions may be initiated manually or automatically by programmed procedures. Authorization includes the process of approving transactions by the appropriate level of management. Recording includes identifying and capturing the relevant information for transactions or events. Processing includes functions such as edit and validation, calculation, measurement, valuation, summarization, and reconciliation, whether performed by IT or manual procedures. Reporting relates to the preparation of financial reports as well as other information, in electronic or printed format, that the entity uses in measuring and reviewing the entity's financial performance and in other functions. The quality of system-generated information affects management's ability to make appropriate decisions in managing and controlling the entity's activities and to prepare reliable financial reports.

B10. Accordingly, an information system encompasses methods and records that:

- Identify and record all valid transactions.
- Describe on a timely basis the transactions in sufficient detail to permit proper classification of transactions for financial reporting.
- Measure the value of transactions in a manner that permits recording their proper monetary value in the financial statements.
- Determine the time period in which transactions occurred to permit recording of transactions in the proper accounting period.
- Present properly the transactions and related disclosures in the financial statements.

B11. Communication involves providing an understanding of individual roles and responsibilities pertaining to internal control over financial reporting. It includes the extent to which personnel understand how their activities in the financial reporting information system relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity. Open communication channels help ensure that exceptions are reported and acted on.

B12. Communication takes such forms as policy manuals, accounting and financial reporting manuals, and memoranda. Communication also can be made electronically, orally, and through the actions of management.

Application to Small and Midsized Entities

B13. Information systems and related business processes relevant to financial reporting in small or midsized organizations are likely to be less formal

AU §RAS

Statement on Auditing Standards No. 109

1651

than in larger organizations, but their role is just as significant. Smaller entities with active management involvement may not need extensive descriptions of accounting procedures, sophisticated accounting records, or written policies. Communication may be less formal and easier to achieve in a small or mid-sized company than in a larger enterprise due to the smaller organization's size and fewer levels as well as management's greater visibility and availability.

Control Activities

B14. Control activities are the policies and procedures that help ensure that management directives are carried out, for example, that necessary actions are taken to address risks that threaten the achievement of the entity's objectives. Control activities, whether automated or manual, have various objectives and are applied at various organizational and functional levels.

B15. Generally, control activities that may be relevant to an audit may be categorized as policies and procedures that pertain to the following:

- *Performance reviews.* These control activities include reviewing and analyzing actual performance versus budgets, forecasts, and prior-period performance; relating different sets of data—operating or financial—to one another, together with analyses of the relationships and investigative and corrective actions; comparing internal data with external sources of information, and reviewing functional or activity performance, such as a bank's consumer loan manager's review of reports by branch, region, and loan type for loan approvals and collections.
- *Information processing.* A variety of controls are performed to check accuracy, completeness, and authorization of transactions. The two broad groupings of information systems control activities are application controls and general controls. Application controls apply to the processing of individual applications. These controls help ensure that transactions occurred, are authorized, and are completely and accurately recorded and processed. Examples of application controls include checking the arithmetical accuracy of records, maintaining and reviewing accounts and trial balances, automated controls such as edit checks of input data and numerical sequence checks, and manual follow-up of exception reports. General controls are policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. General controls commonly include controls over data center and network operations; system software acquisition, change, and maintenance; access security; and application system acquisition, development, and maintenance. These controls apply to mainframe, miniframe, and end-user environments. Examples of such general controls are program change controls, controls that restrict access to programs or data, controls over the implementation of new releases of packaged software applications, and controls over system software that restrict access to or monitor the use of system utilities that could change financial data or records without leaving an audit trail.
- *Physical controls.* These activities encompass the physical security of assets, including adequate safeguards such as secured facilities to limit access to assets and records; authorization for access to computer programs and data files; and periodic counting and comparison with amounts shown on control records (for example, comparing the results

1652 Risk Assessment Standards: SAS No. 104–SAS No. 111

of cash, security, and inventory counts with accounting records). The extent to which physical controls intended to prevent theft of assets are relevant to the reliability of financial statement preparation, and therefore the audit, depends on circumstances such as when assets are highly susceptible to misappropriation. For example, these controls would ordinarily not be relevant when any inventory losses would be detected pursuant to periodic physical inspection and recorded in the financial statements. However, if for financial reporting purposes management relies solely on perpetual inventory records, the physical security controls would be relevant to the audit.

- *Segregation of duties.* Assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud in the normal course of his or her duties. Examples of segregation of duties include reporting, reviewing and approving reconciliations, and approval and control of documents.

B16. Certain control activities may depend on the existence of appropriate higher-level policies established by management or those charged with governance. For example, authorization controls may be delegated under established guidelines, such as investment criteria set by those charged with governance; alternatively, nonroutine transactions such as major acquisitions or divestments may require specific high-level approval, including in some cases that of shareholders.

Application to Small and Midsized Entities

B17. The concepts underlying control activities in small or midsized organizations are likely to be similar to those in larger entities, but the formality with which they operate varies. Further, smaller entities may find that certain types of control activities are not relevant because of controls applied by management. For example, management's retention of authority for approving credit sales, significant purchases, and draw-downs on lines of credit can provide strong control over those activities, lessening or removing the need for more detailed control activities. An appropriate segregation of duties often appears to present difficulties in smaller organizations. Even companies that have only a few employees, however, may be able to assign responsibilities to achieve appropriate segregation or, if that is not possible, to use management oversight of the incompatible activities to achieve control objectives.

Monitoring of Controls

B18. An important management responsibility is to establish and maintain internal control on an ongoing basis. Management's monitoring of controls includes considering whether they are operating as intended and that they are modified as appropriate for changes in conditions. Monitoring of controls may include activities such as management's review of whether bank reconciliations are being prepared on a timely basis, internal auditors' evaluation of sales personnel's compliance with the entity's policies on terms of sales contracts, and a legal department's oversight of compliance with the entity's ethical or business practice policies.

B19. Monitoring of controls is a process to assess the quality of internal control performance over time. It involves assessing the design and operation of controls on a timely basis and taking necessary corrective actions. Monitoring is done to ensure that controls continue to operate effectively. For example, if

AU §RAS

Statement on Auditing Standards No. 109

1653

the timeliness and accuracy of bank reconciliations are not monitored, personnel are likely to stop preparing them. Monitoring of controls is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

B20. Ongoing monitoring activities are built into the normal recurring activities of an entity and include regular management and supervisory activities. Managers of sales, purchasing, and production at divisional and corporate levels are in touch with operations and may question reports that differ significantly from their knowledge of operations.

B21. In many entities, internal auditors or personnel performing similar functions contribute to the monitoring of an entity's controls through separate evaluations. They regularly provide information about the functioning of internal control, focusing considerable attention on evaluating the design and operation of internal control. They communicate information about strengths and weaknesses and recommendations for improving internal control.

B22. Monitoring activities may include using information from communications from external parties that may indicate problems or highlight areas in need of improvement. Customers implicitly corroborate billing data by paying their invoices or complaining about their charges. In addition, regulators may communicate with the entity concerning matters that affect the functioning of internal control, for example, communications concerning examinations by bank regulatory agencies. Also, management may consider communications relating to internal control from external auditors in performing monitoring activities.

Application to Small and Midsized Entities

B23. Ongoing monitoring activities of small and midsized entities are more likely to be informal and are typically performed as a part of the overall management of the entity's operations. Management's close involvement in operations often will identify significant variances from expectations and inaccuracies in financial data.

1654 Risk Assessment Standards: SAS No. 104–SAS No. 111

Appendix C

Conditions and Events That May Indicate Risks of Material Misstatement

C1. The following are examples of conditions and events that may indicate the existence of risks of material misstatement. The examples provided cover a broad range of conditions and events; however, not all conditions and events are relevant to every audit engagement and the list of examples is not necessarily complete.

- Operations in regions that are economically unstable, for example, countries with significant currency devaluation or highly inflationary economies.
- Operations exposed to volatile markets, for example, futures trading.
- High degree of complex regulation.
- Going concern and liquidity issues, including loss of significant customers.
- Marginally achieving explicitly stated strategic objectives.
- Constraints on the availability of capital and credit.
- Changes in the industry in which the entity operates.
- Changes in the supply chain.
- Developing or offering new products or services, or moving into new lines of business.
- Expanding into new locations.
- Changes in the entity, such as large acquisitions, reorganizations, or other unusual events.
- Entities or divisions likely to be sold.
- Complex alliances and joint ventures.
- Use of off-balance-sheet finance, special-purpose entities, and other complex financing arrangements.
- Significant transactions with related parties.
- Lack of personnel with appropriate accounting and financial reporting skills.
- Changes in key personnel, including departure of key executives.
- Weaknesses in internal control, especially those not addressed by management.
- Inconsistencies between the entity's information technology (IT) strategy and its business strategies.
- Changes in the IT environment.
- Installation of significant new IT systems related to financial reporting.
- Inquiries into the entity's operations or financial results by regulatory or government bodies.
- Past misstatements, history of errors, or a significant amount of adjustments at period end.

AU §RAS

Statement on Auditing Standards No. 109**1655**

- Significant amount of nonroutine or nonsystematic transactions, including intercompany transactions and large revenue transactions at period end.
- Transactions that are recorded based on management's intent, for example, debt refinancing, assets to be sold, and classification of marketable securities.
- Application of new accounting pronouncements.
- Complex processes related to accounting measurements.
- Events or transactions that result in significant measurement uncertainty, including accounting estimates.
- Pending litigation and contingent liabilities, for example, sales warranties, financial guarantees, and environmental remediation.

This Statement entitled Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement was unanimously adopted by the assenting votes of the nineteen members of the board.

Auditing Standards Board (2004–2005)

John A. Fogarty, <i>Chair</i>	Wanda L. Lorenz
Harold L. Monk, Jr., <i>Vice Chair</i>	William F. Messier, Jr.
Barton W. Baldwin	Daniel D. Montgomery
Gerald W. Burns	Keith O. Newton
Craig W. Crawford	George A. Rippey
George P. Fritz	Lisa A. Ritter
James W. Goad	Diane M. Rubin
Dan L. Goldwasser	Scott A. Seasock
Lynford Graham	Michael T. Umscheid
James E. Lee	

Risk Assessment Task Force

Darrel R. Schubert, <i>Chair</i>	Auston G. Johnson
Abraham D. Akresh	Wanda L. Lorenz
Brian Ballou	William F. Messier, Jr.
Lynford Graham	

AICPA Staff

Charles E. Landes	Hiram Hasty
<i>Vice President</i>	<i>Technical Manager</i>
<i>Audit and Attest Standards</i>	<i>Audit and Attest Standards</i>

Note: *Statements on Auditing Standards are issued by the Auditing Standards Board, the senior technical body of the Institute designated to issue pronouncements on auditing matters. Rule 202, Compliance With Standards, of the Institute's Code of Professional Conduct requires compliance with these standards in an audit of a nonissuer.*

[The next page is 1671.]

AU §RAS

