

2001

# Effect of information technology on the auditor's consideration of internal control in a financial statement audit; Statement on auditing standards, 094

American Institute of Certified Public Accountants. Auditing Standards Executive Committee

Follow this and additional works at: [https://egrove.olemiss.edu/aicpa\\_sas](https://egrove.olemiss.edu/aicpa_sas)

Part of the [Accounting Commons](#), and the [Taxation Commons](#)

---

## Recommended Citation

American Institute of Certified Public Accountants. Auditing Standards Executive Committee, "Effect of information technology on the auditor's consideration of internal control in a financial statement audit; Statement on auditing standards, 094" (2001). *Statements on Auditing Standards*. 99.

[https://egrove.olemiss.edu/aicpa\\_sas/99](https://egrove.olemiss.edu/aicpa_sas/99)

This Book is brought to you for free and open access by the American Institute of Certified Public Accountants (AICPA) Historical Collection at eGrove. It has been accepted for inclusion in Statements on Auditing Standards by an authorized administrator of eGrove. For more information, please contact [egrove@olemiss.edu](mailto:egrove@olemiss.edu).

May 2001

94

# Statement on Auditing Standards

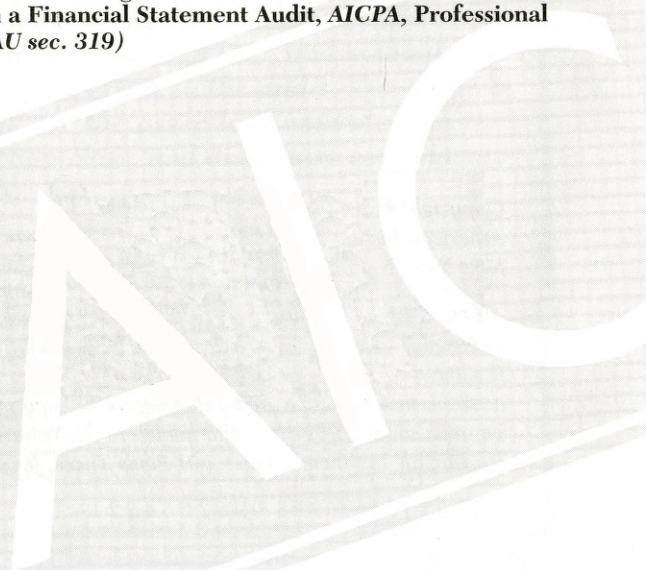
Issued by the Auditing Standards Board

AICPA

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

## The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit

*(Amends Statement on Auditing Standards No. 55, Consideration of Internal Control in a Financial Statement Audit, AICPA, Professional Standards, vol. 1, AU sec. 319)*



Copyright © 2001 by  
American Institute of Certified Public Accountants, Inc.  
New York, NY 10036-8775

*All rights reserved. For information about the procedure for requesting permission to make copies of any part of this work, please call the AICPA Copyright Permissions Hotline at (201) 938-3245. A Permissions Request Form for e-mailing requests is available at [www.aicpa.org](http://www.aicpa.org) by clicking on the copyright notice on any page. Otherwise, requests should be written and mailed to the Permissions Department, AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311-3881.*

1 2 3 4 5 6 7 8 9 0 A A S 0 9 8 7 6 5 4 3 2 1

# The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit

*Amends Statement on Auditing Standards No. 55, Consideration of Internal Control in a Financial Statement Audit (AICPA, Professional Standards, vol. 1, AU sec. 319)\**

## Introduction

1. This Statement provides guidance on the independent auditor's consideration of an entity's internal control in an audit of financial statements in accordance with generally accepted auditing standards. It defines internal control,<sup>1</sup> describes the objectives and components of internal control, and explains how an auditor should consider internal control in planning and performing an audit. In particular, this Statement provides guidance about implementing the second standard of field work<sup>2</sup>: "A sufficient understanding of internal control is to be obtained to plan the audit and to determine the nature, timing, and extent of tests to be performed."

2. In all audits, the auditor should obtain an understanding of internal control sufficient to plan the audit by performing procedures to understand the design of controls relevant to an audit of financial statements; and ***determining*** whether they have been placed in operation. ***In obtaining this understanding, the auditor considers how an entity's use of information technology (IT)<sup>2</sup> and manual procedures may affect controls relevant to the audit. The auditor then assesses control risk for the assertions embodied in the account balance, transaction class, and disclosure components of the financial statements.***

\* New language is shown in boldface italic; deleted language is shown by strikethrough.

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

~~2. This section revises the second standard of fieldwork of the ten generally accepted auditing standards.~~

2. ***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, record, process, and report transactions or other financial data.***

3. *The auditor may determine that assessing control risk below the maximum level<sup>3</sup> for certain assertions would be effective and more efficient than performing only substantive tests. In addition, the auditor may determine that it is not practical or possible to restrict detection risk to an acceptable level by performing only substantive tests for one or more financial statement assertions. In such circumstances, the auditor should obtain evidential matter about the effectiveness of both the design and operation of controls to reduce the assessed level of control risk. Such evidential matter may be obtained from tests of controls planned and performed concurrent with or subsequent to obtaining the understanding.<sup>4</sup> Such evidential matter also may be obtained from procedures that were not specifically planned as tests of controls but that nevertheless provide evidential matter about the effectiveness of the design and operation of the controls. For certain assertions, the auditor may desire to further reduce the assessed level of control risk. In such cases, the auditor considers whether evidential matter sufficient to support a further reduction is likely to be available and whether performing additional tests of controls to obtain such evidential matter would be efficient.*

4.3. ~~After obtaining this understanding, the auditor assesses control risk for the assertions embodied in the account balance, transaction class, and disclosure components of the financial statements. Alternatively, the auditor may assess control risk at the maximum level (the greatest probability that a material misstatement that could occur in an assertion will not be prevented or detected on a timely basis by an entity's internal control) because he or she believes controls are unlikely to pertain to an assertion; or are unlikely to be effective, or because evaluating their effectiveness of controls would be inefficient. However, the auditor needs to be satisfied that performing only substantive tests would be effective in restricting~~

3. *Control risk may be assessed in quantitative terms, such as percentages, or in non-quantitative terms that range, for example, from a maximum to a minimum. The term maximum level is used in this Statement to mean the greatest probability that a material misstatement that could occur in a financial statement assertion will not be prevented or detected on a timely basis by an entity's internal control.*

4. *If the auditor is unable to obtain such evidential matter, he or she should consider the guidance in Statement on Auditing Standards (SAS) No. 31, Evidential Matter (AICPA, Professional Standards, vol. 1, AU 326.14 and 326.25), as amended by SAS No. 80, Amendment to Statement on Auditing Standards No. 31, Evidential Matter.*

***detection risk to an acceptable level. When evidence of an entity's initiation, recording, or processing of financial data exists only in electronic form, the auditor's ability to obtain the desired assurance only from substantive tests would significantly diminish.***

Alternatively, the auditor may obtain evidential matter about the effectiveness of both the design and operation of a control that supports a lower assessed level of control risk. Such evidential matter may be obtained from tests of controls planned or performed concurrently with obtaining the understanding or from procedures performed to obtain the understanding that were not specifically planned as tests of controls.

4. After obtaining the understanding and assessing control risk, the auditor may desire to seek a further reduction in the assessed level of control risk for certain assertions. In such cases, the auditor considers whether evidential matter sufficient to support a further reduction is likely to be available and whether performing additional tests of controls to obtain such evidential matter would be efficient.

5. The auditor uses the knowledge provided by the understanding of internal control and the assessed level of control risk in determining the nature, timing, and extent of substantive tests for financial statement assertions.

## **Definition of Internal Control**

6. *Internal control* is a process—effected by an entity's board of directors, management, and other personnel—designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations.

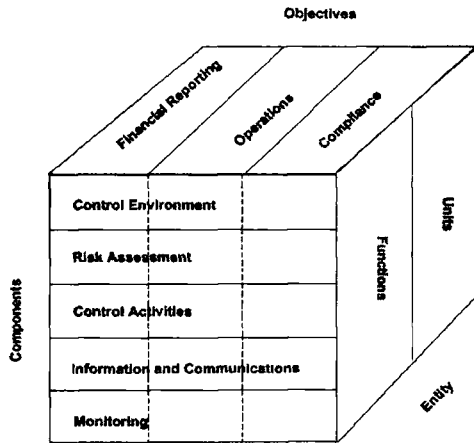
7. Internal control consists of five interrelated components, which are:

- 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. *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. *Control activities* are the policies and procedures that help ensure that management directives are carried out.
- d. *Information and communication systems support* are the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- e. *Monitoring* is a process that assesses the quality of internal control performance over time.

## Relationship Between Objectives and Components

8. There is a direct relationship between objectives, which are what an entity strives to achieve, and components, which represent what is needed to achieve the objectives. In addition, internal control is relevant to the entire entity, or to any of its operating units or business functions. This relationship is depicted as follows:



9. Although an entity's internal control addresses objectives in each of the categories referred to in paragraph 6, not all of these objectives and related controls are relevant to an audit of the entity's financial statements. Also, although internal control is relevant to the entire entity or to any of its operating units or business functions, an understanding of internal control relevant to each of the entity's operating units and business functions may not be necessary *to plan and perform an effective audit*.

## Financial Reporting Objective

10. Generally, controls that are relevant to an audit pertain to the entity's objective of preparing financial statements for external purposes that are fairly presented in conformity with generally accepted accounting principles or a comprehensive basis of accounting other than generally accepted accounting principles.<sup>53</sup>

## Operations and Compliance Objectives

11. The controls relating to operations and compliance<sup>64</sup> objectives may be relevant to an audit if they pertain to data the auditor evaluates or uses in applying auditing procedures. For example, controls pertaining to nonfinancial data that the auditor uses in analytical procedures, such as production statistics, or 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.

12. An entity generally has controls relating to objectives that are not relevant to an audit and therefore need not be considered. For example, controls concerning compliance with health and safety regulations or concerning the effectiveness and efficiency of certain management decision-making processes (such as the appropriate price to charge for its products or whether to make expenditures for certain research and development or advertising activities), although important to the entity, ordinarily do not relate to a financial statement audit. ***Similarly, an entity may rely on a sophisticated system of automated controls to provide efficient and effective operations (such as a commercial airline's system of automated controls to maintain flight schedules), but these controls ordinarily would not be relevant to the financial statement audit and therefore need not be considered.***

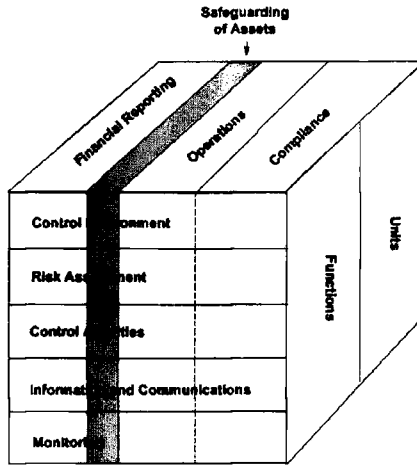
**5.3:** The term *comprehensive basis of accounting other than generally accepted accounting principles* is defined in **Statement on Auditing Standards (SAS) No. 62, Special Reports** (AICPA, Professional Standards, vol. 1, AU sec. 623.04), **as amended by SAS No. 77, Amendments to Statements on Auditing Standards No. 22, Planning and Supervision, No. 59, The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern, and No. 62, Special Reports** (AICPA, Professional Standards, vol. 1, AU sec. 623). Hereafter, reference to generally accepted accounting principles in this Statement includes, where applicable, an other comprehensive basis of accounting.

**6.4:** 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** (AICPA, Professional Standards, vol. 1, AU sec. 801).



## Safeguarding of Assets

13. Internal control over safeguarding of assets against unauthorized acquisition, use, or disposition may include controls relating to financial reporting and operations objectives. This relationship is depicted as follows:



In obtaining an understanding of each of the components of internal control to plan the audit, the auditor's consideration of safeguarding controls is generally limited to those relevant to the reliability of financial reporting. For example, use of a lockbox system for collecting cash or *access controls, such as passwords, that limit* ~~for limiting~~ access to *the data and programs that process cash disbursements* ~~accounts receivable data files~~ may be relevant to a financial statement audit. Conversely, controls to prevent the excess use of materials in production generally are not relevant to a financial statement audit.

## Application of Components to a Financial Statement Audit

14. The division of internal control into five components provides a useful framework for auditors to consider the impact of an entity's internal control in an audit. However, it does not necessarily reflect how an entity considers and implements internal control. Also, the auditor's primary consideration is whether a specific control affects financial statement assertions rather than its classification into any particular component. *Controls relevant to the audit are those that*

***individually or in combination with others are likely to prevent or detect material misstatements in financial statement assertions. Such controls may exist in any of the five components.***

15. The five components of internal control are applicable to the audit of every entity. The components should be considered in the context of—

- The entity's size.
- The entity's organization and ownership characteristics.
- The nature of the entity's business.
- 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.***<sup>7</sup> ~~methods of transmitting, processing, maintaining, and accessing information.~~
- ~~Applicable legal and regulatory requirements.~~

## **Effect of Information Technology on Internal Control**

***16. 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.***

7. See SAS No. 70, Service Organizations (AICPA, Professional Standards, vol. 1, AU sec. 324), as amended by SAS No. 88, Service Organizations and Reporting on Consistency (AICPA, Professional Standards, vol. 1, AU secs. 324.03 and 324.06-.10) for guidance if an entity obtains services that are part of its information system from another organization.

17. *The use of IT also affects the fundamental manner in which transactions are initiated, recorded, processed, and reported.<sup>8</sup> 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, 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. An entity's mix of manual and automated controls varies with the nature and complexity of the entity's use of IT.*

18. *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.*

---

8. Paragraph 12 of the appendix defines initiation, recording, processing, and reporting as used throughout this Statement.

- *Enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems.*

*19. IT also poses specific risks to an entity's internal control, including—*

- *Reliance on systems or programs that are inaccurately processing data, 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.*

*20. 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.*

## **Limitations of an Entity's Internal Control**

~~21.16.~~ Internal control, no matter how well designed and operated, can provide only reasonable assurance to management and the board of directors regarding achievement of **achieving** an entity's

control 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 ~~such~~ human failures *such* as simple errors or mistakes. *For example, errors may occur in designing, maintaining, or monitoring automated controls. If an entity's IT personnel do not completely understand how an order entry system processes sales transactions, they may erroneously design changes to the system to 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 dollar limit 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.*

22. 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 side agreements with customers that alter the terms and conditions of the entity's standard sales contract in ways that would preclude revenue recognition. Also, edit routines in a software program that are designed to identify and report transactions that exceed specified credit limits may be overridden or disabled.*

23.17. Another limiting factor is that *Internal control is influenced by the quantitative and qualitative estimates and judgments made by management in evaluating the cost-benefit relationship of an entity's internal control.* The cost of an entity's internal control should not exceed the benefits that are expected to be derived. Although the cost-benefit relationship is a primary criterion that should be considered in designing internal control, the precise measurement of costs and benefits usually is not possible. ~~Accordingly, management makes both quantitative and qualitative estimates and judgments in evaluating the cost-benefit relationship.~~

24.18. Custom, culture, and the corporate governance system may inhibit ~~irregularities by management~~ *fraud*, but they are not

absolute deterrents. An effective control environment, too, may help **reduce the risk of fraud**. ~~mitigate the probability of such irregularities.~~ For example, an effective board of directors, audit committee, and internal audit function may constrain improper conduct by management. Alternatively, the control environment may reduce the effectiveness of other components. For example, when the **nature** ~~presence~~ of management incentives **increases the risk of** ~~creates an environment that could result in~~ material misstatement of financial statements, the effectiveness of control activities may be reduced. ~~The effectiveness of an entity's internal control might also be adversely affected by such factors as a change in ownership or control, changes in management or other personnel, or developments in the entity's market or industry.~~

## **Obtaining an Understanding Consideration of Internal Control in Planning an Audit**

~~25.19.~~ In all audits, the auditor should obtain an understanding of each of the five components of internal control sufficient to plan the audit. **A sufficient understanding is obtained** by performing procedures to understand the design of controls relevant to an audit of financial statements; and **determining** whether they have been placed in operation. In planning the audit, such knowledge should be used to—

- Identify types of potential misstatement.
- Consider factors that affect the risk of material misstatement.
- **Design tests of controls, when applicable. Paragraphs 65 through 69 of this Statement discuss factors the auditor considers in determining whether to perform tests of controls.**
- Design substantive tests.

~~26.20.~~ The nature, timing, and extent of procedures the auditor chooses to perform to obtain the understanding will vary depending on the size and complexity of the entity, previous experience with the entity, the nature of the specific controls ~~involved~~ **used by the entity including the entity's use of IT, the nature and extent of changes in systems and operations**, and the nature of the entity's documentation of specific controls. For example, the understanding of risk assessment needed to plan an audit for an entity operating in a relatively stable environment may be limited. Also, the understand-

ing of monitoring needed to plan an audit for a small, noncomplex entity may be limited. **Similarly, the auditor may need only a limited understanding of control activities to plan an audit for a noncomplex entity that has significant owner-manager approval and review of transactions and accounting records. On the other hand, the auditor may need a greater understanding of control activities to plan an audit for an entity that has a large volume of revenue transactions and that relies on IT to measure and bill for services based on a complex, frequently changing rate structure.**

~~27.21.~~ Whether a control has been *placed in operation at a point in time* is different from its *operating effectiveness over a period of time*. In obtaining knowledge about whether controls have been placed in operation, the auditor determines that the entity is using them. Operating effectiveness, on the other hand, is concerned with how the control (***whether manual or automated***) was applied, the consistency with which it was applied, and by whom it was applied. ~~For example, a budgetary reporting system may provide adequate reports, but the reports may not be analyzed and acted on. This section does not require the auditor to obtain knowledge about operating effectiveness as part of the understanding of internal control.~~ **The auditor determines whether controls have been placed in operation as part of the understanding of internal control necessary to plan the audit. The auditor evaluates the operating effectiveness of controls as part of assessing control risk, as discussed in paragraphs 62 through 83 of this Statement. Although understanding internal control and assessing control risk are discussed separately in this Statement, they may be performed concurrently in an audit. Furthermore, some of the procedures performed to obtain the understanding may provide evidential matter about the operating effectiveness of controls relevant to certain assertions.**

~~28.22.~~ The auditor's understanding of internal control may sometimes 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. Concerns about the nature and extent of an entity's records may cause the auditor to conclude that it is unlikely

that sufficient competent evidential matter will be available to support an opinion on the financial statements.

### **Understanding of Internal Control Necessary to Plan the Audit**

~~29.23.~~ In making a judgment about the understanding of internal control necessary to plan the audit, the auditor considers the knowledge obtained from other sources about the types of misstatement that could occur, the risk that such misstatements may occur, and the factors that influence the design of **tests of controls, when applicable, and** substantive tests. Other sources of such knowledge include **information from** previous audits and the **auditor's** understanding of the industry **and market** in which the entity operates. The auditor also considers his or her assessment of inherent risk, judgments about materiality, and the complexity and sophistication of the entity's operations and systems, including ~~whether the~~ **extent to which the entity relies on** ~~method of controlling information processing is based on~~ manual **controls** ~~procedures independent of the computer or is highly dependent on~~ **automated** computerized controls. As an entity's operations and systems become more complex and sophisticated, it may be necessary to devote more attention to internal control components to obtain the understanding of them that is necessary to design effective substantive tests.

**30. In making a judgment about the understanding of internal control necessary to plan the audit, the auditor also considers IT risks that could result in misstatements. For example, if an entity uses IT to perform complex calculations, the entity receives the benefit of having the calculations consistently performed. However, the use of IT also presents risks, such as the risk that improperly authorized, incorrectly defined, or improperly implemented changes to the system or programs performing the calculations, or to related program tables or master files, could result in consistently performing those calculations inaccurately. As an entity's operations and systems become more complex and sophisticated, it becomes more likely that the auditor would need to increase his or her understanding of the internal control components to obtain the understanding necessary to design tests of controls, when applicable, and substantive tests.**



*31. The auditor should consider whether specialized skills are needed for the auditor to determine the effect of IT on the audit, to understand the IT controls, or to design and perform tests of IT controls or substantive tests. A professional possessing IT skills may be either on the auditor's staff or an outside professional. In determining whether such a professional is needed on the audit team, the auditor considers factors such as the following:*

- *The complexity of the entity's systems and IT controls and the manner in which they are used in conducting the entity's business*
- *The significance of changes made to existing systems, or the implementation of new systems*
- *The extent to which data is shared among systems*
- *The extent of the entity's participation in electronic commerce*
- *The entity's use of emerging technologies*
- *The significance of audit evidence that is available only in electronic form*

*32. Procedures that the auditor may assign to a professional possessing IT skills include inquiring of an entity's IT personnel how data and transactions are initiated, recorded, processed, and reported and how IT controls are designed; inspecting systems documentation; observing the operation of IT controls; and planning and performing tests of IT controls. If the use of a professional possessing IT skills is planned, the auditor should have sufficient IT-related knowledge to communicate the audit objectives to the professional, to evaluate whether the specified procedures will meet the auditor's objectives, and to evaluate the results of the procedures as they relate to the nature, timing, and extent of other planned audit procedures.<sup>9</sup>*

*33.24. Paragraphs 34 25 through 57 40 of this Statement provide an overview of the five internal control components and the auditor's understanding of the components relating to a financial statement audit. A more detailed discussion of these components is provided in the appendix A.*

<sup>9</sup> See SAS No. 22, Planning and Supervision (AICPA, Professional Standards, vol. 1, AU sec. 311.10), as amended by SAS No. 48, The Effects of Computer Processing on the Audit of Financial Statements.

### **Control Environment**

**34.25.** 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. Control environment factors include the following:

- a. Integrity and ethical values
- b. Commitment to competence
- c. Board of directors or audit committee participation
- d. Management's philosophy and operating style
- e. Organizational structure
- f. Assignment of authority and responsibility
- g. Human resource policies and practices

**35.26.** The auditor should obtain sufficient knowledge of the control environment to understand management's and the board of directors' attitude, awareness, and actions concerning the control environment, considering both the substance of controls and their collective effect. The auditor should concentrate on the substance of controls rather than their form, because controls may be established but not acted upon. For example, management may establish a formal code of conduct but act in a manner that condones violations of that code.

**36.27.** When obtaining an understanding of the control environment, the auditor considers the collective effect on the control environment of strengths and weaknesses in various control environment factors. 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 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, However, human resource policies and practices directed toward hiring competent financial, and accounting, and IT personnel may not mitigate a strong bias by top management to overstate earnings.***

## Risk Assessment

**37.28.** An entity's risk assessment for financial reporting purposes is its identification, analysis, and management of risks relevant to the preparation of financial statements that are fairly presented 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.

**38.29.** Risks relevant to financial reporting include external and internal events and circumstances that may occur and adversely affect an entity's ability to **initiate**, record, process, ~~summarize~~, and report financial data consistent with the assertions of management in the financial statements.<sup>105</sup> 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
- New technology
- New **business models**, ~~lines~~, products, or activities
- Corporate restructurings
- **Expanded f**Foreign operations
- **New a**Accounting pronouncements

**39.30.** 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. This knowledge might include understanding how management identifies risks, estimates the significance of the risks, assesses the likelihood of their occurrence, and relates them to financial reporting. ***The use of IT may be an important element in an entity's risk assessment process, including providing timely information to facilitate the identification and management of risks.***

<sup>105</sup> These assertions are discussed in SAS No. 31, **as amended by SAS No. 80** *Evidential Matter* (AICPA, *Professional Standards*, vol. 1, AU sec. 326).

~~40.31~~ An entity's risk assessment differs from the auditor's consideration of audit risk in a financial statement audit. The purpose of an entity's risk assessment is to identify, analyze, and manage risks that affect entity objectives. In a financial statement audit, the auditor assesses inherent and control risks to evaluate the likelihood that material misstatements could occur in the financial statements.

### **Control Activities**

~~41.32~~ Control activities are the policies and procedures that help ensure that management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities, *whether automated or manual*, have various objectives and are applied at various organizational and functional levels. Generally, control activities that may be relevant to an audit may be categorized as policies and procedures that pertain to the following:

- Performance reviews
- Information processing
- Physical controls
- Segregation of duties

~~42.33~~ The auditor should obtain an understanding of those control activities relevant to planning the audit. As the auditor obtains an understanding of the other components, he or she is also likely to obtain knowledge about some control activities. For example, in obtaining an understanding of the documents, records, and processing steps in the financial reporting information system that pertain to cash, the auditor is likely to become aware of whether bank accounts are reconciled. The auditor should consider the knowledge about the presence or absence of control activities obtained from the understanding of the other components in determining whether it is necessary to devote additional attention to obtaining an understanding of control activities to plan the audit. Ordinarily, audit planning does not require an understanding of the control activities related to each account balance, transaction class, and disclosure component in the financial statements or to every assertion relevant to them.

**43. *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, 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.*

*44. 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.*

*45. 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 and maintenance; access security; and application system acquisition, development, and maintenance.*

*46. 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.*

### **Information and Communication**

**47.34.** The information system relevant to financial reporting objectives, which includes the accounting system, consists of the **procedures**~~methods~~, **whether automated or manual**, and records established to **initiate**, record, process, summarize, and report entity transactions (as well as events and conditions) and to maintain account-

ability 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.

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

**49.36.** The auditor should obtain sufficient knowledge of the information system relevant to financial reporting to understand—

- The classes of transactions in the entity's operations that are significant to the financial statements.
- ***The procedures, both automated and manual, by which ~~How~~ these transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements.***
- The ***related*** accounting records, ***whether electronic or manual***, supporting information, and specific accounts in the financial statements involved in the ***initiating, recording***, processing, and reporting of transactions.
- ***How the information system captures other events and conditions that are significant to the financial statements.***
- ~~The accounting processing involved from the initiation of a transaction to its inclusion in the financial statements, including electronic means (such as computers and electronic data interchange) used to transmit, process, maintain, and access information.~~
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures.

**50.** ***When IT is used to initiate, 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.***

**51.** ***In obtaining an understanding of the financial reporting process, the auditor should understand the automated and manual procedures an entity uses to prepare financial statements***

*and related disclosures, and how misstatements may occur. Such procedures include—*

- *The procedures used to enter transaction totals into the general ledger. In some information systems, IT may be used to automatically transfer such information 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 automatically transfer information there may be little or no visible evidence of such intervention in the information systems.*
- *The procedures used to initiate, 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 monthly 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 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 difficult to identify through physical inspection of printed documents.*
- *Other procedures used to record recurring and nonrecurring adjustments to the financial statements. These are procedures that are not reflected in formal journal entries,*

***such as consolidating adjustments, report combinations, and reclassifications.***

~~52. In addition,~~ The auditor ***also*** should obtain sufficient knowledge of the means the entity uses to communicate financial reporting roles and responsibilities and significant matters relating to financial reporting.

### **Monitoring**

~~53.37.~~ An important management responsibility is to establish and maintain internal control. Management monitors controls to consider whether they are operating as intended and that they are modified as appropriate for changes in conditions.

~~54.38.~~ Monitoring is a process that assesses 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. This process is accomplished through ongoing activities, separate evaluations, or ~~a by various~~ combinations of the two. In many entities, internal auditors or personnel performing similar functions contribute to the monitoring of an entity's activities. 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. ***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 are accurate without having a basis for that assumption, errors may exist in the information, potentially leading management to incorrect conclusions from its monitoring activities.***

~~55.39.~~ The auditor should obtain sufficient knowledge of the major types of activities the entity uses to monitor internal control over financial reporting, including ***the source of the information related to those activities, and*** how those activities are used to initiate corrective actions. When obtaining an understanding of the internal audit function, the auditor should follow the guidance in ***Statement on Auditing Standards*** (SAS) No. 65, *The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, AU sec. 322.04-.08).



### **Application to Small and Midsized Entities**

~~56.40. As indicated in paragraph 15, the way in which the objectives of internal control are achieved~~ components apply will vary based on an entity's size and complexity, among other considerations. Specifically, small and midsized entities may use less formal means to ensure that internal control objectives are achieved. For example, smaller entities with active management involvement in the financial reporting process may not have extensive descriptions of accounting procedures, sophisticated information systems, or written policies. Smaller entities may 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, smaller entities may not have an independent or outside member on their board of directors. ~~However, these conditions may not affect the auditor's assessment of control risk.~~

57. When small or midsized entities are involved in complex transactions or are subject to legal and regulatory requirements also found in larger entities, more formal means of ensuring that internal control objectives are achieved may be present. **Also, small and midsized entities may use IT in various ways to achieve their objectives. For example, a small entity may use sophisticated applications of IT as part of its information system. The impact of IT on an entity's internal control is related more to the nature and complexity of the systems in use than to the entity's size.**

### **Procedures to Obtain Understanding**

~~58.41. In obtaining an understanding of controls that are relevant to audit planning, the auditor should perform procedures to obtain provide~~ sufficient knowledge **about** of the design of the relevant controls pertaining to each of the five internal control components and **determine** whether they have been placed in operation. This knowledge is ordinarily obtained through previous experience with the entity and procedures such as inquiries of appropriate management, supervisory, and staff personnel; inspection of entity documents and records; and observation of entity activities and operations. The nature and extent of the procedures performed generally vary from entity to entity and are influenced by the size and complexity of the entity, the auditor's previous experience with the entity, the nature of the particular control, and the nature of the entity's documentation of specific controls.

~~59.42.~~ For example, the auditor's prior experience with the entity may provide an understanding of its classes of transactions. Inquiries of appropriate entity personnel and inspection of documents and records, such as source documents, journals, and ledgers, may provide an understanding of the accounting records ~~designed to process those transactions and whether they have been placed in operation.~~ Similarly, in obtaining an understanding of the design of **automated computer-programmed controls activities** and **determining** whether they have been placed in operation, the auditor may make inquiries of appropriate entity personnel and inspect relevant systems documentation, **reports (for example, exception reports or reports evidencing the processing of transactions or application of other controls), or other documents.** ~~to understand control activity design and may inspect exception reports generated as a result of such control activities to determine that they have been placed in operation.~~

~~60.43.~~ The auditor's assessments of inherent risk and judgments about materiality for various account balances and transaction classes also affect the nature and extent of the procedures performed to obtain the understanding. For example, the auditor may conclude that planning the audit of the prepaid insurance account does not require specific procedures to be included in obtaining the understanding of internal control.

### **Documenting the ~~ation~~ of Understanding**

~~61.44.~~ The auditor should document the understanding of the entity's internal control components obtained to plan the audit. The form and extent of this documentation is influenced by the ~~size and complexity of the entity, as well as the nature~~ **and complexity** of the entity's ~~internal controls.~~ For example, documentation of the understanding of internal control of a ~~large~~ **complex information system entity in which a large volume of transactions are electronically initiated, recorded, processed, or reported** may include flowcharts, questionnaires, or decision tables. For an **information system making limited or no use of IT or for which few transactions are processed (for example, long-term debt)** ~~small entity, however,~~ documentation in the form of a memorandum may be sufficient. Generally, the more complex **the entity's** internal control and the more extensive the procedures performed **by the auditor**, the more extensive the auditor's documentation should be.

## **Consideration of Internal Control in Assessing Control Risk**

**62.45.** SAS No. 31, *Evidential Matter* (AICPA, *Professional Standards*, vol. 1, AU sec. 326), **as amended by SAS No. 80, Amendment to Statement on Auditing Standards No. 31, Evidential Matter**, states that most of the independent auditor's work in forming an opinion on financial statements consists of obtaining and evaluating evidential matter concerning the assertions in such financial statements. These assertions are embodied in the account balance, transaction class, and disclosure components of financial statements and are classified according to the following broad categories:

- Existence or occurrence
- Completeness
- Rights and obligations
- Valuation or allocation
- Presentation and disclosure

In planning and performing an audit, an auditor considers these assertions in the context of their relationship to a specific account balance or class of transactions.

**63.46.** The risk of material misstatement<sup>11.6</sup> in financial statement assertions consists of inherent risk, control risk, and detection risk. Inherent risk is the susceptibility of an assertion to a material misstatement assuming there are no related controls. Control risk is the risk that a material misstatement that could occur in an assertion will not be prevented or detected on a timely basis by the entity's internal control. Detection risk is the risk that the auditor will not detect a material misstatement that exists in an assertion.

**64.47.** Assessing control risk is the process of evaluating the effectiveness of an entity's internal control in preventing or detecting material misstatements in the financial statements. Control risk should be assessed in terms of financial statement assertions.

**11.6.** For purposes of this Statement, a material misstatement in a financial statement assertion is a misstatement whether caused by error or fraud as discussed in SAS No. 47, *Audit Risk and Materiality in Conducting an Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 312), **as amended by SAS No. 82, Consideration of Fraud in a Financial Statement Audit** (AICPA, *Professional Standards*, vol. 1, AU sec. 312), that either individually or when aggregated with other misstatements in other assertions would be material to the financial statements taken as a whole.

65. After obtaining the understanding of internal control, the auditor may assess control risk at the maximum level<sup>12</sup> for some or all assertions because he or she believes controls are unlikely to pertain to an assertion; **or** are unlikely to be effective, or because evaluating their effectiveness **of controls** would be inefficient.<sup>7</sup> *However, the auditor needs to be satisfied that performing only substantive tests would be effective in restricting detection risk to an acceptable level. For example, the auditor may determine that performing only substantive tests would be effective and more efficient than performing tests of controls for assertions related to fixed assets and to long-term debt in an entity where a limited number of transactions are related to those financial statement components, and when the auditor can readily obtain corroborating evidence in the form of documents and confirmations. In circumstances where the auditor is performing only substantive tests in restricting detection risk to an acceptable level and where the information used by the auditor to perform such substantive tests is produced by the entity's information system, the auditor should obtain evidence about the accuracy and completeness of the information.*

66. *In other circumstances, the auditor may determine that assessing control risk below the maximum level for certain assertions would be effective and more efficient than performing only substantive tests. In addition, the auditor may determine that it is not practical or possible to restrict detection risk to an acceptable level by performing only substantive tests for one or more financial statement assertions. In such circumstances, the auditor should obtain evidential matter about the effectiveness of both the design and operation of controls to reduce the assessed level of control risk.*<sup>13</sup>

67. *In determining whether assessing control risk at the maximum level or at a lower level would be an effective approach for specific assertions, the auditor should consider—*

---

12. See footnote 3.

7. Control risk may be assessed in quantitative terms, such as percentages, or in nonquantitative terms that range, for example, from a maximum to a minimum. The term *maximum level* is used in this Statement to mean the greatest probability that a material misstatement that could occur in a financial statement assertion will not be prevented or detected on a timely basis by an entity's internal control.

13. See footnote 4.

- *The nature of the assertion.*
- *The volume of transactions or data related to the assertion.*
- *The nature and complexity of the systems, including the use of IT, by which the entity processes and controls information supporting the assertion.*
- *The nature of the available evidential matter, including audit evidence that is available only in electronic form.*

68. *In circumstances where a significant amount of information supporting one or more financial statement assertions is electronically initiated, recorded, processed, or reported, the auditor may determine that it is not possible to design effective substantive tests that by themselves would provide sufficient evidence that the assertions are not materially misstated. For such assertions, significant audit evidence may be available only in electronic form. In such cases, its competence and sufficiency as evidential matter 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, recorded, processed, or reported only in electronic form and appropriate controls are not operating effectively. In such circumstances, the auditor should perform tests of controls to gather evidential matter to use in assessing control risk.*

69. *Examples of situations where the auditor may find it impossible to design effective substantive tests that by themselves would provide sufficient evidence that certain assertions are not materially misstated include the following:*

- *An entity that conducts business using IT to initiate orders for goods based on predetermined decision rules and to pay the related payables based on system-generated information regarding receipt of goods. No other documentation of orders or goods received is produced or maintained.*
- *An entity that provides electronic services to customers (for example, an Internet service provider or a telephone company) and uses IT to log services provided to users, initiate bills for the services, process the billing transactions, and automatically record such amounts in electronic accounting records that are used to produce the financial statements.*

## **Assessing Control Risk Below the Maximum Level**

**70.48:** Assessing control risk ~~at~~ below the maximum level involves<sup>14</sup>—

- Identifying specific controls relevant to specific assertions ~~that are likely to prevent or detect material misstatements in those assertions.~~
- Performing tests of controls ~~to evaluate the effectiveness of such controls.~~
- *Concluding on the assessed level of control risk.*

### **Identifying Specific Controls Relevant to Specific Assertions**

**71.49:** *The auditor's understanding about internal control should be used to identify the types of potential misstatements that could occur and to consider factors that affect the risk of material misstatement. In assessing control risk, the auditor should identify the controls that are likely to prevent or detect material misstatement in specific assertions.* In identifying controls relevant to specific financial statement assertions, the auditor should consider that the controls can have either a pervasive effect on many assertions or a specific effect on an individual assertion, depending on the nature of the particular internal control component involved. For example, the conclusion that an entity's control environment is highly effective may influence the auditor's decision about the number of an entity's locations at which auditing procedures are to be performed or whether to perform certain auditing procedures for some account balances or transaction classes at an interim date. Either decision affects the way in which auditing procedures are applied to specific assertions, even though the auditor may not have specifically considered each individual assertion that is affected by such decisions.

**72.50:** Conversely, some control activities *may* ~~often~~ have a specific effect on an individual assertion embodied in a particular account balance or transaction class. 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 assertion for the inventory account balance.

<sup>14</sup> SAS No. 70, as amended by SAS No. 88, describes reports that an auditor may obtain that may assist in identifying controls relevant to specific assertions and obtaining evidential matter regarding their operating effectiveness when an entity uses a service organization.

~~73.51.~~ Controls can be either directly or indirectly related to an assertion. The more indirect the relationship, the less effective that control may be in reducing control risk for that assertion. For example, a sales manager's review of a summary of sales activity for specific stores by region ordinarily is indirectly related to the completeness assertion for sales revenue. Accordingly, it may be less effective in reducing control risk for that assertion than controls more directly related to that assertion, such as matching shipping documents with billing documents.

**74. General controls relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. The auditor should consider the need to identify not only application controls directly related to one or more assertions, but also relevant general controls.**

### Performing Tests of Controls

~~75.52.~~ Procedures directed toward either the effectiveness of the design or operation of a control are referred to as tests of controls. **Procedures** Tests of controls directed toward **evaluating** the effectiveness of the design of a control are concerned with whether that control is suitably designed to prevent or detect material misstatements in specific financial statement assertions. **Procedures** Tests to obtain such evidential matter ordinarily include ~~procedures such as~~ inquiries of appropriate entity personnel; inspection of documents, ~~and~~ reports, **or electronic files**; and observation of the application of specific controls. For entities with complex internal control, the auditor should consider ~~that~~ the use of flowcharts, questionnaires, or decision tables **to might** facilitate the application of **procedures directed toward evaluating the effectiveness** tests of **the design of a control**.

~~76.53.~~ **Procedures to obtain evidential matter about the effectiveness of the operation of a control are referred to as tests of controls (paragraphs 90 through 104 of this Statement discuss characteristics of evidential matter to consider when performing tests of controls).** Tests of controls directed toward the operating effectiveness of a control are concerned with how the control (**whether manual or automated**) was applied, the consistency with which it was applied during the audit period, and by whom it was applied. These tests ordinarily include procedures such as inquiries of appropriate entity personnel; inspection of documents,

reports, or electronic files, indicating performance of the control; observation of the application of the control; and reperformance of the application of the control by the auditor. In some circumstances, a specific procedure may address the effectiveness of both design and operation. However, a combination of procedures may be necessary to evaluate the effectiveness of the design or operation of a control.

*77. In designing tests of automated controls, the auditor should consider the need to obtain evidence supporting the effective operation of controls directly related to the assertions as well as other indirect controls on which these controls depend. For example, the auditor may identify a "user review of an exception report of credit sales over a customer's authorized credit limit" as a direct control related to an assertion. In such cases, the auditor should consider the effectiveness of the user review of the report and also the controls related to the accuracy of the information in the report (for example, the general controls).*

*78. Because of the inherent consistency of IT processing, the auditor may be able to reduce the extent of testing of an automated control. For example, a programmed application control should function consistently unless the program (including the tables, files, or other permanent data used by the program) is changed. Once the auditor determines that an automated control is functioning as intended (which could be done at the time the control is initially implemented or at some other date), the auditor should consider performing tests to determine that the control continues to function effectively. Such tests might include determining that changes to the program are not made without being subject to the appropriate program change controls, that the authorized version of the program is used for processing transactions, and that other relevant general controls are effective. Such tests also might include determining that changes to the programs have not been made, as may be the case when the entity uses packaged software applications without modifying or maintaining them.*

*79. To test automated controls, the auditor may need to use techniques that are different from those used to test manual controls. For example, computer-assisted audit techniques may be used to test automated controls or data related to assertions. Also, the auditor may use other automated tools or reports produced*



*by IT to test the operating effectiveness of general controls, such as program change controls, access controls, and system software controls. The auditor should consider whether specialized skills are needed to design and perform such tests of controls.*

### **Concluding on the Assessed Level of Control Risk**

**80.54.** The conclusion reached as a result of assessing control risk is referred to as the assessed level of control risk. In determining the evidential matter necessary to support ~~an~~ **specific** assessed level of control risk ~~at~~ below the maximum level, the auditor should consider the characteristics of evidential matter about control risk discussed in paragraphs **90 64** through **104 78**. Generally, however, the lower the assessed level of control risk, the greater the assurance the evidential matter must provide that the controls relevant to an assertion are designed and operating effectively.

**81.55.** The auditor uses the assessed level of control risk (together with the assessed level of inherent risk) to determine the acceptable level of detection risk for financial statement assertions. The auditor uses the acceptable level of detection risk to determine the nature, timing, and extent of the auditing procedures to be **applied to the account balance or class of transactions** ~~used~~ to detect material misstatements in the financial statement assertions. Auditing procedures designed to detect such misstatements are referred to in this Statement as substantive tests.

**82.56.** As the acceptable level of detection risk decreases, the assurance provided from substantive tests should increase. Consequently, the auditor may do one or more of the following:

- Change the nature of substantive tests from a less effective to a more effective procedure, such as using tests directed toward independent parties outside the entity rather than tests directed toward parties or documentation within the entity.
- Change the timing of substantive tests, such as performing them at year end rather than at an interim date.
- Change the extent of substantive tests, such as using a larger sample size.

## **Documenting ~~ation~~ of the Assessed Level of Control Risk**

~~83.57.~~ In addition to the documentation of the understanding of internal control discussed in paragraph ~~61 44~~, the auditor should document ~~the basis for~~ his or her conclusions about the assessed level of control risk. Conclusions about the assessed level of control risk may differ as they relate to various account balances or classes of transactions. ~~However, f~~For those financial statement assertions where control risk is assessed at the maximum level, the auditor should document his or her conclusion that control risk is at the maximum level but need not document the basis for that conclusion. For those assertions where the assessed level of control risk is below the maximum level, the auditor should document the basis for his or her conclusion that the effectiveness of the design and operation of controls supports that assessed level. The nature and extent of the auditor's documentation are influenced by the assessed level of control risk ~~used~~, the nature of the entity's internal control, and the nature of the entity's documentation of internal control.

## **Relationship of Understanding to Assessing Control Risk**

~~84.58.~~ Although understanding internal control and assessing control risk are discussed separately in this Statement, they may be performed concurrently in an audit. The objective of procedures performed to obtain an understanding of internal control (discussed in paragraphs ~~58 41~~ through ~~60 43~~) is to provide the auditor with knowledge necessary for audit planning. The objective of tests of controls (discussed in paragraphs ~~75 52~~ **through** ~~and 79 53~~) is to provide the auditor with evidential matter to use in assessing control risk. However, procedures performed to achieve one objective may also pertain to the other objective.

~~85.59.~~ Based on the assessed level of control risk the auditor expects to support and audit efficiency considerations, the auditor often plans to perform some tests of controls concurrently with obtaining the understanding of internal control. In addition, even though some of the procedures performed to obtain the understanding ~~were may~~ not have been specifically planned as tests of controls, they may ~~also~~ **nevertheless** provide evidential matter about the

effectiveness of both the design and operation of the controls relevant to certain assertions ~~and, consequently, serve as tests of controls.~~ For example, *because of the inherent consistency of IT processing, performing procedures to determine whether an automated control has been placed in operation may serve as a test of that control's operating effectiveness, depending on such factors as whether the program has been changed or whether there is a significant risk of unauthorized change or other improper intervention.* Also, in obtaining an understanding of the control environment, the auditor may have made inquiries about management's use of budgets, observed management's comparison of monthly budgeted and actual expenses, and inspected reports pertaining to the investigation of variances between budgeted and actual amounts. Although these procedures provide knowledge about the design of the entity's budgeting policies and whether they have been placed in operation, they may also provide evidential matter about the effectiveness of the ~~design and~~ operation of budgeting policies in preventing or detecting material misstatements in the classification of expenses. In some circumstances, that evidential matter may be sufficient to support an assessed level of control risk that is below the maximum level for the presentation and disclosure assertions pertaining to expenses in the income statement.

~~86.60.~~ When the auditor concludes that procedures performed to obtain the understanding of internal control also provide evidential matter for assessing control risk, he or she should consider the guidance in paragraphs ~~90 64~~ through ~~104 78~~ in judging the degree of assurance provided by that evidential matter. Although such evidential matter may not provide sufficient assurance to support an assessed level of control risk that is below the maximum level for certain assertions, it may do so for other assertions and thus provide a basis for modifying the nature, timing, or extent of the substantive tests that the auditor plans for those assertions. However, such procedures are not sufficient to support an assessed level of control risk below the maximum level if they do not provide sufficient evidential matter to evaluate the effectiveness of both the design and operation of a control relevant to an assertion.

### **Further Reduction in the Assessed Level of Control Risk**

~~87.61.~~ After obtaining the understanding of internal control and assessing control risk, the auditor may desire to ~~seek a~~ further reduce

tion in the assessed level of control risk for certain assertions. In such cases, the auditor considers whether additional evidential matter sufficient to support a further reduction is likely to be available, and whether it would be efficient to perform tests of controls to obtain that evidential matter. The results of the procedures performed to obtain the understanding of the internal control, as well as pertinent information from other sources, help the auditor to evaluate those two factors.

~~88.62.~~ In considering efficiency, the auditor recognizes that additional evidential matter that supports a further reduction in the assessed level of control risk for an assertion would result in less audit effort for the substantive tests of that assertion. The auditor weighs the increase in audit effort associated with the additional tests of controls that is necessary to obtain such evidential matter against the resulting decrease in audit effort associated with the reduced substantive tests. ~~When the auditor concludes it is inefficient to obtain additional evidential matter for specific assertions, the auditor uses the assessed level of control risk based on the understanding of internal control in planning the substantive tests for those assertions.~~

~~89.62.~~ For those assertions for which the auditor performs additional tests of controls, the auditor determines the assessed level of control risk that the results of those tests will support. This assessed level of control risk is used in determining the appropriate detection risk to accept for those assertions and, accordingly, in determining the nature, timing, and extent of substantive tests for such assertions.

## **Evidential Matter to Support the Assessed Level of Control Risk**

90.64. When the auditor assesses control risk at below the maximum level, he or she should obtain sufficient evidential matter to support that assessed level. The evidential matter<sup>15\*</sup> that is sufficient to support a specific assessed level of control risk is a matter of auditing judgment. Evidential matter varies substantially in the assurance it provides to the auditor as he or she develops an assessed level of control risk. The type of evidential matter, its source, its timeliness, and the existence of other evidential matter related to the conclusion to which it leads all bear on the degree of assurance evidential matter provides.

<sup>15.\*</sup> See also SAS No. 31, *as amended by SAS No. 80*, for guidance on evidential matter.

**91.65.** These characteristics influence the nature, timing, and extent of the tests of controls that the auditor applies to obtain evidential matter about control risk. The auditor selects such tests from a variety of techniques such as inquiry, observation, inspection, and reperformance of a control that pertains to an assertion. No one specific test of controls is always necessary, applicable, or equally effective in every circumstance.

### **Type of Evidential Matter**

**92.66.** The nature of the particular controls that pertain to an assertion influences the type of evidential matter that is available to evaluate the effectiveness of the design or operation of those controls. For some controls, documentation of design or operation may exist. In such circumstances, the auditor may decide to inspect the documentation to obtain evidential matter about the effectiveness of design or operation.

**93.67.** For other controls, however, such documentation may not be available or relevant. For example, documentation of design or operation may not exist for some factors in the control environment, such as assignment of authority and responsibility, or for some types of control activities, such as **undocumented monitoring controls** segregation of duties or some control activities performed by a computer. In such circumstances, evidential matter about the effectiveness of design or operation may be obtained through **such methods as** observation, **inquiry**, or the use of computer-assisted audit techniques to reperform the application of relevant controls.

### **Source of Evidential Matter**

**94.68.** Generally, evidential matter about the effectiveness of the design and operation of controls obtained directly by the auditor, such as through observation, provides more assurance than evidential matter obtained indirectly or by inference, such as through inquiry. For example, evidential matter about the proper segregation of duties that is obtained by the auditor's direct personal observation of the individual who applies a control generally provides more assurance than making inquiries about the **application of the control** individual. The auditor should consider, however, that the observed application of a control might not be performed in the same manner when the auditor is not present.

~~95.69.~~ Inquiry alone generally will not provide sufficient evidential matter to support a conclusion about the effectiveness of design or operation of a specific control. When the auditor determines that a specific control may have a significant effect in reducing control risk to a low level for a specific assertion, he or she ordinarily needs to perform additional tests to obtain sufficient evidential matter to support the conclusion about the effectiveness of the design or operation of that control.

### **Timeliness of Evidential Matter**

~~96.70.~~ The timeliness of the evidential matter concerns when it was obtained and the portion of the audit period to which it applies. In evaluating the degree of assurance that is provided by evidential matter, the auditor should consider that the evidential matter obtained by some tests of controls, such as observation, pertains only to the point in time at which the auditing procedure was applied. Consequently, such evidential matter may be insufficient to evaluate the effectiveness of the design or operation of controls for periods not subjected to such tests. In such circumstances, the auditor may decide to supplement *those* ~~these~~ tests with other tests of controls that are capable of providing evidential matter about the entire audit period. For example, for *an application* control activity performed by a computer program, the auditor may test the operation of the control at a particular point in time to obtain evidential matter about whether ~~the program executes~~ the control *is operating* effectively *at that point in time*. The auditor may then perform tests of controls directed toward *obtaining evidential matter about whether the application control operated consistently during the audit period, such as tests of general controls pertaining to the modification and use of that computer program during the audit period.* ~~the design and operation of other control activities pertaining to the modification and the use of that computer program during the audit period to obtain evidential matter about whether the programmed control activity operated consistently during the audit period.~~

~~97.71.~~ Evidential matter about the effective design or operation of controls that was obtained in prior audits may be considered by the auditor in assessing control risk in the current audit. To evaluate the use of such evidential matter for the current audit, the auditor should consider the significance of the assertion involved, the specific controls that were evaluated during the prior audits, the degree to which the

effective design and operation of those controls were evaluated, the results of the tests of controls used to make those evaluations, and the evidential matter about design or operation that may result from substantive tests performed in the current audit. The auditor should also consider that the longer the time elapsed since ~~the performance of~~ tests of controls **were performed** to obtain evidential matter about control risk, the less assurance **they** ~~it~~ may provide.

**98.72.** When considering evidential matter obtained from prior audits, the auditor should obtain evidential matter in the current period about whether changes have occurred in internal control, including its policies, procedures, and personnel, subsequent to the prior audits, as well as the nature and extent of any such changes. ***For example, in performing the prior audit, the auditor may have determined that an automated control was functioning as intended. The auditor should obtain evidence to determine whether changes to the automated control have been made that would affect its continued effective functioning.*** Consideration of evidential matter about these changes, together with the considerations in the preceding paragraph, may support either increasing or decreasing the ~~additional~~ evidential matter about the effectiveness of design and operation to be obtained in the current period.

**99.73.** When the auditor obtains evidential matter about the design or operation of controls during an interim period, he or she should determine what additional evidential matter should be obtained for the remaining period. In making that determination, the auditor should consider the significance of the assertion involved, the specific controls that were evaluated during the interim period, the degree to which the effective design and operation of those controls were evaluated, the results of the tests of controls used to make that evaluation, the length of the remaining period, and the evidential matter about design or operation that may result from the substantive tests performed in the remaining period. The auditor should obtain evidential matter about the nature and extent of any significant changes in internal control, including its policies, procedures, and personnel, that occur subsequent to the interim period.

### **Interrelationship of Evidential Matter**

**100.74.** The auditor should consider the combined effect of various types of evidential matter relating to the same assertion in evaluat-

ing the degree of assurance that evidential matter provides. In some circumstances, a single type of evidential matter may not be sufficient to evaluate the effective design or operation of a control. To obtain sufficient evidential matter in such circumstances, the auditor may perform other tests of controls pertaining to that control. For example, an auditor may observe ***the procedures for opening the mail and processing cash receipts to evaluate the operating effectiveness of controls over cash receipts*** that programmers are not authorized to operate the computer. Because an observation is pertinent only at the point in time at which it is made, the auditor may supplement the observation with inquiries ***of entity personnel and inspection of documentation about the operation of such controls at other times during the audit period*** about the frequency and circumstances under which programmers may have access to the computer and may inspect documentation of past instances when programmers attempted to operate the computer to determine how such attempts were prevented or detected.

**101.75:** In addition, when evaluating the degree of assurance provided by evidential matter, the auditor should consider the interrelationship of an entity's control environment, risk assessment, control activities, information and communication, and monitoring. Although an individual internal control component may affect the nature, timing, or extent of substantive tests for a specific financial statement assertion, the auditor should consider the evidential matter about an individual component in relation to the evidential matter about the other components in assessing control risk for a specific assertion.

**102.76:** Generally, when various types of evidential matter support the same conclusion about the design or operation of a control, the degree of assurance provided increases. Conversely, if various types of evidential matter lead to different conclusions about the design or operation of a control, the assurance provided decreases. For example, based on the evidential matter that the control environment is effective, the auditor may have reduced the number of locations at which auditing procedures will be performed. If, however, when evaluating specific control activities, the auditor obtains evidential matter that such activities are ineffective, he or she may reevaluate his or her conclusion about the control environment and, among other things, decide to perform auditing procedures at additional locations.



**103.77.** Similarly, evidential matter indicating that the control environment is ineffective may adversely affect an otherwise effective control for a particular assertion. For example, a control environment that is likely to permit unauthorized changes in a computer program may reduce the assurance provided by evidential matter obtained from evaluating the effectiveness of the program at a particular point in time. In such circumstances, the auditor may decide to obtain additional evidential matter about the design and operation of that program during the audit period. For example, the auditor might obtain and control a copy of the program and use computer-assisted audit techniques to compare that copy with the program that the entity uses to process data.

**104.78.** An audit of financial statements is a cumulative process; as the auditor assesses control risk, the information obtained may cause him or her to modify the nature, timing, or extent of the other planned tests of controls for assessing control risk. In addition, information may come to the auditor's attention as a result of performing substantive tests or from other sources during the audit that differs significantly from the information on which his or her planned tests of controls for assessing control risk were based. For example, the extent of misstatements that the auditor detects by performing substantive tests may alter his or her judgment about the assessed level of control risk. In such circumstances, the auditor may need to reevaluate the planned substantive procedures, based on a revised consideration of the assessed level of control risk for all or some of the financial statement assertions.

---

## **Correlation of Control Risk With Detection Risk**

**105.79.** The ultimate purpose of assessing control risk is to contribute to the auditor's evaluation of the risk that material misstatements exist in the financial statements. The process of assessing control risk (together with assessing inherent risk) provides evidential matter about the risk that such misstatements may exist in the financial statements. The auditor uses this evidential matter as part of the reasonable basis for an opinion referred to in the third standard of field work, which follows:

Sufficient competent evidential matter is to be obtained through inspection, observation, inquiries, and confirmations to afford a reasonable basis for an opinion regarding the financial statements under audit.

**106.80.** After considering the level to which he or she seeks to restrict the risk of a material misstatement in the financial statements and the assessed levels of inherent risk and control risk, the auditor performs substantive tests to restrict detection risk to an acceptable level. As the assessed level of control risk decreases, the acceptable level of detection risk increases. Accordingly, the auditor may alter the nature, timing, and extent of the substantive tests performed.

**107.81.** Although the inverse relationship between control risk and detection risk may permit the auditor to change the nature or the timing of substantive tests or limit their extent, ordinarily the assessed level of control risk cannot be sufficiently low to eliminate the need to perform any substantive tests to restrict detection risk for all of the assertions relevant to significant account balances or transaction classes. Consequently, regardless of the assessed level of control risk, the auditor should perform substantive tests for significant account balances and transaction classes.

**108.82.** The substantive tests that the auditor performs consist of tests of details of transactions and balances, and analytical procedures. In assessing control risk, the auditor also may use tests of details of transactions as tests of controls. The objective of tests of details of transactions performed as substantive tests is to detect material misstatements in the financial statements. The objective of tests of details of transactions performed as tests of controls is to evaluate whether a control operated effectively. Although these objectives are different, both may be accomplished concurrently through performance of a test of details on the same transaction. The auditor should recognize, however, that careful consideration should be given to the design and evaluation of such tests to ensure that both objectives will be accomplished.

**109.83.**

## **Effective Date**

**109.83.** This section is effective for audits of financial statements for periods beginning on or after January 1, 1990. Paragraphs 1 to 40 and the appendix are effective for audits of financial statements for periods beginning on or after January 1, 1997. Early application of the provisions of this section is permissible. ***This amendment is effective for audits of financial statements for periods beginning on or after June 1, 2001. Earlier application is permissible.***

## APPENDIX

# Internal Control Components

1. This appendix discusses the five internal control components set forth in paragraph 7 and **further** ~~briefly~~ described in paragraphs 34 ~~25~~ through 57 ~~40~~ as they relate to a financial statement audit.

~~OBJECTIVE~~

## Control Environment

2. 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.

3. The control environment encompasses the following factors:

- a. *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, affecting the design, administration, and monitoring of other components. 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. *Board of directors or audit committee participation.* An entity's control consciousness is influenced significantly by the entity's board of directors or audit committee. Attributes include the board or audit committee's independence from management, the experi-

ence and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, 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 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 monitored. 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 hiring, orientation, training, evaluating, counseling, promoting, compensating, and remedial actions. For example, standards for hiring 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**

4. Small and midsized entities may implement the control environment factors 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, smaller entities may not have an independent or outside member on their board of directors. ~~However, these conditions may not affect the auditor's assessment of control risk.~~

### **Risk Assessment**

5. An entity's risk assessment for financial reporting purposes is its identification, analysis, and management of risks relevant to the preparation of financial statements that are fairly presented 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.

6. Risks relevant to financial reporting include external and internal events and circumstances that may occur and adversely affect an entity's ability to *initiate*, record, process, ~~summarize~~, 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 circumstances such 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**, lines, 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 ~~impact~~ **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**

7. The basic concepts of the risk assessment process should be present in 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.

## Control Activities

8. Control activities are the policies and procedures that help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities, *whether automated or manual*, have various objectives and are applied at various organizational and functional levels.

9. 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 reviews of 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; and review of 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* and *application 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.* General controls commonly include controls over data center *and network* operations; system software acquisition and maintenance; access security; and application system *acquisition*, development, and maintenance. These controls apply to mainframe, *miniframe*~~minicomputer~~, 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.* Application controls apply to the processing of individual applications. These controls help ensure that transactions are valid, properly authorized, and completely and accurately processed.

- *Physical controls.* These activities encompass the physical security of assets, including adequate safeguards such as secured facilities, over 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. 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 ~~the~~ the 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** irregularities in the normal course of his or her duties.

### **Application to Small and Midsized Entities**

10. The concepts underlying control activities in small or mid-sized 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 their responsibilities to achieve appropriate segregation or, if that is not possible, to use management oversight of the incompatible activities to achieve control objectives.



## Information and Communication

**11.** *An information system consists of infrastructure (physical and hardware components), software, people, procedures (manual and automated), and data. Infrastructure and software will be absent, or have less significance, in systems that are exclusively or primarily manual. Many information systems make extensive use of information technology.*

**12.11.** *The information system relevant to financial reporting objectives, which includes the accounting system, consists of the ~~procedures~~ methods, whether automated or manual, and records established to initiate, record, process, summarize, 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. 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 automated 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 monitoring and 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.

**13.12.** *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.

**14.13.** 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.

**15.14.** 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**

**16.15.** Information systems in small or midsized organizations are likely to be less formal 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 midsized 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.

---

## **Monitoring**

**17.16.** Monitoring is a process that assesses 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. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

**18.17.** 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.

**19.18.** In many entities, internal auditors or personnel performing similar functions contribute to the monitoring of an entity's activ-

ities 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.

**20.19.** Monitoring activities may include using information from communications from external parties. 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**

**21.20.** 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.

*This Statement entitled The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit was unanimously adopted by the assenting votes of the fifteen members of the board.*

### **Auditing Standards Board (2000–2001)**

James S. Gerson, *Chair*  
O. Ray Whittington, *Vice Chair*  
Linda K. Cheatham  
Craig W. Crawford  
Robert F. Dacey  
Richard Dieter  
Sally L. Hoffman  
Michael P. Manspeaker  
W. Scott McDonald  
Susan L. Menelaides  
Keith O. Newton  
Alan G. Paulus

Robert C. Steiner  
Bruce P. Webb  
Carl L. Williams III

---

Arleen R. Thomas  
*Vice President*  
*Professional Standards*  
*and Services*  
Julie Anne Dilley  
*Technical Manager*  
*Audit and Attest Standards*

### **Technology Issues Task Force**

George H. Tucker, *Chair*  
Jayne E. Burke  
Robert Dohrer  
James E. Grossman  
Stephen W. Head

Carol A. Langelier  
Keith O. Newton  
Thomas E. Wallace  
O. Ray Whittington

**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 of the Institute's Code of Professional Conduct requires compliance with these standards.*

