EXPOSURE DRAFT

PROPOSED STATEMENT ON AUDITING STANDARDS

UNDERSTANDING THE ENTITY AND ITS ENVIRONMENT AND ASSESSING THE RISKS OF MATERIAL MISSTATEMENT

(Supersedes Statement on Auditing Standards [SAS] No. 122,* Statements on Auditing Standards: Clarification and Recodification*, as amended, section 315,* Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement *[AICPA, Professional Standards, AU-C sec. 315]; Amends:

- ***SAS No. 117,* Compliance Audits, *as amended [AICPA, Professional Standards, AU-C sec. 935]***
- ***Various other sections in SAS No. 122, as amended [AICPA,* Professional Standards*, AU-C secs. 200, 210, 240, 250, 260, 265, 300, 330, 402, 501, 530, 550, 600, 620, and 930])***
- ***SAS No. 128,* Using the Work of Internal Auditors *[AICPA,* Professional Standards*, AU-C sec. 610]***
- ***SAS No. 134,* Auditor Reporting and Amendments, Including Amendments Addressing Disclosures in the Audit of Financial Statements*, as amended***
  - ***Section 701,* Communicating Key Audit Matters in the Independent Auditor's Report *[AICPA,* Professional Standards*, AU-C sec. 701]***
- ***SAS No. 137,* The Auditor's Responsibilities Relating to Other Information Included in Annual Reports, *as amended [AICPA,* Professional Standards*, AU-C sec. 720]***
- ***SAS No. 140,* An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements, *as amended [AICPA,* Professional Standards*, AU-C sec. 940]***
- ***SAS No. 143,* Auditing Accounting Estimates and Related Disclosures *[AICPA,* Professional Standards*, AU-C sec. 540])***

August 27, 2020

Comments are requested by November 25, 2020

Prepared by the AICPA Auditing Standards Board for comment from persons interested in auditing and reporting issues.

Comments should be addressed to CommentLetters@aicpa-cima.com

CONTENTS

Explanatory Memorandum

Introduction

This memorandum provides background to the proposed Statement on Auditing Standards (SAS) *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*. If issued as final, this proposed SAS will supersede SAS No. 122, *Statements on Auditing Standards: Clarification and Recodification*, as amended, section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* (AU-C section 315).[1]

Background

SAS No. 122 was issued by the Auditing Standards Board (ASB) in October 2011 to apply the clarity drafting conventions to all outstanding SASs issued by the ASB through SAS No. 121, including AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*.

The AICPA's Enhancing Audit Quality Initiative identified the auditor's risk assessment as an area of focus in 2019, in part, because deficiencies in the process of obtaining the required understanding of internal control is a common audit issue identified by practice monitoring programs worldwide.

This project to enhance the auditing standards relating to the auditor's risk assessment is intended to enable auditors to appropriately address the following:

a. Understanding the entity's system of internal control, in particular, relating to the auditor's work effort to obtain the necessary understanding

b. Modernizing the standard in relation to IT considerations, including addressing risks arising from entity's use of IT

c. Determining risks of material misstatements, including significant risks

The ASB has monitored developments related to the auditor's risk assessment. In particular, the ASB followed the project of the International Auditing and Assurance Standards Board (IAASB) to revise International Standard on Auditing (ISA) 315, *Identifying and Assessing the Risks of Material Misstatement* (ISA 315 Revised). ISA 315 (Revised) is effective for audits of financial statements for periods beginning on or after December 15, 2021.The ASB Risk Assessment Task Force was formed to consider the implications of this project when identifying assessing the risks of material misstatements for audits of nonissuers.

Convergence

The ASB has a strategy to converge its standards with those of the IAASB. In doing that, the ASB uses the corresponding ISA as the base in developing its standards. In making the proposed

[1] All AU-C sections can be found in AICPA *Professional Standards*.

revisions to the accompanying proposed SAS, the ASB used ISA 315 (Revised) as the base. The ASB has made certain changes to the language in ISA 315 (Revised) to use terms or phrases that are more common in the United States and to tailor examples and guidance to the U.S. environment.

Effective Date

If issued as final, the proposed SAS will be effective for audits of financial statements for periods ending on or after December 15, 2023.

Fundamental Aspects of the Proposed SAS

I. Public Interest Issues Addressed in the Proposed SAS

Although all the proposed revisions in this exposure draft are made with the public interest in the forefront, revisions that are most important in supporting the public interest are set out in the sections that follow.

A proper identification and assessment of the risks of material misstatement drives the performance of a quality audit because a proper risk assessment is the basis on which the auditor plans and performs audit procedures and gathers audit evidence to support the audit opinion on the financial statements.

The proposed SAS builds on the foundational concepts relating to an audit of financial statements in AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards*, (such as audit risk, identifying risks at the financial statement and assertion levels, and the definitions of *inherent risk* and *control risk*). In undertaking the revision of extant AU-C section 315, the ASB did not seek to fundamentally change the key concepts underpinning audit risk as the ASB continues to have the view that the audit risk model is fundamentally sound. Rather, the ASB focused on how certain aspects of the identification and assessment of the risks of material misstatement can be clarified and improved in order to drive better risk assessments and, therefore, enhance audit quality.

Scalability

In proposing revisions to the proposed SAS, the ASB recognizes that the auditor's ability to serve the public interest includes the ability to apply the standard to the audits of financial statements for all entities, ranging from noncomplex entities to complex multinational entities.

The ASB believes that although size of the entity matters, the level of complexity in the nature of an entity and its financial reporting is the primary driver of scalability in the application of the proposed SAS. Many smaller entities have complexities in their business models and financial reporting processes; therefore, auditors may be required to perform more detailed risk assessments.

The ASB agreed to include in the application material considerations for audits of entities that are less complex, which are those audits that would typically require simpler risk assessment procedures. Some of these considerations are contrasted with considerations for audits of more

complex entities (for example, in relation to the understanding of an entity's risks arising from the use of IT). This approach is intended to demonstrate scalability in both directions, in relation to the nature, timing, and extent of the auditor's risk assessment procedures.

The ASB recognizes that the considerations for audits of less complex entities may be relevant to audits of large entities that have simple business models or financial reporting processes and for which the auditor's risk assessment may be simpler than it would be for a more complex entity. Therefore, paragraph 9 of the proposed SAS notes that some of the considerations for entities that are less complex may be applicable in audits of large but less complex entities.

In making the proposed revisions with regard to scalability, the ASB has removed the extant "Considerations Specific to Smaller Entities" sections throughout the proposed SAS. However, most of the matters previously included in these sections have been retained and incorporated into the text of the application material of the proposed SAS, as appropriate, together with further proposed revisions to promote scalability. In some cases, the content of the extant "Considerations Specific to Smaller Entities" sections is not unique to audits of smaller and less complex entities. The ASB has also considered the placement of guidance related to scalability, in many cases, placing guidance relating to audits of less complex entities at the start of the relevant sections, so that auditors of such entities are able to more appropriately consider the material that follows in context.

Request for Comment

1. Are the requirements and application material of the proposed SAS sufficiently scalable, that is, is the proposed SAS capable of being applied to the audits of entities with a wide range of sizes, complexities, and circumstances?

Modernizing and Updating AU-C Section 315 for an Evolving Business Environment

Significant changes in, and the evolution and increasingly complex nature of, the economic, technological, and regulatory aspects of the markets and environment in which entities and audit firms operate, and recent developments relating to internal control and other relevant frameworks, have necessitated proposed revisions to extant AU-C section 315.

Automated Tools and Techniques

Auditors increasingly use automated tools and techniques (including audit data analytics) when performing risk assessment procedures. The ASB acknowledges the importance of explicitly recognizing the usage of such tools and techniques, but also understands the need to not require the use of specific tools and techniques, and which might, in the judgment of the auditor, not be necessary or appropriate in the circumstances.

Information Technology

Because IT is a medium through which a significant amount of audit evidence is obtained, it is important for auditors to understand an entity's IT environment, with particular focus on those aspects that are relevant to financial reporting, including how the integrity of the information is

maintained. As part of the modernization of the standard, the ASB recognized that changes and enhancements were needed with regard to an entity's use of IT. Accordingly, the ASB has proposed significant clarifications and enhancements to the requirements in the proposed SAS such that the auditor is required to understand certain aspects of the entity's use of IT in its business and system of internal control. This understanding forms the basis for the auditor's identification of risks of material misstatement arising from the entity's use of IT and the identification of relevant general IT controls that the entity has put in place to address those risks of material misstatement.

Fostering Independence of Mind and Professional Skepticism

The ASB recognizes the central role that professional skepticism plays in an audit. The proposed SAS contains several key provisions that are designed to enhance the auditor's exercise of professional skepticism, including the following:

- Emphasizing the importance of exercising professional skepticism in the introductory paragraphs
- Clarifying that an appropriate understanding of the entity and its environment, and the applicable financial reporting framework, provides a foundation for being able to exercise professional skepticism throughout the rest of the audit
- Highlighting the benefits of exercising professional skepticism during the required engagement team discussion
- Highlighting that contradictory evidence may be obtained as part of the auditor's risk assessment procedures

In addition, the ASB has explained that the purpose of performing risk assessment procedures is to obtain sufficient appropriate audit evidence as the basis for the identification and assessment of the risks of material misstatement.

The Auditor's Considerations Relating to Fraud

The proposed SAS contains a number of other proposed changes intended to further the public interest, including the introduction of the inherent risk factors (described further in section IV). As part of the guidance related to inherent risk factors, which is intended to assist with the identification and assessment of the susceptibility of assertions to misstatement, a link has been made to the auditor's consideration of susceptibility of misstatement due to fraud. On balance, the ASB believes that there are sufficient references within the proposed SAS to AU-C section 240 but has highlighted in paragraph 6 of this proposed SAS the need to also apply AU-C section 240 when identifying and assessing the risks of material misstatement due to fraud.

II. Understanding the Entity and Its Environment

Focusing on the Applicable Financial Reporting Framework in Identifying Risks of Material Misstatement

The ASB has restructured the requirement that focuses on the auditor's understanding of the entity and its environment and has elevated the importance of the auditor's required understanding of the applicable financial reporting framework because it is the application of the framework in the context of the nature and circumstances of the entity that gives rise to potential risks of misstatement. This revision is intended to clarify the context of the understanding of the applicable financial reporting framework and includes enhancements requiring the auditor to focus on the reasons for changes to the entity's accounting policies. The concept of *inherent risk factors* is also discussed as the auditor contemplates potential risks arising from the application of the applicable financial reporting framework (the concept of *inherent risk factors* is further described in the section IV).

III. Understanding the Entity's System of Internal Control

In inspection findings and outreach, significant concerns have been highlighted relating to expectations regarding the requirements for the auditor to obtain an understanding of the entity's system of internal control. In particular, it was noted that the following matters were not always clear:

- Why the understanding is required to be obtained (for example, when a primarily substantive approach to the audit is planned) and how the information obtained is to be used
- What procedures are required in order to "obtain the necessary understanding" for certain components of internal control
- Whether all components of internal control as set out in the standard need to be understood
- When controls are considered "relevant to the audit"

In addition, it was noted that it can be confusing when inconsistent terminology is used when describing concepts such as "internal control" and "controls."

The ASB believes that understanding certain aspects of the entity's system of internal control is integral to the auditor's identification and assessment of the risks of material misstatement, regardless of the auditor's planned controls reliance strategy. Understanding how management has set up its system of internal control helps the auditor to form a view about where the auditor's attention should be placed, including where risks of material misstatement may occur in the financial statements and what constitutes a significant class of transactions, account balances, or disclosure in the specific audit. In addition, the understanding informs the auditor's expectations about the operating effectiveness of controls and, therefore, is the foundation for the auditor's assessment of control risk. It is important to be clear about the work effort necessary in obtaining the required understanding, and the ASB has proposed revisions, as explained subsequently, in this regard.

The proposed SAS also makes it clear that the overall requirement for understanding the entity's system of internal control is achieved through the requirements that address understanding each of the components of the system of internal control. The order in which the components are presented

has also been changed as a result of the following clarification related to the nature of each component, such that the three components that consist primarily of "indirect controls" are presented separately from the two components that consist of primarily "direct controls" ("indirect" and "direct" controls are also described in the following text).

Terms Used to Describe Aspects of the Entity's System of Internal Control

The ASB has considered the various terms used to describe an entity's system of internal control or aspects thereof and has made amendments to the descriptions of terms used, as well as revisions throughout the proposed SAS to apply the revised terms consistently. These changes, made throughout the proposed standard, include the following:

- The term *internal control*, as it is used in extant AU-C section 315, has been changed to *system of internal control*, and the definition has been updated to reflect that it comprises five interrelated components.

- The use of the term *controls* has been clarified by including the following definition in the standard:

  > "Controls are…[p]olicies or procedures that are embedded within the components of the system of internal control to achieve the control objectives of management or those charged with governance. Within this context, policies are statements of what should, or should not, be done within the entity to effect internal control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Procedures are actions to implement policies."

The ASB also agreed that "policies and procedures" should be considered in a broad context and may include aspects of governance (for example, tone at the top) and other aspects of the entity's systems (such as the risk assessment process in some entities) that are established but are not formally documented. Accordingly, proposed revisions have been made to the application material to recognize that some aspects of the entity's system of internal control may be less formalized but still functioning. The ASB believes that this acknowledges that controls may also be less formalized, thereby contributing to the scalability of the required understanding, and the way it is interpreted within each of the components.

- Components of internal control for purposes of generally accepted auditing standards (GAAS) include the control environment, the entity's risk assessment process, the entity's process to monitor the system of internal control, the information system (including related business processes) and communication, and control activities. Within each of these components, individual controls are embedded (that is, each component comprises a collection of controls). The proposed revisions to the requirements for each component have specified the matters for which an understanding is required.

- *Control activities* refers to the component of the entity's system of internal control that typically includes controls over the flows of information within the information system. The required understanding for this component is obtained through the auditor's identification and understanding of certain controls that address risks of material

misstatement (see the discussion that follows about controls that address the risks of material misstatement).

Understanding Internal Control Through Understanding the Five Components of Internal Control

The ASB continues to believe that the five components of internal control as described previously, comprising the entity's system of internal control, remain an appropriate structure to describe the auditor's understanding of the system of internal control required to be obtained for purposes of GAAS. In its deliberations, the ASB agreed that the auditor needs to obtain an understanding of certain aspects of all the components, specifically whether and how they have been addressed by the entity, and revised the requirements for each of the components to be clearer about the specific matters relating to that component that need to be understood. The proposed SAS makes it clear that the auditor obtains an understanding of each of the components of internal control by performing risk assessment procedures, and that inquiry alone is not sufficient for this purpose.

In its deliberations about obtaining an understanding about the components of the system of internal control, the ASB agreed that differentiating the nature of each of the components would help the auditor recognize how the understanding provides the basis for the auditor's identification and assessment of the risks of material misstatement. In the ASB's view, controls can be distinguished between indirect and direct controls as follows:

- "Control environment," "entity's risk assessment process," and "entity's process to monitor the system of internal control" components have controls that are typically more "indirect" in nature (that is, they are controls that generally do not directly address the risks of material misstatement at the assertion level). Such indirect controls are more likely to be relevant to the auditor's identification and assessment of risks of material misstatement at the financial statement level. For example, if the entity's control environment is not functioning as expected given the size and complexity of the entity, this could affect the opportunity for fraud to be committed, which may be identified as a financial statement level risk (that is, a risk that has a pervasive effect on the financial statements).

- "Information system and communication" and "control activities" components comprise controls that are more likely to directly address the risks of material misstatement at the assertion level (direct controls). The design of the information system is established in the policies and procedures that define the nature, timing, and extent of the entity's financial reporting processes and how the entity's personnel, IT, and other resources are deployed in applying them. Such controls are referred to as *information system controls relevant to financial reporting*. The auditor is required to evaluate the design of certain information system controls relevant to financial reporting (as listed in the standard) and determine whether they have been implemented. This evaluation will assist the auditor in identifying risks of material misstatement at the assertion level. Controls in the control activities component are controls over the flows of information and the financial reporting processes within the entity's information system. (See the section, "Controls That Address the Risks of Material Misstatement.")

Work Effort for Understanding Each of the Components of Internal Control

Clarifying the requirements related to the understanding of each component of the system of internal control is an important aspect of the proposed enhancements to the standard. Within each component, the ASB has set out the matters that need to be understood and provided further guidance about the extent and scalability of procedures necessary to obtain that understanding. The nature, timing, and extent of risk assessment procedures that the auditor performs to obtain the required understanding are matters of the auditor's professional judgment and are based on the auditor's determination regarding the procedures that will provide sufficient appropriate audit evidence to serve as a basis for the identification and assessment of the risks of material misstatement.

Controls That Address the Risks of Material Misstatement

To assist the auditor with identifying controls that address the risks of material misstatement, the related requirement (paragraph 26 of this proposed SAS) has been clarified to create a list of the types of control activities that, if applicable, the ASB believes are always relevant to the risks of material misstatement. Recognizing that entities have a wide variety of circumstances, in addition to the specifically enumerated types of controls in this component, auditors are required to use professional judgment to determine if there are any other controls for which evaluation of their design and determination of whether they have been implemented are necessary to enable the auditor to identify and assess risks of material misstatement. It has also been clarified that controls that address the risks of material misstatement at the assertion level are primarily direct controls, residing in the control activities component. However, the auditor may identify certain controls that address the risks of material misstatement at the assertion level in other components of the system of internal control.

The "Control Activities" section of this proposed SAS also includes enhanced requirements to identify general IT controls relevant to the audit. These enhanced requirements are discussed in the next section.

The auditor is required to evaluate the design of certain control activities, as described in paragraph 26 of this proposed SAS, that address the risks of material misstatement, including general IT controls, and determine whether they have been implemented (this is referred to as "D&I"). The related requirement and application material have been clarified and enhanced. In particular, new guidance has been included about the benefits of the auditor's D&I procedures for the design and performance of further audit procedures. Although the requirements in paragraph 26 are located in the "Control Activities" section of the proposed SAS, application material in paragraph A165 reminds the auditor that the controls described in paragraph 26 may reside in other components of internal control.

Application material provides further details related to understanding and evaluating information system controls relevant to financial reporting and control activities that address the risks of material misstatement.

Request for Comment

2. Do the proposals made relating to the auditor's understanding of the entity's system of internal control assist with understanding the nature and extent of the work effort required

and the relationship of the work effort to the identification and assessment of the risks of material misstatement? Specifically:

a. Have the requirements related to the auditor's understanding of each component of the entity's system of internal control been appropriately enhanced and clarified? Is it clear why the understanding is obtained and how this informs the risk identification and assessment process?

b. Have the requirements related to the auditor's identification of controls that address the risks of material misstatement been appropriately enhanced and clarified? Is it clear how controls that addressed the risks of material misstatement are identified, particularly for audits of smaller and less complex entities?

c. Given that COSO's 2013 *Internal Control—Integrated Framework* (COSO framework) is often used by entities subject to the AICPA's generally accepted auditing standards, is the terminology in paragraphs 21–27 and related application material of the proposed SAS clear and capable of consistent interpretation for audits of entities that use the COSO framework?

Enhanced Guidance Related to IT

Because IT is the medium through which a significant amount of audit evidence is obtained, it is important for auditors to understand certain aspects of an entity's IT system, including how the integrity of information relevant to the preparation of the financial statements is maintained.

The most significant proposed enhancements to the proposed SAS addressing the entity's use of IT are in the requirements for the information system and communication component and for the identification of certain controls that address the risks of material misstatement. In understanding the information system relevant to financial reporting, the auditor is required to understand the related IT environment in order to gain a high-level understanding of the nature and complexity of the environment and its supporting processes. Using the auditor's understanding of the information system and communication relevant to preparation of the financial statements, as well as the identification of certain controls that address the risks of material misstatement (see previous section), the auditor determines which IT applications and other aspects of the IT environment are subject to risks arising from the use of IT, as defined in the proposed SAS. This process helps the auditor identify IT applications for which risks arising from the entity's use of IT may exist, and that may affect the design, implementation, or operating effectiveness of automated controls, or other controls over the integrity of information.

For IT applications and other aspects of the IT environment determined to be subject to risks arising from the entity's use of IT, the auditor identifies the risks arising from the entity's use of IT and identifies general IT controls that address those risks. The application material to these requirements has been enhanced to explain some possible risks and controls that the auditor may consider, and to explain that the extent to which general IT controls address the risks of material misstatement will vary, based on the circumstances of the engagement and planned audit approach or strategy. A new appendix E, "Considerations for Understanding Information Technology," has

also been added to the proposed SAS to provide further considerations related to general IT controls.

The ASB believes that this approach will assist the auditor's decision making in determining the extent of general IT controls that address the risks of material misstatement. In particular, the ASB is of the view that it is not necessary for the auditor to identify risks arising from the entity's use of IT or general IT controls, unless they relate to IT applications that are determined to be relevant for the auditor's purposes.

When an entity's IT environment consists only of commercial software for which the entity does not have access to the underlying source code such that no program changes can be made (which may be the case for many less complex entities), the auditor's procedures with respect to the entity's IT applications maybe more limited. In contrast, for more complex entities or for audits in which the auditor plans to test the operating effectiveness of automated controls, the auditor may determine that a greater level of effort related to IT applications is necessary. This may drive a greater amount of general IT controls being identified as controls that address the risks of material misstatement.

Request for Comment

3. Are the enhanced requirements and application material related to the auditor's understanding of the IT environment, the identification of the risks arising from the entity's use of IT, and the identification of general IT controls clear to support the auditor's consideration of the effects of the entity's use of IT on the identification and assessment of the risks of material misstatement?

Other Matters Relevant to Understanding the Entity's System of Internal Control

Deficiencies in internal control (including material weaknesses and significant deficiencies) are described and addressed in AU-C section 265, *Communicating Internal Control Related Matters Identified in an Audit*. Extant AU-C section 315 contains an explicit requirement that the auditor consider whether deficiencies in internal control were identified only in the context of the auditor's understanding of the entity's risk assessment process. The ASB has recognized that a deficiency in internal control may arise within any of the components of the entity's system of internal control and that these deficiencies may be identified when the auditor is obtaining an understanding of the system of internal control. Because identified deficiencies in any components may have implications for the audit, including informing the auditor's identification of risks of material misstatement, as well as reporting requirements in terms of AU-C section 265, the ASB has added a link to AU-C section 265 for the auditor to determine, on the basis of the work performed under this proposed SAS (that is, for all the components of the system of internal control), whether control deficiencies have been identified and to evaluate the implications on the audit when such deficiencies have been identified (see paragraph 27 of the proposed SAS).

IV. Identifying and Assessing the Risks of Material Misstatement

Identifying and Assessing the Risks of Material Misstatement

The ASB has noted continuing concerns related to the implementation of the requirements for the identification and assessment of risks of material misstatement. In addition, the ASB has noted that inspection findings commonly refer to an apparent lack of consistency in the determination of significant risks.

To assist auditors in understanding the requirements related to the identification and assessment of risks of material misstatement, the ASB believes a clearer description of the required risk identification and assessment process will help drive a more consistent and focused approach and, thus, improve audit quality through its impact on the design and performance of further audit procedures. To facilitate this, the ASB has introduced the following new concepts and definitions and significantly enhanced the related requirements:

- *Inherent risk factors* (new definition). Characteristics that affect susceptibility to misstatement of an assertion about a class of transactions, account balance, or disclosure, and that may be quantitative or qualitative in nature. Such factors include complexity, subjectivity, change, uncertainty, and susceptibility to misstatement due to management bias or fraud. Inherent risk factors are intended to assist the auditor in focusing on those aspects of events or conditions that affect an assertion's susceptibility to misstatement, which in turn, facilitates a more focused identification of risks of material misstatement. Taking into account the degree to which the inherent risk factors affect susceptibility to misstatement assists in the assessment of inherent risk (see the explanation of "spectrum of inherent risk" that follows).

- *Relevant assertions.* The definition has been revised to focus auditors on those assertions relevant to a class of transactions, account balance, or disclosure when the nature or circumstances are such that there is a reasonable possibility of occurrence of misstatement, with respect to an assertion, that is material, either individually or in combination with other misstatements. Application material to the definition explains that a relevant assertion is one for which one or more risks of material misstatement exist. The revised guidance on *relevant assertions* is expected to enhance the likelihood the auditor will identify risks of material misstatement by requiring the auditor to identify those assertions in which risks of material misstatement exist (that is, are reasonably possible) and, therefore, need to be assessed so further audit procedures may be designed and performed.

- *Significant class of transactions, account balance, or disclosure* (new definition). A class of transactions, account balance, or disclosure for which there is one or more relevant assertions. The introduction of the concept of a significant class of transactions, account balance, or disclosure is viewed by the ASB to have the benefit of clarifying the scope of the auditor's understanding of the information system, and for the auditor's identification and assessment of, and responses to, assessed risks of material misstatement, including the related requirements in the recently revised AU-C section 540 that address these topics in the context of auditing accounting estimates.

- *Spectrum of inherent risk*. A concept included in the introductory paragraphs (see paragraph 5 of the proposed SAS) and application material recognizing that inherent risk factors individually or in combination affect inherent risk to varying degrees and that inherent risk will be higher for some assertions than for others. The degree to which

inherent risk varies is referred to as the *spectrum of inherent risk*. The relative degrees of the likelihood and magnitude of a possible misstatement determine where on the spectrum of inherent risk the risk of misstatement is assessed. The ASB is of the view that the introduction of the spectrum of inherent risk will facilitate greater consistency in the auditor's identification and assessment of risks of material misstatement by providing a frame of reference for the auditor's consideration of the likelihood and magnitude of possible misstatements and the influence of the inherent risk factors.

Request for Comment

4. Do you support the introduction in the proposed SAS of the new concepts and related definitions of significant classes of transactions, account balances, and disclosures, and their relevant assertions? Is there sufficient guidance to explain how they are determined (that is, that an assertion is relevant when there is a reasonable possibility of occurrence of a misstatement that is material with respect to that assertion), and how they assist the auditor in identifying where risks of material misstatement exist?

5. Do you support the introduction of the spectrum of inherent risk into the proposed SAS?

Questions have arisen in both the AU-C section 540 and AU-C section 315 projects about the "combined" assessment of inherent risk and control risk as permitted by extant AU-C section 200. Noting the requirements in paragraph 7 of AU-C section 330 that require the auditor to consider inherent risk and control risk separately in order to respond appropriately to assessed risks of material misstatement, the ASB agreed that a separate assessment of inherent risk and control risk should be required, and that this requirement would initially appear in SAS No. 143, *Auditing Accounting Estimates and Related Disclosures*.[2] The proposed SAS extends the requirement for the separate assessments of inherent and control risk in relation to all risks of material misstatement at the assertion level. New requirements have been included in the proposed SAS that address these separate assessments of inherent risk and control risk (see paragraphs 31 and 34 of the proposed SAS).

The ASB acknowledges that the order in which the requirements related to the identification of the risks of material misstatement are to be applied should not be prescribed. For example, firms may have different approaches in their methodologies regarding the order in which the risks of material misstatement, and the significant classes of transactions, account balances, and disclosures and the relevant assertions to which they relate, are identified. The process is iterative and is likely to be applied differently in an initial audit engagement versus a recurring engagement. Regardless of an auditor's methodology, the auditor should comply with each of the relevant requirements, and the auditor's understanding of the system of internal control should be appropriate to enable the auditor to identify and assess risks of material misstatement sufficient to form a basis for the design and performance of further audit procedures. For example, the auditor is required to identify controls that address the risks of material misstatement based on the determination of significant risks and risks for which substantive procedures alone cannot provide

[2] Statement on Auditing Standards (SAS) No. 143, *Auditing Accounting Estimates and Related Disclosures*, was approved by the Auditing Standards Board in May 2020 and, when issued, will have an effective date of audits of financial statement for periods ending or after December 15, 2023.

sufficient appropriate audit evidence. As another example, the auditor forms an initial expectation of the significant classes of transactions, account balances, and disclosures when understanding the entity and its environment and the applicable financial reporting framework. The auditor uses this expectation in understanding the information system and communication component, which may affect the auditor's ultimate determination of the significant classes of transactions, account balances, and disclosures when identifying the risks of material misstatement.

The ASB has clarified the work performed on the D&I of certain controls that address the risks of material misstatement by enhancing the application material to further explain how the D&I work interacts with the auditor's identification of risks and assessment of control risk. The ASB has made it clear that if the auditor does not contemplate testing the operating effectiveness of controls, or is not required to test controls, control risk is assessed at maximum (that is, the assessment of the risk of material misstatement is the same as the assessment of inherent risk). This means that control risk cannot be reduced based on the effective operation of controls unless the auditor intends to test them. Although auditors who intend to perform a primarily substantive audit and, thus, will not need to test the operating effectiveness of controls, work on the D&I of controls may affect the identification and assessment of risks of material misstatement and the nature and extent of substantive procedures to be performed.

In making these revisions, the ASB has focused on how clearer requirements will help auditors make more consistent and effective assessments of identified risks of material misstatement, thereby providing an enhanced basis for the design and performance of further audit procedures, as well as overall responses to risks of material misstatement at the financial statement level (as required by AU-C section 330).

Request for Comment

6. Do you support the separate assessments of inherent and control risk in relation to all risks of material misstatement at the assertion level?

7. What are your views regarding the clarity of the requirement to assess the control risk, in particular, when the auditor does not plan to test the operating effectiveness of controls?

8. What are your views regarding the clarity of the requirement in paragraph 26*d* of the proposed SAS to evaluate design and determine implementation of certain control activities (including, specifically, the requirement related to controls over journal entries)?

Relationship of Concepts With AU-C Section 540

The ASB has endeavored to closely coordinate the work between the AU-C section 315 and AU-C section 540 task forces in the development of proposed revisions to both standards. Some of the new concepts in the proposed SAS have already been approved in SAS No. 143, which supersedes AU-C section 540, including inherent risk factors, the spectrum of inherent risk, and the separate assessments of inherent risk and control risk. The ASB believes these concepts are appropriate for this proposed SAS because they are applicable to all types of classes of transactions, account balances, and disclosures, not just those involving accounting estimates. The ASB has also worked toward addressing the use of these concepts consistently between the standards, recognizing that

references to these concepts in SAS No. 143 specifically relate to accounting estimates. Because of the close interaction between the proposed SAS and SAS No. 143, the ASB is proposing to align the effective dates of the standards. Both standards would be effective for audits of financial statements for periods ending on or after December 15, 2023.

Significant Risks

A key inspection finding related to a lack of consistency with which significant risks are determined. The ASB believes that one of the main reasons for this inconsistency lies in the definition of *significant risk*. The current definition focuses the auditor on the response to the risk, rather than the nature of the risk. In extant AU-C section 315, significant risks are those that require "special audit consideration."

In its deliberations, the ASB specifically considered the introduction of the spectrum of inherent risk and whether the spectrum alone might provide a framework sufficiently robust to properly assess all risks or whether the auditor should still be required to separately determine significant risks. On balance, the ASB believed that it was important to retain the concept of, and requirement to determine, significant risks because of the focused work effort in other AU-C sections on these types of risks.

To promote a more consistent approach to determining significant risks, the ASB revised the definition to focus not on the response but on those risks for which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk. This revision to the definition also incorporates the extant requirement for significant risks to be determined, excluding the effects of identified controls related to the risks (that is, based on inherent risk alone).

In revising the definition of *significant risk*, the ASB also deliberated whether these risks are represented on the spectrum of inherent risk by a higher likelihood of occurrence *and* a higher magnitude of potential misstatement should the risk occur, or whether a significant risk could also be present when there is a higher magnitude of potential misstatement but a lower likelihood of the risk occurring. On balance, the ASB agreed that there could be risks potentially lower in likelihood but for which the magnitude could be very high if it occurred, and that it was probably not appropriate to explicitly exclude these risks from the auditor's determination of significant risks. The proposed SAS, therefore, acknowledges that the determination of whether a risk is a significant risk requires the application of professional judgment.

Request for Comment

9. Do you support the revised definition, and related material, on the determination of significant risks? What are your views on the matters previously presented relating to how significant risks are determined based on the spectrum of inherent risk?

Identified and Assessed Risks of Material Misstatement at the Financial Statement Level

Extant AU-C section 315 requires identification and assessment of the risks of material misstatement at the financial statement level but does not prescribe how to do this or specify how this interacts with the identification and assessment of the risks of material misstatement at the

assertion level. The ASB considered the nature of risks of material misstatement at the financial statement level, reflecting on how they are described in AU-C section 200, in order to better describe and address them in the proposed SAS.

Under AU-C section 200, every identified risk of material misstatement relates either specifically to an individual assertion or to a number of assertions, which could be in one or more classes of transactions, account balances, or disclosures. However, when the risk relates to a number of assertions in multiple classes of transactions, account balances, or disclosures (that is, is more pervasive), the risk is considered to exist at the financial statement level. The assessment of risks of material misstatement at the financial statement level involves determining the effect of such risks on the assessment of risks of material misstatement at the assertion level. However, because of the pervasive nature of the risks at the financial statement level, it may be difficult to identify specific assertions that are affected (for example, fraud risks, such as risk of management override of controls). For that reason, assessment of risks at the financial statement level also involves evaluating the nature and extent of their pervasive effect on the financial statements to provide the basis for designing and implementing overall responses to the risks. Proposed revisions have been made to the requirements and application material to better reflect the relationship of these risks to the risks of material misstatement at the assertion level.

The ASB is also of the view that risks at the financial statement level will often arise from deficiencies in the components of the entity's system of internal control that consist primarily of "indirect controls," in particular, the control environment, which will likely have a more pervasive effect on a number of, or all, classes of transactions, account balances, and disclosures, in the financial statements. Accordingly, the application material has been enhanced to link the auditor's understanding of the components of the system of internal control, including the required evaluations thereof and the effect of any identified deficiencies, to the auditor's identification and assessment of the risks of material misstatement at the financial statement level.

Stand-Back and Paragraph .18 of AU-C section 330

In considering the risk identification and assessment process, the ASB has also proposed a new "stand-back" requirement (paragraph 36), which is intended to drive an evaluation of the completeness of the identification of significant classes of transactions, account balances, and disclosures by the auditor. In turn, this helps drive the completeness of the identification of the risks of material misstatement (refer to the previous section on "Identifying and Assessing the Risks of Material Misstatement" for further explanation of the process that the auditor may follow to determine the significant classes of transactions, account balances, and disclosures).

The stand-back is intended to focus on material classes of transactions, account balances, or disclosures that have not been determined to be significant (that is, the auditor has not identified any risks of material misstatement that are reasonably possible and, therefore, has not identified any relevant assertions).

Paragraph .18 of extant AU-C section 330 is also targeted at "material" classes of transactions, account balances, and disclosures and requires substantive procedures with respect to relevant assertions for all such classes of transactions, account balances, and disclosures. In developing the scope of work for the project to revise AU-C section 315, paragraph .18 of AU-C section 330 was

included because of inconsistent interpretations in practice about how the requirement should be applied. The ASB agreed to further consider the interaction of paragraph .18 of AU-C section 330 with the revisions proposed to extant AU-C section 315, including whether this paragraph is still needed.

The ASB decided to retain paragraph .18 of AU-C section 330. It should be noted that a difference exists between paragraph 18 of ISA 330 and paragraph .18 of extant AU-C section 330 because at the time AU-C section 315 was originally developed, the ASB decided to align paragraph .18 of the original standard with the PCAOB, thus, creating a difference between paragraph 18 of ISA 330 and paragraph 18 of extant AU-C section 330. In deliberating the development of the proposed SAS, the ASB agreed that paragraph .18 of AU-C section 330 should be amended to require the auditor to design and perform substantive procedures for all relevant assertions related to each *significant* (instead of material) class of transactions, account balance, and disclosure. The intent of this conforming amendment is to more fully align the wording of paragraph .18 of AU-C section 330 with the wording in PCAOB standard AS 2301, *The Auditor's Responses to the Risks of Material Misstatement.* This change is reflected in appendix G, "Considerations Regarding the Use of External Information Sources," to the proposed SAS.

Request for Comment

10. What are your views about the proposed stand-back requirement in paragraph 36 of the proposed SAS and the conforming amendments proposed to paragraph .18 of AU-C section 330?

V. *Audit Documentation*

Paragraph 38 of the proposed SAS includes the key matters that, in applying the requirements of the proposed SAS and the related application material, should be included in the audit documentation. This requirement includes the rationale for the significant judgments made in identifying and assessing the risks of material misstatement (see paragraph 38*d*). As explained in preceding section IV, the proposed SAS would require that the auditor assess inherent risk and control risk separately. Paragraphs A262–A263 of the proposed SAS give examples of situations to which these requirements apply, including key judgments reached in arriving at the required assessments of inherent and control risk.

Request for Comment

11. What are your views with respect to the clarity and appropriateness of the documentation requirements?

Guide for Respondents

Comments are most helpful when they refer to specific paragraphs, include the reasons for the comments and, when appropriate, make specific suggestions for any proposed changes to wording. When a respondent agrees with proposals in the exposure draft, it will be helpful for the ASB to be made aware of this view, as well.

Written comments on this exposure draft will become part of the public record of the AICPA and will be available for public inspection at the offices of the AICPA after November 25, 2020, for one year. Responses should be sent to CommentLetters@aicpa-cima.com and received no later than November 25, 2020.

Comment Period

The comment period for this exposure draft ends on November 25, 2020.

Auditing Standards Board
(2020–2021)

Tracy W. Harding, *Chair*
Brad C. Ames
Monique Booker
Patricia Bottomly
Joseph S. Cascio
Sherry Chesser
Harry Cohen
Jeanne Dee
Horace Emery
Audrey A. Gramling
Robert Harris
Kathleen K. Healy
Jon Heath
Clay Huffman
Kristen A. Kociolek
Sara Lord
Maria C. Manasses
Chris Rogers
Tania Desilva Sergott

Risk Assessment Task Force

Tracy W. Harding, *Chair*
Diane Hardesty
Kathleen K. Healy
Susan Jones
April King
Maria C. Manasses
Tania Desilva Sergott
Dan Wernke

AICPA Staff

Robert Dohrer
Chief Auditor
Professional Standards and Services

Hiram Hasty
Associate Director
Audit and Attest Standards — Public Accounting

Teighlor S. March
Assistant General Counsel — Office of General Counsel

PROPOSED STATEMENT ON AUDITING STANDARDS
Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement

TABLE OF CONTENTS

Proposed Statement on Auditing Standards, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*

Introduction

Scope of This Proposed SAS

1. This proposed Statement on Auditing Standards (SAS) addresses the auditor's responsibility to identify and assess the risks of material misstatement in the financial statements.

Key Concepts in This Proposed SAS

2. AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards*, addresses the overall objectives of the auditor in conducting an audit of the financial statements, including to obtain sufficient appropriate audit evidence to reduce audit risk to an acceptably low level.[1] Audit risk is a function of the risks of material misstatement and detection risk.[2] AU-C section 200 explains that the risks of material misstatement may exist at two levels:[3] the overall financial statement level and the assertion level for classes of transactions, account balances, and disclosures.

3. AU-C section 200 requires the auditor to exercise professional judgment in planning and performing an audit and to plan and perform an audit with professional skepticism, recognizing that circumstances may exist that cause the financial statements to be materially misstated.[4]

4. Risks at the financial statement level relate pervasively to the financial statements as a whole and potentially affect many assertions. Risks of material misstatement at the assertion level consist of two components: inherent risk and control risk:

- *Inherent risk* is described as the susceptibility of an assertion about a class of transaction, account balance, or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls.
- *Control risk* is described as the risk that a misstatement that could occur in an assertion about a class of transaction, account balance, or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be

---

1 Paragraph .19 of AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards*.

2 Paragraph .14 of AU-C section 200.

3 Paragraph .A38 of AU-C section 200.

4 Paragraphs .17–.18 of AU-C section 200.

prevented, or detected and corrected, on a timely basis by the entity's system of internal control.

5. AU-C section 200 explains that risks of material misstatement are assessed at the assertion level in order to determine the nature, timing, and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence. For purposes of generally accepted auditing standards (GAAS), a risk of material misstatement exists when (*a*) there is a reasonable possibility of a misstatement occurring (that is, its likelihood), and (*b*) if it were to occur, there is a reasonable possibility of the misstatement being material (that is, its magnitude).[5] For the identified risks of material misstatement at the assertion level, a separate assessment of inherent risk and control risk is required by this proposed SAS. As explained in AU-C section 200, inherent risk is higher for some assertions and related classes of transactions, account balances, and disclosures than for others. The degree to which inherent risk varies is referred to in this proposed SAS as the *spectrum of inherent risk*.

6. Risks of material misstatement identified and assessed by the auditor include both those due to error and those due to fraud. Although both are addressed by this proposed SAS, the significance of fraud is such that further requirements and guidance are included in AU-C section 240, *Consideration of Fraud in a Financial Statement Audit*, in relation to risk assessment procedures and related activities to obtain information that is used to identify, assess, and respond to the risks of material misstatement due to fraud.

7. The auditor's risk identification and assessment process is iterative and dynamic. The auditor's understanding of the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control are interdependent with concepts within the requirements to identify and assess the risks of material misstatement. In obtaining the understanding required by this proposed SAS, initial expectations of risks may be developed, which may be further refined as the auditor progresses through the risk identification and assessment process. In addition, this proposed SAS and AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*, require the auditor to revise the risk assessments and modify further overall responses and further audit procedures, based on audit evidence obtained from performing further audit procedures in accordance with AU-C section 330, or if new information is obtained.

8. AU-C section 330 requires the auditor to design and implement overall responses to address the assessed risks of material misstatement at the financial statement level.[6] AU-C section 330 further explains that the auditor's assessment of the risks of material misstatement at the financial statement level, and the auditor's overall responses, is affected by the auditor's understanding of the control environment. AU-C section 330 also requires the auditor to design and perform further audit procedures whose nature, timing, and extent are based on and are responsive to the assessed risks of material misstatement at the assertion level.[7]

---

5 Paragraph .A43*a* of AU-C section 200 and paragraph .06 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*.

6 Paragraph .05 of AU-C section 330.

7 Paragraph .06 of AU-C section 330.

Scalability

9. AU-C section 200 states that some AU-C sections include scalability considerations, which illustrate the application of the requirements to all entities regardless of whether their nature and circumstances are less complex or more complex.[8] This proposed SAS is intended for audits of all entities, regardless of size or complexity; therefore, the application material incorporates considerations specific to both less and more complex entities, where appropriate. Although the size of an entity may be an indicator of its complexity, some smaller entities may be complex, and some larger entities may be less complex.

Effective Date

10. This proposed SAS is effective for audits of financial statements for periods ending on or after December 15, 2023.

Objective

11. The objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement.

Definitions

12. For purposes of GAAS, the following terms have the meanings attributed:

> **Assertions.** Representations, explicit or otherwise, with respect to the recognition, measurement, presentation, and disclosure of information in the financial statements, which are inherent in management, representing that the financial statements are prepared in accordance with the applicable financial reporting framework. Assertions are used by the auditor to consider the different types of potential misstatements that may occur when identifying, assessing, and responding to the risks of material misstatement. (Ref: par. A1)
>
> **Business risk.** A risk resulting from significant conditions, events, circumstances, actions, or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.
>
> **Controls.** Policies or procedures that an entity establishes to achieve the control objectives of management or those charged with governance. In this context (Ref: par. A2–A5)
>
> i. policies are statements of what should, or should not, be done within the entity to effect control. Such statements may be documented, explicitly stated in

[8] Paragraph .A65*a* of AU-C section 200.

communications, or implied through actions and decisions.

ii. procedures are actions to implement policies.

General information technology (IT) controls. Controls over the entity's IT processes that support the continued proper operation of the IT environment, including the continued effective functioning of information-processing controls and the integrity of information in the entity's information system. Also see **IT environment**. (Ref: par. A6)

Information-processing controls. Controls relating to the processing of information in IT applications or manual information processes in the entity's information that directly address risks to the integrity of information. (Ref: par. A6–A7)

Inherent risk factors. Characteristics of events or conditions that affect susceptibility to misstatement, whether due to fraud or error, of an assertion about a class of transactions, account balance, or disclosure, before consideration of controls. Such factors may be qualitative or quantitative and include complexity, subjectivity, change, uncertainty, or susceptibility to misstatement due to management bias or other fraud risk factors[9] insofar as they affect inherent risk. (Ref: par. A8–A10)

IT environment. The IT applications and supporting IT infrastructure, as well as the IT processes and personnel involved in those processes, that an entity uses to support business operations and achieve business strategies. For the purposes of this definition

i. an *IT application* is a program or a set of programs that is used in the initiation, processing, recording, and reporting of transactions or information. IT applications include data warehouses and report writers.

ii. the IT infrastructure comprises the network, operating systems, and databases and their related hardware and software.

iii. the IT processes are the entity's processes to manage access to the IT environment, manage program changes or changes to the IT environment, and manage IT operations.

Relevant assertions. An assertion about a class of transactions, account balance, or disclosure is relevant when it has an identified risk of material misstatement. The determination of whether an assertion is a relevant assertion is made before consideration of any related controls (that is, the inherent risk). (Ref: par. A11)

Risks arising from the use of IT. Susceptibility of information-processing controls to ineffective design or operation, or risks to the integrity of information in the entity's

---

[9] Paragraphs .A28–.A32 of AU-C section 240, *Consideration of Fraud in a Financial Statement Audit*.

information system, due to ineffective design or operation of controls in the entity's IT processes. See **IT environment**. (Ref: par. A6 and A12)

Risk assessment procedures. The audit procedures designed and performed to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels.

Significant class of transactions, account balance, or disclosure. A class of transactions, account balance, or disclosure for which there is one or more relevant assertions.

Significant risk. An identified risk of material misstatement (Ref: par. A13)

i. for which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk due to the degree to which inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur, or

ii. that is to be treated as a significant risk in accordance with the requirements of other AU-C sections.[10]

System of internal control. The system designed, implemented, and maintained by those charged with governance, management, and other personnel, to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. For purposes of GAAS, the system of internal control consists of five interrelated components:

i. Control environment

ii. The entity's risk assessment process

iii. The entity's process to monitor the system of internal control

iv. The information system and communication

v. Control activities

(Ref: par. A14)

Requirements

Risk Assessment Procedures and Related Activities

13. The auditor should design and perform risk assessment procedures to obtain audit evidence that provides an appropriate basis for (Ref: par. A15–A22)

[10] Paragraph .25 of AU-C section 240 and paragraph .18 of AU-C section 550, *Related Parties*.

a. the identification and assessment of risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels, and

b. the design of further audit procedures in accordance with AU-C section 330.

The auditor should design and perform risk assessment procedures in a manner that is not biased towards obtaining audit evidence that may be corroborative or towards excluding audit evidence that may be contradictory.

14. The risk assessment procedures should include the following: (Ref: par. A23–A25)

a. Inquiries of management and of other appropriate individuals within the entity, including individuals within the internal audit function (if the function exists) (Ref: par. A26–A30)

b. Analytical procedures (Ref: par. A31–A35)

c. Observation and inspection (Ref: par. A36–A40)

Information From Other Sources

15. In obtaining audit evidence in accordance with paragraph 13, the auditor should consider information from (Ref: par. A41–A42)

a. the auditor's procedures regarding acceptance or continuance of the client relationship or the audit engagement, and

b. when applicable, other engagements performed by the engagement partner for the entity.

16. When the auditor intends to use information obtained from the auditor's previous experience with the entity and from audit procedures performed in previous audits, the auditor should evaluate whether such information remains relevant and reliable as audit evidence for the current audit. (Ref: par. A43–A45)

Engagement Team Discussion

17. The engagement partner and other key engagement team members should discuss the application of the applicable financial reporting framework and the susceptibility of the entity's financial statements to material misstatement. (Ref: par. A46–A52)

18. When there are engagement team members not involved in the engagement team discussion, the engagement partner should determine which matters are to be communicated to those members.

Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework, and the Entity's System of Internal Control (Ref: par. A53–A55)

Understanding the Entity and Its Environment, and the Applicable Financial Reporting Framework (Ref: par. A56–A61)

19. The auditor should perform risk assessment procedures to obtain an understanding of

a. the following aspects of the entity and its environment:

i. The entity's organizational structure, ownership and governance, and its business model, including the extent to which the business model integrates the use of IT (Ref: par. A62–A74)

ii. Industry, regulatory, and other external factors (Ref: par. A75–A80)

iii. The measures used, internally and externally, to assess the entity's financial performance (Ref: par. A81–A88)

b. the applicable financial reporting framework and the entity's accounting policies and the reasons for any changes thereto. (Ref: par. A89–A91)

c. how inherent risk factors affect susceptibility of assertions to misstatement and the degree to which they do so, in the preparation of the financial statements in accordance with the applicable financial reporting framework, based on the understanding obtained in subparagraphs *a* and *b*. (Ref: par. A92–A97)

20. The auditor should evaluate whether the entity's accounting policies are appropriate and consistent with the applicable financial reporting framework.

Understanding the Components of the Entity's System of Internal Control (Ref: par. A98–A107)

Control Environment, the Entity's Risk Assessment Process, and the Entity's Process to Monitor the System of Internal Control (Ref: par. A108–A110)

Control Environment

21. The auditor should, through performing risk assessment procedures, obtain an understanding of the control environment relevant to the preparation of the financial statements by (Ref: par. A111–A112)

a. understanding the set of controls, processes, and structures that address (Ref: par. A113)

i. how management's oversight responsibilities are carried out, such as the entity's culture and management's commitment to integrity and ethical values;

ii. when those charged with governance are separate from management, the independence of, and oversight over the entity's system of internal control by, those charged with governance;

iii. the entity's assignment of authority and responsibility;

iv. how the entity attracts, develops, and retains competent individuals;

v. how the entity holds individuals accountable for their responsibilities in the pursuit of the objectives of the system of internal control; and

b. evaluating whether (Ref: par. A114–A119)

i. management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior;

ii. the control environment provides an appropriate foundation for the other components of the entity's system of internal control considering the nature and complexity of the entity; and

iii. control deficiencies identified in the control environment undermine the other components of the entity's system of internal control.

The Entity's Risk Assessment Process

22. The auditor should, through performing risk assessment procedures, obtain an understanding of the entity's risk assessment process relevant to the preparation of the financial statements by

a. understanding the entity's process for (Ref: par. A120–A122)

i. identifying business risks relevant to financial reporting objectives; (Ref: par. A69)

ii. assessing the significance of those risks, including the likelihood of their occurrence;

iii. addressing those risks; and

b. evaluating whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity. (Ref: par. A123–A125)

23. If the auditor identifies risks of material misstatement that management failed to identify, the auditor should

a. determine whether any such risks are of a kind that the auditor expects would have been identified by the entity's risk assessment process and, if so, obtain an understanding of why the entity's risk assessment process failed to identify such risks of material misstatement; and

b. consider the implications for the auditor's evaluation in paragraph 22*b.*

The Entity's Process for Monitoring the System of Internal Control

24. The auditor should, through performing risk assessment procedures, obtain an understanding of the entity's process for monitoring the system of internal control relevant to the preparation of the financial statements by (Ref: par. A126–A127)

a. understanding those aspects of the entity's process that address

i. ongoing and separate evaluations for monitoring the effectiveness of controls and the identification and remediation of control deficiencies identified (Ref: par.

A128–A129) and

ii. the entity's internal audit function, if any, including its nature, responsibilities, and activities (Ref: par. A130–A131).

b. understanding the sources of the information used in the entity's process to monitor the system of internal control, and the basis upon which management considers the information to be sufficiently reliable for the purpose (Ref: par. A132–A133).

c. evaluating whether the entity's process for monitoring the system of internal control is appropriate to the entity's circumstances considering the nature and complexity of the entity (Ref: par. A134–A135).

Information System and Communication, and Control Activities (Ref: par. A136–A143)

The Information System and Communication

25. The auditor should, through performing risk assessment procedures, obtain an understanding of the entity's information system and communication relevant to the preparation of the financial statements by (Ref: par. A144–A145)

a. understanding the entity's information-processing activities, including its data and information, the resources to be used in such activities and the policies that define, for significant classes of transactions, account balances, and disclosures (Ref: par. A146–A158)

i. how information flows through the entity's information system, including how

(a) transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger, and reported in the financial statements and

(b) information about events and conditions, other than transactions, is captured, processed, and disclosed in the financial statements,

ii. the accounting records, specific accounts in the financial statements, and other supporting records relating to the flows of information in the information system,

iii. the financial reporting process used to prepare the entity's financial statements, including disclosures, and

iv. the entity's resources, including the IT environment, relevant to preceding *a*(i) to *a*(iii).

b. understanding how the entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control (Ref: par. A159–A160)

i. between people within the entity, including how financial reporting roles and responsibilities are communicated,

ii. between management and those charged with governance,

iii. with external parties, such as those with regulatory authorities.

c. evaluating whether the entity's information system and communication appropriately support the preparation of the entity's financial statements in accordance with the applicable financial reporting framework (Ref: par. A161).

Control Activities

26. The auditor should, through performing risk assessment procedures, obtain an understanding of the control activities component by (Ref: par. A162–A173)

a. identifying controls that address risks of material misstatement at the assertion level in the control activities component as follows:

i. Controls that address a risk that is determined to be a significant risk (Ref: par. A174–A175)

ii. Controls over journal entries, including nonstandard journal entries used to record nonrecurring, unusual transactions, or adjustments (Ref: par. A176–A177)

iii. Controls for which the auditor plans to test operating effectiveness in determining the nature, timing, and extent of substantive testing, which should include controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence (Ref: par. A178–A180)

iv. Other controls that the auditor considers are appropriate to enable the auditor to meet the objectives of paragraph 13 with respect to risks at the assertion level, based on the auditor's professional judgment (Ref: par. A181–A182)

b. based on controls identified in (*a*), identifying the IT applications and the other aspects of the entity's IT environment that are subject to risks arising from the use of IT (Ref: par. A183–A190).

c. for such IT applications and other aspects of the IT environment identified in (*b*), identifying (Ref: par. A191–A193)

i. the related risks arising from the use of IT, and

ii. the entity's general IT controls that address such risks.

d. for each control identified in *a* or *c*(ii) (Ref: par. A194–A202)

i. evaluating whether the control is designed effectively to address the risk of material misstatement at the assertion level or effectively designed to support the operation of other controls

ii. determining whether the control has been implemented by performing procedures in addition to inquiry of the entity's personnel.

Control Deficiencies Within the Entity's System of Internal Control

27. Based on the auditor's evaluation of each of the components of the entity's system of internal control, the auditor should determine whether one or more control deficiencies have been identified. (Ref: par. A203–A204)

Identifying and Assessing the Risks of Material Misstatement (Ref: par. A205–A206)

Identifying Risks of Material Misstatement

28. The auditor should identify the risks of material misstatement and determine whether they exist at (Ref: par. A207–A213)

a. the financial statement level (Ref: par. A214–A221) or

b. the assertion level for classes of transactions, account balances, and disclosures (Ref: par. A222–A223).

29. The auditor should determine the relevant assertions and the related significant classes of transactions, account balances, and disclosures. (Ref: par. A224–A226)

Assessing Risks of Material Misstatement at the Financial Statement Level

30. For identified risks of material misstatement at the financial statement level, the auditor should assess the risks and (Ref: par. A214–A221)

a. determine whether such risks affect the assessment of risks at the assertion level, and

b. evaluate the nature and extent of their pervasive effect on the financial statements.

Assessing Risks of Material Misstatement at the Assertion Level

Assessing Inherent Risk (Ref: par. A227–A239)

31. For identified risks of material misstatement at the assertion level, the auditor should assess inherent risk by assessing the likelihood and magnitude of misstatement. In doing so, the auditor should take into account how, and the degree to which

a. inherent risk factors affect the susceptibility of relevant assertions to misstatement, and

b. the risks of material misstatement at the financial statement level affect the assessment of inherent risk for risks of material misstatement at the assertion level. (Ref: par. A237–A239)

32. The auditor should determine whether any of the assessed risks of material misstatement are significant risks. (Ref: par. A240–A243)

33. The auditor should determine whether substantive procedures alone cannot provide sufficient appropriate audit evidence for any of the risks of material misstatement at the assertion level. (Ref: par. A244–A247)

Assessing Control Risk

34. If the auditor plans to test the operating effectiveness of controls, the auditor should assess control risk. If the auditor does not plan to test the operating effectiveness of controls, the auditor's assessment of control risk should be such that the assessment of the risk of material misstatement is the same as the assessment of inherent risk. (Ref: par. A248–A252)

Evaluating the Audit Evidence Obtained From the Risk Assessment Procedures

35. The auditor should evaluate whether the audit evidence obtained from the risk assessment procedures provides an appropriate basis for the identification and assessment of the risks of material misstatement. If not, the auditor should perform additional risk assessment procedures until audit evidence has been obtained to provide such a basis. In identifying and assessing the risks of material misstatement, the auditor should take into account all audit evidence obtained from the risk assessment procedures, whether corroborative or contradictory to assertions made by management. (Ref: par. A253–A255)

Classes of Transactions, Account Balances, and Disclosures That Are Not Significant but Are Material

36. For material classes of transactions, account balances, or disclosures that have not been determined to be significant classes of transactions, account balances, or disclosures, the auditor should evaluate whether the auditor's determination remains appropriate. (Ref: par. A256–A257)

Revision of Risk Assessment

37. If the auditor obtains new information that is inconsistent with the audit evidence on which the auditor originally based the identification or assessments of the risks of material misstatement, the auditor should revise the identification or assessment. (Ref: par. A258)

Audit Documentation

38. The auditor should include in the audit documentation[11] (Ref: par. A259–A263)

a. the discussion among the engagement team and the significant decisions reached

b. key elements of the auditor's understanding in accordance with paragraphs 19, 21, 22, 24, and 26; the sources of information from which the auditor's understanding was obtained; and the risk assessment procedures performed

c. the evaluation of the design of identified controls, and determination whether such controls have been implemented, in accordance with the requirements in paragraph 26; and

d. the identified and assessed risks of material misstatement at the financial statement level and at the assertion level, including significant risks and risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence, and the rationale for the significant judgments made.

---

[11] Paragraphs .08–.12 and .A8–.A9 of AU-C section 230, *Audit Documentation*.

***

Application and Other Explanatory Material

Definitions (Ref: par. 12)

Assertions

A1. Categories of assertions are used by auditors to consider the different types of potential misstatements that may occur when identifying, assessing, and responding to the risks of material misstatement. Examples of these categories of assertions are described in paragraph A211. The assertions differ from the written representations required by AU-C section 580, *Written Representations*, to confirm certain matters or support other audit evidence.

Controls

A2. Controls are embedded within the components of the entity's system of internal control.

A3. Policies are implemented through the actions of personnel within the entity or through the restraint of personnel from taking actions that would conflict with such policies.

A4. Procedures may be mandated, through formal documentation or other communication by management or those charged with governance, or may result from behaviors that are not mandated but, rather, are conditioned by the entity's culture. Procedures may be enforced through the actions permitted by the IT applications used by the entity or other aspects of the entity's IT environment.

A5. Controls may be direct or indirect (see paragraph A107 and A136). *Direct controls* are controls that are precise enough to address risks of material misstatement at the assertion level. *Indirect controls* are controls that support direct controls. Although indirect controls are not sufficiently precise to prevent, or detect and correct, misstatements at the assertion level, they are foundational and may have an indirect effect on the likelihood that a misstatement will be prevented or detected on a timely basis.

General IT Controls

A6. The integrity of information may include the completeness, accuracy, and validity of transactions and other information. Although this proposed SAS does not prescribe the use of a particular internal control framework, the auditor may find the following guidance regarding the concepts encompassed by the term *validity*, from COSO's 2013 *Internal Control—Integrated Framework* (COSO framework), helpful: "Recorded transactions represent economic events that actually occurred and were executed according to prescribed procedures. Validity is generally achieved through control activities that include the authorization of transactions as specified by an organization's established policies and procedures (that is, approval by a person having the authority to do so)."[12]

---

[12] Section 7, "Control Activities" of COSO's 2013 *Internal Control—Integrated Framework.*

Information-Processing Controls

A7. Risks to the integrity of information arise from susceptibility to ineffective implementation of the entity's information policies, which are policies that define the information flows, records, and reporting processes in the entity's information system. Information-processing controls are procedures that support effective implementation of the entity's information policies. Information-processing controls may be automated (that is, embedded in IT applications) or manual (for example, input or output controls) and may rely on other controls, including other information-processing controls or general IT controls.

Inherent Risk Factors

A8. Appendix B sets out further considerations relating to understanding inherent risk factors.

A9. Inherent risk factors may be qualitative or quantitative and affect the susceptibility of assertions to misstatement. Qualitative inherent risk factors relating to the preparation of information required by the applicable financial reporting framework include the following:

- Complexity
- Subjectivity
- Change
- Uncertainty
- Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk

A10. Other inherent risk factors that affect susceptibility to misstatement of an assertion about a class of transactions, account balance, or disclosure may include one or both of the following:

- The quantitative or qualitative significance of the class of transactions, account balance, or disclosure
- The volume or a lack of uniformity in the composition of the items to be processed through the class of transactions or account balance, or to be reflected in the disclosure

Relevant Assertions

A11. A risk of material misstatement may relate to more than one assertion, in which case, all the assertions to which such a risk relates are relevant assertions. For the purposes of the AU-C sections, a risk of material misstatement exists when (*a*) there is a reasonable possibility of a misstatement occurring (that is, its likelihood), and (*b*) if it were to occur, there is a reasonable possibility of the misstatement being material (that is, its magnitude).[13] If an assertion does not have an identified risk of material misstatement, then it is not a relevant assertion.

---

[13] Paragraph .A43*a* of AU-C section 200 and paragraph .06 of AU-C section 330.

Risk Arising From the Use of IT

A12. Appendix E sets out further considerations relating to understanding IT.

Significant Risk

A13. Significance can be described as the relative importance of a matter and is judged by the auditor in the context in which the matter is being considered. For inherent risk, significance may be considered in the context of how, and the degree to which, inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur.

System of Internal Control

A14. Internal control frameworks may use different terms that are similar to the concept of *system of internal control*. For example, the 2013 COSO framework uses the term *internal control*.

Risk Assessment Procedures and Related Activities (Ref: par. 13–18)

A15. The risks of material misstatement to be identified and assessed include both those due to fraud and those due to error, and both are covered by this proposed SAS. However, the significance of fraud is such that further requirements and guidance are included in AU-C section 240 in relation to risk assessment procedures and related activities to obtain information that is used to identify and assess the risks of material misstatement due to fraud.[14] In addition, the following AU-C sections provide further requirements and guidance on identifying and assessing risks of material misstatement regarding specific matters or circumstances:

- AU-C section 540, *Auditing Accounting Estimates and Related Disclosures,* with regard to accounting estimates
- AU-C section 550, *Related Parties*, with regard to related party relationships and transaction
- AU-C section 570, *The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern,* with regard to going concern
- AU-C section 600, *Special Considerations — Audits of Group Financial Statements (Including the Work of Component Auditors)*, with regard to group financial statements

A16. Professional skepticism is necessary for the critical assessment of audit evidence gathered when performing the risk assessment procedures and assists the auditor in remaining alert to audit evidence that is not biased towards corroborating the existence of risks or that may be contradictory. Professional skepticism is an attitude that is applied by the auditor when making professional judgments that then provides the basis for the auditor's actions. The auditor applies professional judgment in determining when the auditor has audit evidence that provides an appropriate basis for risk assessment.

---

[14] Paragraphs .12–.27 of AU-C section 240.

A17. The application of professional skepticism by the auditor may include the following:

- Questioning contradictory information and the reliability of documents
- Considering responses to inquiries and other information obtained from management and those charged with governance
- Being alert to conditions that may indicate possible misstatement due to fraud or error
- Considering whether audit evidence obtained supports the auditor's identification and assessment of the risks of material misstatement in light of the entity's nature and circumstances

Why Obtaining Audit Evidence in an Unbiased Manner Is Important (Ref: par. 13)

A18. Designing and performing risk assessment procedures to obtain audit evidence to support the identification and assessment of the risks of material misstatement in an unbiased manner may assist the auditor in identifying potentially contradictory information, which may assist the auditor in exercising professional skepticism in identifying and assessing the risks of material misstatement.

Sources of Audit Evidence (Ref: par. 13)

A19. Designing and performing risk assessment procedures to obtain audit evidence in an unbiased manner may involve obtaining evidence from multiple sources within and outside the entity. However, the auditor is not required to perform an exhaustive search to identify all possible sources of audit evidence. In addition to information from other sources,[15] sources of information for risk assessment procedures may include the following:

- Interactions with management, those charged with governance, and other key entity personnel, such as internal auditors
- Certain external parties such as regulators, whether obtained directly or indirectly
- Publicly available information about the entity, for example, entity-issued press releases, materials for analysts or investor group meetings, analysts' reports, or information about trading activity

Regardless of the source of information, the auditor considers the relevance and reliability of the information to be used as audit evidence in accordance with AU-C section 500, *Audit Evidence*.[16]

Scalability (Ref: par. 13)

A20. The nature and extent of risk assessment procedures, including obtaining an understanding pursuant to the following requirements will vary based on the nature and circumstances of the

---

[15] See paragraph A41 and A42 of this proposed SAS.

[16] Paragraph .07 of AU-C section 500, *Audit Evidence*.

entity (for example, the formality of the entity's policies and procedures, and processes and systems):

a. Performing risk assessment procedures (paragraph 19)

b. Understanding the components of internal control

i. Control environment (paragraph 21)

ii. The entity's risk assessment process (paragraph 22)

iii. The entity's process to monitor the system of internal control (paragraph 24)

iv. The information system and communication (paragraph 25)

v. Control activities (paragraph 26)

The auditor uses professional judgment to determine the nature and extent of the risk assessment procedures to be performed to meet the requirements of this proposed SAS.

A21. Some entities, including less complex entities, and particularly owner-managed entities, may not have established structured processes and systems (for example, a risk assessment process or a process to monitor the system of internal control) or may have established processes or systems with limited documentation or a lack of consistency in how they are undertaken. When such systems and processes lack formality, the auditor may still be able to perform risk assessment procedures through observation and inquiry. Other entities, typically more complex entities, are expected to have more formalized and documented policies and procedures. The auditor may use such documentation in performing risk assessment procedures.

A22. The nature and extent of risk assessment procedures to be performed in an initial audit may be more extensive than procedures for a recurring engagement. In subsequent periods, the auditor may focus on changes that have occurred since the preceding period.

Types of Risk Assessment Procedures (Ref: par. 14)

A23. AU-C section 500[17] explains the types of audit procedures that may be performed in obtaining audit evidence from risk assessment procedures and further audit procedures. The nature, timing, and extent of the audit procedures may be affected by the fact that some of the accounting data and other evidence may be available only in electronic form or only at certain points in time.[18] The auditor may perform substantive procedures or tests of controls, in accordance with AU-C section 330, concurrently with risk assessment procedures, such as when it is efficient to do so. Audit evidence obtained that supports the identification and assessment of risks of material misstatement may also support the detection of misstatements at the assertion level or the evaluation of the operating effectiveness of controls.

---

17 Paragraphs .A14–.A17 and .A21–.A26 of AU-C section 500.

18 Paragraph .A12 of AU-C section 500.

A24. Although the auditor is required to perform all the risk assessment procedures described in paragraph 14 in the course of obtaining the required understanding of the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control (see paragraphs 19–26), the auditor is not required to perform all of them for each aspect of that understanding. Other procedures may be performed when the information to be obtained may be helpful in identifying risks of material misstatement. Examples of such procedures may include making inquiries of the entity's external legal counsel, or of valuation specialists that the entity has used.

Automated Tools and Techniques (Ref: par. 14)

A25. Using automated tools and techniques, the auditor may perform risk assessment procedures on large volumes of data (from the general ledger, sub-ledgers, or other operational data), including for analysis, recalculations, reperformance, or reconciliations.

Inquiries of Management and Others Within the Entity (Ref: par. 14a)

Why Inquiries Are Made of Management and Others Within the Entity

A26. Information obtained by the auditor to support an appropriate basis for the identification and assessment of risks, and the design of further audit procedures, may be obtained through inquiries of management and those responsible for financial reporting.

A27. Inquiries of management and those responsible for financial reporting and of other appropriate individuals within the entity and other employees with different levels of authority may offer the auditor varying perspectives when identifying and assessing risks of material misstatement. Examples follow:

- Inquiries directed toward those charged with governance may help the auditor understand the extent of oversight by those charged with governance over the preparation of the financial statements by management. AU-C section 260, *The Auditor's Communication With Those Charged With Governance*,[19] identifies the importance of effective two-way communication in assisting the auditor to obtain information from those charged with governance in this regard.
- Inquiries of employees responsible for initiating, processing, or recording complex or unusual transactions may help the auditor to evaluate the appropriateness of the selection and application of certain accounting policies.
- Inquiries directed toward in-house legal counsel may provide information about such matters as litigation; compliance with laws and regulations; knowledge of fraud or suspected fraud affecting the entity; warranties; post-sales obligations; arrangements (such as joint ventures) with business partners; and the meaning of contractual terms.

[19] Paragraph .A1 of AU-C section 260, *The Auditor's Communication With Those Charged With Governance*.

- Inquiries directed toward marketing or sales personnel may provide information about changes in the entity's marketing strategies, sales trends, or contractual arrangements with its customers.
- Inquiries directed toward the risk management function (or inquiries of those performing such roles) may provide information about operational and regulatory risks that may affect financial reporting.
- Inquiries directed toward IT personnel may provide information about IT processes as well as system changes, system or control failures, or other IT-related risks.

Considerations Specific to Governmental Entities

A28. When making inquiries of those who may have information that is likely to assist in identifying risks of material misstatement, auditors of governmental entities may obtain information from additional sources such as from the auditors that are involved in performance or other audits related to the entity.

*Inquiries of the Internal Audit Function (Ref: par. 14*a*)*

Why Inquiries Are Made of the Internal Audit Function (If the Function Exists)

A29. If an entity has an internal audit function, inquiries of the appropriate individuals within the function may assist the auditor in understanding the entity and its environment, and the entity's system of internal control, in the identification and assessment of risks. Appendix D sets out considerations for understanding an entity's internal audit function.

Considerations Specific to Governmental Entities

A30. Auditors of governmental entities often have additional responsibilities with regard to internal control and compliance with applicable laws and regulations. Inquiries of appropriate individuals in the internal audit function may assist the auditors in identifying the risk of material noncompliance with applicable laws and regulations and the risk of control deficiencies related to financial reporting.

Analytical Procedures (Ref: par. 14*b*)

Why Analytical Procedures Are Performed as a Risk Assessment Procedure

A31. Analytical procedures help identify inconsistencies, unusual transactions or events, and amounts, ratios, and trends that indicate matters that may have audit implications. Unusual or unexpected relationships that are identified may assist the auditor in identifying risks of material misstatement, especially risks of material misstatement due to fraud.

A32. Analytical procedures performed as risk assessment procedures may, therefore, assist in identifying and assessing the risks of material misstatement by identifying aspects of the entity of which the auditor was unaware or understanding how inherent risk factors, such as change, affect susceptibility of assertions to misstatement.

Types of Analytical Procedures

A33. Analytical procedures performed as risk assessment procedures may be as follows:

- Include both financial and nonfinancial information, for example, the relationship between sales and square footage of selling space or volume of goods sold (nonfinancial).
- Use data aggregated at a high level. Accordingly, the results of those analytical procedures may provide a broad initial indication about the likelihood and potential magnitude of a material misstatement. For example, in the audit of many entities, including those with less complex business models and processes, and a less complex information system, the auditor may perform a comparison of information, such as the change in interim or monthly account balances from balances in prior periods, to obtain an indication of potentially higher risk areas.

A34. This proposed SAS addresses the auditor's use of analytical procedures as risk assessment procedures. AU-C section 520, *Analytical Procedures*, addresses the auditor's use of analytical procedures as substantive procedures (substantive analytical procedures) and the auditor's responsibility to perform analytical procedures near the end of the audit. Accordingly, analytical procedures performed as risk assessment procedures are not required to be performed in accordance with the requirements of AU-C section 520. However, the requirements and application material in AU-C section 520 may provide useful guidance to the auditor when performing analytical procedures as part of the risk assessment procedures.

Automated Tools and Techniques

A35. Analytical procedures can be performed using a number of tools or techniques, which may be automated. Applying automated analytical procedures to the data may be referred to as *data analytics*. For example, the auditor may use a spreadsheet to perform a comparison of actual recorded amounts to budgeted amounts or may perform a more advanced procedure by extracting data from the entity's information system, and further analyzing this data using visualization techniques to identify classes of transactions, account balances, or disclosures for which further specific risk assessment procedures may be warranted.

Observation and Inspection (Ref: par. 14c)

Why Observation and Inspection Are Performed as Risk Assessment Procedures

A36. Observation and inspection may support, corroborate, or contradict inquiries of management and others and may also provide information about the entity and its environment.

Scalability

A37. When policies or procedures are not documented, or the entity has less formalized controls, the auditor may still be able to obtain some audit evidence to support the identification and assessment of the risks of material misstatement through observation or inspection of the performance of the control. Examples are as follows:

- The auditor may obtain an understanding of controls over an inventory count, even if they have not been documented by the entity, through a combination of inquiry and direct observation.

- The auditor may be able to observe segregation of duties.

- The auditor may be able to observe passwords being entered.

Observation and Inspection as Risk Assessment Procedures

A38. Risk assessment procedures may include observation or inspection of the following:

- The entity's operations
- Internal documents (such as business plans and strategies), records, and internal control manuals
- Reports prepared by management (such as quarterly management reports and interim financial statements) and those charged with governance (such as minutes of board of directors' meetings)
- The entity's premises and plant facilities
- Information obtained from external sources such as trade and economic journals; reports by analysts, banks, or rating agencies; regulatory or financial publications; or other external documents about the entity's financial performance (such as those referred to in paragraph A86)
- The behaviors and actions of management or those charged with governance (such as the observation of an audit committee meeting)

Automated Tools or Techniques

A39. Automated tools or techniques may also be used to observe or inspect, in particular assets, for example, through the use of remote observation tools (for example, a drone).

Considerations Specific to Governmental Entities

A40. Risk assessment procedures performed by auditors of governmental entities may also include observation and inspection of documents prepared by management for the governing body, for example, documents related to performance reporting.

Information From Other Sources (Ref: par. 15)

Why the Auditor Considers Information From Other Sources

A41. Information obtained from other sources may be relevant to the identification and assessment of the risks of material misstatement by providing information and insights about the following:

- The nature of the entity and its business risks, and what may have changed from previous periods
- The integrity and ethical values of management and those charged with governance, which may also be relevant to the auditor's understanding of the control environment

The Applicable Financial Reporting Framework and Its Application to the Nature and Circumstances of the Entity

Other Relevant Sources

A42. Other relevant sources of information are as follows:

- The auditor's procedures regarding acceptance or continuance of the client relationship or the audit engagement in accordance with AU-C section 220, *Quality Control for an Engagement Conducted in Accordance With Generally Accepted Auditing Standards*, including the conclusions reached thereon.[20]
- Other engagements performed for the entity by the engagement partner. The engagement partner may have obtained knowledge relevant to the audit, including about the entity and its environment, when performing other engagements for the entity. Such engagements may include agreed-upon procedures engagements or other audit or assurance engagements, including engagements to address incremental reporting requirements in the jurisdiction.

Information From the Auditor's Previous Experience With the Entity and Previous Audits (Ref: par. 16)

Why Information From Previous Audits Is Important to the Current Audit

A43. The auditor's previous experience with the entity and from audit procedures performed in previous audits may provide the auditor with information that is relevant to the auditor's determination of the nature and extent of risk assessment procedures, and the identification and assessment of risks of material misstatement.

Nature of the Information From Previous Audits

A44. The auditor's previous experience with the entity and audit procedures performed in previous audits may provide the auditor with information about the following matters:

- Past misstatements and whether they were corrected on a timely basis
- The nature of the entity and its environment, and the entity's system of internal control (including control deficiencies)

---

[20] Paragraph .14 of AU-C section 220, *Quality Control for an Engagement Conducted in Accordance With Generally Accepted Auditing Standards*.

- Significant changes that the entity or its operations may have undergone since the prior financial period
- Those particular types of transactions and other events or account balances (and related disclosures) in which the auditor experienced difficulty in performing the necessary audit procedures, for example, due to their complexity

A45. The auditor is required to determine whether information obtained from the auditor's previous experience with the entity and from audit procedures performed in previous audits remains relevant and reliable, if the auditor intends to use that information for the purposes of the current audit. If the nature or circumstances of the entity have changed, or new information has been obtained, the information from prior periods may no longer be relevant or reliable for the current audit. To determine whether changes have occurred that may affect the relevance or reliability of such information, the auditor may make inquiries and perform other appropriate audit procedures, such as walk-throughs of relevant systems. If the information is not reliable, the auditor may consider performing additional procedures that are appropriate in the circumstances.

Engagement Team Discussion (Ref: par. 17–18)

Why the Engagement Team Is Required to Discuss the Application of the Applicable Financial Reporting Framework and the Susceptibility of the Entity's Financial Statements to Material Misstatement

A46. Key engagement team members include those members who have significant engagement responsibilities, including the engagement partner. The manner in which the discussion is conducted depends on the individuals involved and the circumstances of the engagement. For example, if the audit involves more than one location, there could be multiple discussions with team members in different locations.

A47. The discussion among the engagement team about the application of the applicable financial reporting framework and the susceptibility of the entity's financial statements to material misstatement accomplishes the following:

- Provides an opportunity for more experienced engagement team members, including the engagement partner, to share their insights based on their knowledge of the entity. Sharing information contributes to an enhanced understanding by all engagement team members.
- Allows the engagement team members to exchange information about the business risks to which the entity is subject, how inherent risk factors may affect the susceptibility to misstatement of classes of transactions, account balances, and disclosures, and about how and where the financial statements might be susceptible to material misstatement due to fraud or error.
- Assists the engagement team members to gain a better understanding of the potential for material misstatement of the financial statements in the specific areas assigned to them and to understand how the results of the audit procedures that they perform may affect other aspects of the audit, including the decisions about the nature, timing, and

extent of further audit procedures. In particular, the discussion assists engagement team members in further considering contradictory information based on each member's own understanding of the nature and circumstances of the entity.

- Provides a basis upon which engagement team members communicate and share new information obtained throughout the audit that may affect the assessment of risks of material misstatement or the audit procedures performed to address these risks.

AU-C section 240 requires the engagement team discussion to place particular emphasis on how and where the entity's financial statements may be susceptible to material misstatement due to fraud, including how fraud may occur.[21]

A48. Professional skepticism is necessary for the critical assessment of audit evidence, and a robust and open engagement team discussion, including for recurring audits, may lead to improved identification and assessment of the risks of material misstatement. Another outcome from the discussion may be that the auditor identifies specific areas of the audit for which exercising professional skepticism may be particularly important and may lead to the involvement of more experienced members of the engagement team who are appropriately skilled to be involved in the performance of audit procedures related to those areas.

Scalability

A49. When the engagement is carried out by a single individual, such as a sole practitioner (that is, when an engagement team discussion would not be possible), consideration of the matters referred to in paragraphs A47 and A51, nonetheless, may assist the auditor in identifying where there may be risks of material misstatement.

A50. When an engagement is carried out by a large engagement team, such as for an audit of group financial statements, it is not always necessary or practical for the discussion to include all members in a single discussion (for example, in a multi-location audit), nor is it necessary for all the members of the engagement team to be informed of all the decisions reached in the discussion. The engagement partner may discuss matters with key members of the engagement team, including, if considered appropriate, those with specific skills or knowledge and those responsible for the audits of components, while delegating discussion with others, taking into account the extent of communication considered necessary throughout the engagement team. A communications plan, agreed to by the engagement partner, may be useful.

Discussion of Disclosures in the Applicable Financial Reporting Framework

A51. As part of the discussion among the engagement team, consideration of the disclosure requirements of the applicable financial reporting framework assists in identifying early in the audit where there may be risks of material misstatement in relation to disclosures, even in circumstances in which the applicable financial reporting framework requires only simplified disclosures. Matters the engagement team may discuss include the following:

---

[21] Paragraph .15 of AU-C section 240.

- Changes in financial reporting requirements that may result in significant, new, or revised disclosures
- Changes in the entity's environment, financial condition, or activities that may result in significant, new, or revised disclosures, for example, a significant business combination in the period under audit
- Disclosures for which obtaining sufficient appropriate audit evidence may have been difficult in the past
- Disclosures about complex matters, including those involving significant management judgment about what information to disclose

Considerations Specific to Governmental Entities

A52. As part of the discussion among the engagement team by auditors of governmental entities, consideration may also be given to any additional broader objectives, and related risks, arising from audit requirements of governmental entities.

Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework, and the Entity's System of Internal Control (Ref: par. 19–27)

A53. Appendixes A–F set out further considerations relating to obtaining an understanding of the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control.

Obtaining the Required Understanding (Ref: par. 19–27)

A54. Obtaining an understanding of the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control is a dynamic and iterative process of gathering, updating, and analyzing information and continues throughout the audit. Therefore, the auditor's expectations may change as new information is obtained.

A55. The auditor's understanding of the entity and its environment and the applicable financial reporting framework may also assist the auditor in developing initial expectations about the classes of transactions, account balances, and disclosures that may be significant classes of transactions, account balances, and disclosures. These expected significant classes of transactions, account balances, and disclosures form the basis for the scope of the auditor's understanding of the entity's information system.

Why an Understanding of the Entity and Its Environment, and the Applicable Financial Reporting Framework, Is Required (Ref: par. 19–20)

A56. The auditor's understanding of the entity and its environment and the applicable financial reporting framework assist the auditor

a. in understanding the events and conditions that are relevant to the entity, and

b. in identifying how inherent risk factors affect the susceptibility of assertions to misstatement in the preparation of the financial statements, in accordance with the applicable financial reporting framework, and the degree to which they do so.

Such information establishes a frame of reference within which the auditor identifies and assesses risks of material misstatement. This frame of reference also assists the auditor in planning the audit and exercising professional judgment and professional skepticism throughout the audit, for example, when

- identifying and assessing risks of material misstatement of the financial statements in accordance with this proposed SAS or other relevant AU-C sections (for example, relating to risks of fraud in accordance with AU-C section 240 or when identifying or assessing risks related to accounting estimates in accordance with AU-C section 540);
- performing procedures to help identify instances of noncompliance with laws and regulations that may have a material effect on the financial statements in accordance with AU-C section 250, *Consideration of Laws and Regulations in an Audit of Financial Statements*;[22]
- evaluating whether the financial statements provide adequate disclosures in accordance with AU-C section 700, *Forming an Opinion and Reporting on Financial Statements*;[23]
- determining materiality or performance materiality in accordance with AU-C section 320, *Materiality in Planning and Performing an Audit*;[24] or
- considering the appropriateness of the selection and application of accounting policies and the adequacy of financial statement disclosures.

A57. The auditor's understanding of the entity and its environment, and the applicable financial reporting framework, also informs how the auditor plans and performs further audit procedures, for example, when

- developing expectations for use when performing analytical procedures in accordance with AU-C section 520;[25]
- designing and performing further audit procedures to obtain sufficient appropriate audit evidence in accordance with AU-C section 330; and
- evaluating the sufficiency and appropriateness of audit evidence obtained (for example, relating to assumptions or management's oral and written representations).

Scalability (Ref: par. 19–20)

---

22 Paragraph .13 of AU-C section 250, *Consideration of Laws and Regulations in an Audit of Financial Statements*.

23 Paragraph .15*f* of AU-C section 700, *Forming an Opinion and Reporting on Financial Statements*.

24 Paragraphs .10–.11 of AU-C section 320, *Materiality in Planning and Performing an Audit*.

25 Paragraph .05 of AU-C section 520, *Analytical Procedures*.

A58. The nature and extent of the required understanding is a matter of the auditor's professional judgment and varies from entity to entity based on the nature and circumstances of the entity, including the following:

- The size and complexity of the entity, including its IT environment
- The auditor's previous experience with the entity
- The nature of the entity's systems and processes, including whether they are formalized or not
- The nature and form of the entity's documentation

A59. The auditor's risk assessment procedures to obtain the required understanding may be less extensive in audits of less complex entities and more extensive for entities that are more complex. The depth of the understanding that is required by the auditor is expected to be less than that possessed by management in managing the entity.

A60. Some financial reporting frameworks allow smaller entities to provide simpler and less detailed disclosures in the financial statements. However, this does not relieve the auditor of the responsibility to obtain an understanding of the entity and its environment and the applicable financial reporting framework as it applies to the entity.

A61. The entity's use of IT and the nature and extent of changes in the IT environment, including the risks arising from the use of IT, may also affect the specialized skills that are needed to assist with obtaining the required understanding.

The Entity and Its Environment (Ref: par. 19)

The Entity's Organizational Structure, Ownership and Governance, and Business Model (Ref: par. 19*a*(i))

The Entity's Organizational Structure and Ownership (Ref: par. 19*a*(i))

A62. An understanding of the entity's organizational structure and ownership may enable the auditor to understand the following matters:

- The complexity of the entity's structure. For example, the entity may be a single entity or the entity's structure may include subsidiaries, divisions, or other components in multiple locations. Further, the legal structure may be different from the operating structure. Complex structures often introduce factors that may give rise to increased susceptibility to risks of material misstatement. Such issues may include whether goodwill, joint ventures, investments, or variable interest entities are accounted for appropriately and whether adequate disclosure of such issues in the financial statements has been made.
- The ownership, and relationships between owners and other people or entities, including related parties. This understanding may assist in determining whether related

party transactions have been appropriately identified, accounted for, and adequately disclosed in the financial statements.[26]

- The distinction between the owners, those charged with governance and management. For example, in less complex entities, owners of the entity may be involved in managing the entity, therefore, there is little or no distinction. In contrast, such as in some larger entities with diverse ownership, there may be a clear distinction between management, the owners of the entity, and those charged with governance.[27]
- The structure and complexity of the entity's IT environment. For example, an entity may
  - — have multiple legacy IT systems in diverse businesses that are not well integrated, resulting in a complex IT environment.
  - — be using external or internal service providers for aspects of its IT environment (for example, outsourcing the hosting of its IT environment to a third party or using a shared service center for central management of IT processes in a group).

Automated Tools and Techniques

A63. The auditor may use automated tools and techniques to understand flows of transactions and processing as part of the auditor's procedures to understand the information system. An outcome of these procedures may be that the auditor obtains information about the entity's organizational structure or those with whom the entity conducts business (for example, vendors, customers, related parties).

Considerations Specific to Governmental Entities

A64. Ownership of a governmental entity may not have the same relevance as in the private sector because many governmental entities do not have owners or because decisions related to the entity may be made outside of the entity as a result of political processes. Therefore, management may not have control over certain decisions that are made. Matters that may be relevant include understanding the ability of the entity to make unilateral decisions and the ability of other governmental entities to control or influence the entity's mandate and strategic direction. For example, a governmental entity may be subject to laws or other directives from authorities that require it to obtain approval from parties external to the entity of its strategy and objectives prior to it implementing them. Therefore, matters related to understanding the legal structure of the entity may include applicable laws and regulations, and the classification of the entity (that is, whether the entity is a department, agency, or other type of entity).

Governance (Ref: par. 19*a*(i))

---

[26] AU-C section 550 addresses the auditor's considerations relevant to related parties.

[27] Paragraphs .A6–.A7 of AU-C section 260 provide guidance on the identification of those charged with governance and explain that in some cases, some or all of those charged with governance may be involved in managing the entity.

Why the Auditor Obtains an Understanding of Governance

A65. Understanding the entity's governance may assist the auditor with understanding the entity's ability to provide appropriate oversight of its system of internal control. However, this understanding may also provide evidence of deficiencies, which may indicate an increase in the susceptibility of the entity's financial statements to risks of material misstatement.

Understanding the Entity's Governance

A66. The following matters may be relevant for the auditor to consider in obtaining an understanding of the governance of the entity:

- Whether any or all of those charged with governance are involved in managing the entity
- The existence (and separation) of a non-executive board, if any, from executive management
- Whether those charged with governance hold positions that are an integral part of the entity's legal structure, for example, as directors
- The existence of subgroups of those charged with governance, such as an audit committee, and the responsibilities of such a group
- The responsibilities of those charged with governance for oversight of financial reporting, including approval of the financial statements

The Entity's Business Model (Ref: par. 19*a*(i))

A67. Appendixes A–B set out additional considerations for obtaining an understanding of the entity and its business model as well as additional considerations for auditing variable interest entities.

Why the Auditor Obtains an Understanding of the Entity's Business Model

A68. Understanding the entity's objectives, strategy, and business model helps the auditor to understand the entity at a strategic level and to understand the business risks the entity takes and faces. An understanding of the business risks that have an effect on the financial statements assists the auditor in identifying risks of material misstatement because most business risks will eventually have financial consequences and, therefore, an effect on the financial statements. For example, an entity's business model may rely on the use of IT in different ways:

- An entity sells shoes from a physical store and uses an advanced stock and point of sale system to record the selling of shoes.
- An entity sells shoes online so that all sales transactions are processed in an IT environment, including initiation of the transactions through a website.

The business risks arising from a significantly different business model would be substantially different, notwithstanding both entities sell shoes.

Understanding the Entity's Business Model

A69. Not all aspects of the business model are relevant to the auditor's understanding. Business risks are broader than the risks of material misstatement of the financial statements, although business risks include the latter. The auditor does not have a responsibility to understand or identify all business risks because not all business risks give rise to risks of material misstatement.

A70. Business risks increasing the susceptibility to risks of material misstatement may arise from the following:

- Inappropriate objectives or strategies, ineffective execution of strategies, or change or complexity
- A failure to recognize the need for change may also give rise to business risk, for example, from
  - — the development of new products or services that may fail;
  - — a market which, even if successfully developed, is inadequate to support a product or service; or
  - — flaws in a product or service that may result in legal liability and reputational risk
- Incentives and pressures on management, which may result in intentional or unintentional management bias and, therefore, affect the reasonableness of significant assumptions and the expectations of management or those charged with governance

A71. Examples of matters that the auditor may consider when obtaining an understanding of the entity's business model, objectives, strategies, and related business risks that may result in a risk of material misstatement of the financial statements may include the following:

- Industry developments, such as the lack of personnel or expertise to deal with the changes in the industry
- New products and services that may lead to increased product liability
- Expansion of the entity's business, and demand has not been accurately estimated
- New accounting requirements in which there has been incomplete or improper implementation
- Regulatory requirements resulting in increased legal exposure
- Current and prospective financing requirements, such as loss of financing due to the entity's inability to meet requirements
- Use of IT, such as the implementation of a new IT system that will affect both operations and financial reporting
- The effects of implementing a strategy, particularly any effects that will lead to new accounting requirements

A72. Ordinarily, management identifies business risks and develops approaches to address them. Such a risk assessment process is part of the entity's system of internal control and is discussed in paragraph 22 and paragraphs A119–A124.

Considerations Specific to Governmental Entities

A73. Entities operating in the governmental sector may create and deliver value in different ways from those creating wealth for owners but will still have an operating "model" with specific objectives. Matters that governmental sector auditors may obtain an understanding of that are relevant to the model of the entity include the following:

- Knowledge of relevant government activities, including related programs
- Program objectives and strategies, including public policy elements

A74. For the audits of governmental entities, "management objectives" may be influenced by requirements to demonstrate public accountability and may include objectives that have their source in law, regulation, or other authority.

*Industry, Regulatory, and Other External Factors (Ref: par. 19*a*(ii))*

Industry Factors

A75. Relevant industry factors include industry conditions such as the competitive environment, supplier and customer relationships, and technological developments. The following are matters the auditor may consider:

- The market and competition, including demand, capacity, and price competition
- Cyclical or seasonal activity
- Product technology relating to the entity's products
- Energy supply and cost

A76. The industry in which the entity operates may give rise to specific risks of material misstatement arising from the nature of the business or the degree of regulation. For example, in the construction industry, long-term contracts may involve significant estimates of revenues and expenses that give rise to risks of material misstatement. In such cases, it is important that the engagement team include members with sufficient relevant knowledge and experience.[28]

Regulatory Factors (Ref: par. 19*a*(ii))

A77. Relevant regulatory factors include the regulatory environment. The regulatory environment encompasses, among other matters, the applicable financial reporting framework and

[28] Paragraph .16 of AU-C section 220.

the legal and political environment and any changes thereto. The following are matters the auditor may consider:

- Regulatory framework for a regulated industry, including related disclosures
- Legislation and regulation that significantly affect the entity's operations, for example, labor laws and regulations
- Taxation legislation and regulations
- Government policies currently affecting the conduct of the entity's business, such as monetary policies, including foreign exchange controls, fiscal policies, financial incentives (for example, government aid programs), and tariffs or trade restriction policies
- Environmental requirements affecting the industry and the entity's business

A78. AU-C section 250 includes some specific requirements related to the legal and regulatory framework applicable to the entity and the industry or sector in which the entity operates.[29]

Considerations Specific to Governmental Entities

A79. For the audits of governmental entities, particular laws or regulations may affect the entity's operations. Such elements may be an essential consideration when obtaining an understanding of the entity and its environment.

Other External Factors (Ref: par. 19*a*(ii))

A80. Other external factors affecting the entity that the auditor may consider include the general economic conditions, interest rates and availability of financing, and inflation or currency revaluation.

*Measures Used by Management to Assess the Entity's Financial Performance (Ref: par. 19*a(iii)*)*

Why the Auditor Understands Measures Used by Management

A81. An understanding of the entity's measures assists the auditor in considering whether such measures, whether used externally or internally, create pressures on the entity to achieve performance targets. These pressures may motivate management to take actions that increase the susceptibility to misstatement due to management bias or fraud (for example, to improve the business performance or to intentionally misstate the financial statements) (see AU-C section 240 for requirements and guidance in relation to the risks of fraud).

A82. Measures may also indicate to the auditor the likelihood of risks of material misstatement of related financial statement information. For example, performance measures may indicate that

[29] Paragraph .12 of AU-C section 250.

the entity has unusually rapid growth or profitability when compared to that of other entities in the same industry.

Measures Used by Management

A83. Management and others ordinarily measure and review those matters they regard as important. Inquiries of management may reveal that it relies on certain key indicators, regardless of public availability, for evaluating financial performance and taking action. In such cases, the auditor may identify relevant performance measures, whether internal or external, by considering the information that the entity uses to manage its business. If such inquiry indicates an absence of performance measurement or review, there may be an increased risk of misstatements not being detected and corrected.

A84. Key indicators used for evaluating financial performance may include the following:

- Key performance indicators (financial and nonfinancial) and key ratios, trends, and operating statistics
- Period-on-period financial performance analyses
- Budgets, forecasts, variance analyses, segment information and divisional, departmental, or other level performance reports
- Employee performance measures and incentive compensation policies
- Comparisons of an entity's performance with that of competitors

Scalability (Ref: par. 19*a*(iii))

A85. The procedures undertaken to understand the entity's measures may vary depending on the size or complexity of the entity as well as the involvement of owners or those charged with governance in the management of the entity.

Other Considerations

A86. External parties may also review and analyze the entity's financial performance, in particular, for entities in which financial information is publicly available. The auditor may also consider publicly available information to help the auditor further understand the business or identify contradictory information, such as information from the following sources:

- Analysts or credit agencies
- News and other media, including social media
- Taxation authorities
- Regulators
- Trade unions
- Providers of finance

Such financial information can often be obtained from the entity being audited.

A87. The measurement and review of financial performance is not the same as the monitoring of the system of internal control (discussed as a component of the system of internal control in paragraphs A125–A134), though their purposes may overlap:

- The measurement and review of performance is directed at whether business performance is meeting the objectives set by management (or third parties).
- In contrast, monitoring of the system of internal control is concerned with monitoring the effectiveness of controls including those related to management's measurement and review of financial performance.

In some cases, however, performance indicators also provide information that enables management to identify control deficiencies.

Considerations Specific to Governmental Entities

A88. In addition to considering relevant measures used by a governmental entity to assess the entity's financial performance, auditors of governmental entities may also consider nonfinancial information, such as achievement of public benefit outcomes (for example, the number of people assisted by a specific program).

The Applicable Financial Reporting Framework (Ref: par. 19b)

Understanding the Applicable Financial Reporting Framework and the Entity's Accounting Policies

A89. Matters that the auditor may consider when obtaining an understanding of the entity's applicable financial reporting framework and how it applies in the context of the nature and circumstances of the entity and its environment include the following:

- The entity's financial reporting practices in terms of the applicable financial reporting framework, such as
  - accounting principles and industry-specific practices, including for industry-specific significant classes of transactions, account balances, and related disclosures in the financial statements (for example, loans and investments for banks or research and development for pharmaceuticals)
  - revenue recognition
  - accounting for financial instruments, including related credit losses
  - foreign currency assets, liabilities, and transactions
  - accounting for unusual or complex transactions, including those in controversial or emerging areas (for example, accounting for cryptocurrency)

- An understanding of the entity's selection and application of accounting policies, including any changes thereto as well as the reasons therefor, may encompass the following matters:
    - The methods the entity uses to recognize, measure, present, and disclose significant and unusual transactions
    - The effect of significant accounting policies in controversial or emerging areas for which there is a lack of authoritative guidance or consensus
    - Changes in the environment, such as changes in the applicable financial reporting framework or tax reforms that may necessitate a change in the entity's accounting policies
    - Financial reporting standards and laws and regulations that are new to the entity and when and how the entity will adopt, or comply with, such requirements

A90. Obtaining an understanding of the entity and its environment may assist the auditor in considering where changes in the entity's financial reporting (for example, from prior periods) may be expected. For example, if the entity has had a significant business combination during the period, the auditor would likely expect changes in classes of transactions, account balances, and disclosures associated with that business combination. Alternatively, if there were no significant changes in the financial reporting framework during the period, the auditor's understanding may help confirm that the understanding obtained in the prior period remains applicable.

Considerations Specific to Governmental Entities

A91. The applicable financial reporting framework for a governmental entity may be generally accepted accounting principles established by the Federal Accounting Standards Advisory Board or GASB, or a special purpose framework.

How Inherent Risk Factors Affect Susceptibility of Assertions to Misstatement (Ref: par. 19c)

A92. Appendix B provides examples of events and conditions that may give rise to the existence of risks of material misstatement, categorized by inherent risk factor.

Why the Auditor Understands Inherent Risk Factors When Understanding the Entity and Its Environment, and the Applicable Financial Reporting Framework

A93. Understanding the entity and its environment, and the applicable financial reporting framework, assists the auditor in identifying events or conditions, the characteristics of which may affect the susceptibility of assertions about classes of transactions, account balances, or disclosures to misstatement. These characteristics are inherent risk factors. Inherent risk factors may affect susceptibility of assertions to misstatement by influencing the likelihood of occurrence of a misstatement or the magnitude of the misstatement if it were to occur. Understanding how inherent risk factors affect the susceptibility of assertions to misstatement may assist the auditor with a preliminary understanding of the likelihood or magnitude of misstatements, which assists the auditor in identifying risks of material misstatement at the assertion level in accordance with

paragraph 28*b*. Understanding the degree to which inherent risk factors affect susceptibility of assertions to misstatement also assists the auditor in assessing the likelihood and magnitude of a possible misstatement when assessing inherent risk in accordance with paragraph 31*b*. Accordingly, understanding the inherent risk factors may also assist the auditor in designing and performing further audit procedures in accordance with AU-C section 330.

A94. The auditor's identification of risks of material misstatement at the assertion level and assessment of inherent risk may also be influenced by audit evidence obtained by the auditor in performing other risk assessment procedures, further audit procedures, or in fulfilling other requirements in GAAS (see paragraph A105).

The Effect of Inherent Risk Factors on a Class of Transactions, Account Balance, or Disclosure

A95. The extent of susceptibility to misstatement of a class of transactions, account balance, or disclosure arising from complexity or subjectivity is often closely related to the extent to which it is subject to change or uncertainty. For example, if the entity has an accounting estimate that is based on assumptions, the selection of which are subject to significant judgment, the measurement of the accounting estimate is likely to be affected by both subjectivity and uncertainty.

A96. The greater the extent to which a class of transactions, account balance, or disclosure is susceptible to misstatement because of complexity or subjectivity, the greater the need for the auditor to apply professional skepticism. Further, when a class of transactions, account balance, or disclosure is susceptible to misstatement because of complexity, subjectivity, change, or uncertainty, these inherent risk factors may create opportunity for management bias, whether unintentional or intentional, and affect susceptibility to misstatement due to management bias. The auditor's identification of risks of material misstatement, and assessment of inherent risk at the assertion level, are also affected by the interrelationships among inherent risk factors.

A97. Events or conditions that may affect susceptibility to misstatement due to management bias may also affect susceptibility to misstatement due to other fraud risk factors. Accordingly, this may be relevant information for use in accordance with AU-C section 240,[30] which requires the auditor to evaluate whether the information obtained from the other risk assessment procedures and related activities indicates that one or more fraud risk factors are present.

Obtaining an Understanding of the Entity's System of Internal Control (Ref: par. 21–27)

A98. Appendix C further describes the nature of the entity's system of internal control and inherent limitations of internal control, respectively. Appendix C also provides further explanation of the components of a system of internal control for purposes of GAAS.

A99. The auditor's understanding of the entity's system of internal control is obtained through risk assessment procedures performed to understand and evaluate each of the components of the system of internal control as set out in paragraphs 21–27. An audit does not require an understanding of all the controls within each component.

---

[30] Paragraph .20 of AU-C section 240.

A100. Risk assessment procedures to obtain an understanding of the control environment, the entity's risk assessment process, and the entity's process to monitor the system of internal control include a combination of inquiry, observation, and inspection, as required by paragraph 14. Inquiry alone is not sufficient to obtain an understanding of or to evaluate each of these components as required by this proposed SAS.

A101. For the information system and communication, and control activities components of the entity's system of internal control, controls are primarily more direct in addressing assertion-level risks (see paragraphs A5 and A136). Accordingly, this proposed SAS requires performing risk assessment procedures, beyond inquiry, to evaluate whether the controls identified in accordance with paragraph 26 are effectively designed and determine whether those controls have been implemented (see paragraph 26*d)*. An audit does not require an understanding of all the control activities related to each significant class of transactions, account balance, and disclosure in the financial statements or to every assertion relevant to them. The auditor may identify, in accordance with paragraph 26, direct controls within the other components of the entity's system of internal control for which the auditor evaluates design and determines implementation (see paragraphs A108 and A165).

A102. The components of the entity's system of internal control for the purpose of this proposed SAS may not necessarily reflect how an entity designs, implements, and maintains its system of internal control, or how it may classify any particular component. Entities may use different terminology or frameworks to describe the various aspects of the system of internal control. For the purpose of an audit, auditors may also use different terminology or frameworks, provided all the components described in this proposed SAS are addressed.

Scalability

A103. The way in which the entity's system of internal control is designed, implemented, and maintained varies with an entity's size and complexity. For example, less complex entities may use less structured or simpler controls (that is, policies and procedures) to achieve their objectives.

Considerations Specific to Governmental Entities

A104. Auditors of governmental entities often have additional responsibilities with respect to internal control, for example, to report on compliance with an established code of practice or reporting on spending against budget. Auditors of governmental entities may also have responsibilities to report on compliance with law, regulation, or other authority. As a result, their considerations about the system of internal control may be broader and more detailed.

IT in the Components of the Entity's System of Internal Control

A105. Appendix E provides further guidance on understanding the entity's use of IT in the components of the system of internal control.

A106. The requirements of the auditor to obtain sufficient appropriate audit evidence in an audit does not differ whether an entity operates in a mainly manual environment, a completely automated environment, or an environment involving some combination of manual and automated

elements (that is, manual and automated controls and other resources, including service organizations, used in the entity's system of internal control).

Understanding the Nature of the Components of the Entity's System of Internal Control

A107. The auditor's understanding of each of the components of the entity's system of internal control provides a preliminary understanding of how the entity identifies business risks relevant to financial reporting and how it responds to them. It may also influence the auditor's identification and assessment of the risks of material misstatement in different ways (see paragraph A94). The auditor's identification and assessment of the risks of material misstatement assists the auditor in designing and performing further audit procedures, including any plans to test the operating effectiveness of controls. Examples follow:

- The auditor's understanding of the entity's control environment, the entity's risk assessment process, and the entity's process to monitor controls components is more likely to affect the identification and assessment of risks of material misstatement at the financial statement level.
- The auditor's understanding of the entity's information system and communication, and the entity's control activities component, is more likely to affect the identification and assessment of risks of material misstatement at the assertion level.

Control Environment, the Entity's Risk Assessment Process, and the Entity's Process to Monitor the System of Internal Control (Ref: par. 21–24)

A108. The controls in the control environment, the entity's risk assessment process, and the entity's process to monitor the system of internal control are primarily indirect controls (see paragraph A5). However, controls within these components may vary in nature and precision and, therefore, some controls within these components may also be direct controls that address risks of material misstatement at the assertion level (see paragraph A165).

Why the Auditor Is Required to Understand the Control Environment, The Entity's Risk Assessment Process, and the Entity's Process to Monitor the System of Internal Control

A109. The control environment provides an overall foundation for the operation of the other components of the system of internal control. The control environment does not directly prevent, or detect and correct, misstatements. It may, however, influence the effectiveness of controls in the other components of the system of internal control. Similarly, the entity's risk assessment process and its process for monitoring the system of internal control are designed to operate in a manner that also supports the entire system of internal control.

A110. Because these components are foundational to the entity's system of internal control, deficiencies in their operation could have pervasive effects on the preparation of the financial statements. Therefore, the auditor's understanding and evaluations of these components affect the auditor's identification and assessment of risks of material misstatement at the financial statement level and may also affect the identification and assessment of risks of material misstatement at the assertion level (see paragraphs A114, A123, and A134). Risks of material misstatement at the financial statement level affect the auditor's design of overall responses, including, as explained

in AU-C section 330, an influence on the nature, timing, and extent of the auditor's further procedures.[31]

Obtaining an Understanding of the Control Environment (Ref: par. 21)

Scalability

A111. The nature of the control environment in a less complex entity is likely to be different from the control environment in a more complex entity. For example, those charged with governance in less complex entities may not include an independent or outside member, and the role of governance may be undertaken directly by the owner-manager when there are no other owners. Accordingly, some considerations about the entity's control environment may be less relevant or may not be applicable.

A112. In addition, audit evidence about elements of the control environment in less complex entities may not be available in documentary form, in particular, where communication between management and other personnel is informal, but the evidence may still be appropriately relevant and reliable in the circumstances. Examples are as follows:

- The organizational structure in a less complex entity will likely be simpler and may include a small number of employees involved in roles related to financial reporting.
- If the role of governance is undertaken directly by the owner-manager, the auditor may determine that the independence of those charged with governance is not relevant.
- Less complex 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. Consequently, the attitudes, awareness, and actions of management or the owner-manager are of particular importance to the auditor's understanding of a less complex entity's control environment.

*Understanding the Control Environment (Ref: par. 21*a*)*

A113. In considering the extent to which management demonstrates a commitment to integrity and ethical values, the auditor may obtain an understanding through inquiries of management and employees and through considering information from external sources about

- how management communicates to employees its views on business practices and ethical behavior, and
- inspecting management's written code of conduct and observing whether management acts in a manner that supports that code.

*Evaluating the Control Environment (Ref: par. 21*b*)*

[31] Paragraphs .A1–.A3 of AU-C section 330.

Why the Auditor Evaluates the Control Environment

A114. The auditor's evaluation of how the entity demonstrates behavior consistent with the entity's commitment to integrity and ethical values; whether the control environment provides an appropriate foundation for the other components of the entity's system of internal control; and whether any identified control deficiencies undermine the other components of the system of internal control, assists the auditor in identifying potential issues in the other components of the system of internal control as well as the controls the auditor might identify in accordance with paragraph 26. This is because the control environment is foundational to the other components of the entity's system of internal control. This evaluation may also assist the auditor in understanding risks faced by the entity and, therefore, in identifying and assessing the risks of material misstatement at the financial statement and assertion levels (see paragraph A107).

The Auditor's Evaluation of the Control Environment

A115. The auditor's evaluation of the control environment is based on the understanding obtained in accordance with paragraph 21*a*.

A116. Some entities may be dominated by a single individual who may exercise a great deal of discretion. The actions and attitudes of that individual may have a pervasive effect on the culture of the entity, which in turn, may have a pervasive effect on the control environment. Such an effect may be positive or negative. For example, direct involvement by a single individual may be key to enabling the entity to meet its growth and other objectives and can also contribute significantly to an effective system of internal control. On the other hand, such concentration of knowledge and authority can also lead to an increased susceptibility to misstatement through management override of controls.

A117. The auditor may consider how the different elements of the control environment may be influenced by the philosophy and operating style of senior management, taking into account the involvement of independent members of those charged with governance.

A118. Although the control environment may provide an appropriate foundation for the system of internal control and may help reduce the risk of fraud, an appropriate control environment is not necessarily an effective deterrent to fraud. For example, human resource policies and procedures directed toward hiring competent financial, accounting, and IT personnel may mitigate the risk of errors in processing and recording financial information. However, such policies and procedures may not mitigate the override of controls by senior management (for example, to overstate earnings).

A119. The auditor's evaluation of the control environment as it relates to the entity's use of IT may include such matters as the following:

- Whether governance over IT is commensurate with the nature and complexity of the entity and its business operations enabled by IT, including the complexity or maturity of the entity's technology platform or architecture and the extent to which the entity relies on IT applications to support its financial reporting

- The management organizational structure regarding IT and the resources allocated (for example, whether the entity has invested in an appropriate IT environment and necessary enhancements or whether a sufficient number of appropriately skilled individuals have been employed, including when the entity uses commercial software [with no or limited modifications])

Obtaining an Understanding of the Entity's Risk Assessment Process (Ref: par. 22–23)

Understanding the Entity's Risk Assessment Process (Ref: par. 22*a*)

A120. As explained in paragraph A69, not all business risks give rise to risks of material misstatement, whether due to error or fraud. In understanding how management and those charged with governance have identified business risks relevant to the preparation of the financial statements, and decided about actions to address those risks, matters the auditor may consider include how management or, as appropriate, those charged with governance, has done the following:

- Specified the entity's objectives with sufficient precision and clarity to enable the identification and assessment of the risks relating to the objectives
- Identified the risks to achieving the entity's objectives and analyzed the risks as a basis for determining how the risks should be managed
- Considered the potential for fraud when considering the risks to achieving the entity's objectives[32]

A121. Paragraph 22 of this proposed SAS requires the auditor to obtain an understanding of the entity's process for identifying business risks. AU-C section 240[33] requires the auditor to make inquiries of management regarding, among other things, management's process for identifying, responding to, and monitoring the risks of fraud in the entity, including any specific risks of fraud that management has identified or that have been brought to its attention, or classes of transactions, account balances, or disclosures for which a risk of fraud is likely to exist.

A122. The auditor may consider the implications of such business risks for the preparation of the entity's financial statements and other aspects of its system of internal control.

Evaluating the Entity's Risk Assessment Process (Ref: par. 22*b*)

Why the Auditor Evaluates Whether the Entity's Risk Assessment Process Is Appropriate

A123. The auditor's evaluation of the entity's risk assessment process may assist the auditor in understanding where the entity has identified risks that may occur and how the entity has responded to those risks. The auditor's evaluation of how the entity identifies its business risks and how it assesses and addresses those risks assists the auditor in understanding whether the risks faced by the entity have been identified, assessed, and addressed, as appropriate, to the nature and

---

[32] Paragraph .18 of AU-C section 240.

[33] Paragraph .17 of AU-C section 240.

complexity of the entity. This evaluation may also assist the auditor with identifying and assessing financial-statement-level and assertion-level risks of material misstatement (see paragraph A107).

Evaluating Whether the Entity's Risk Assessment Process Is Appropriate (Ref: par. 22*b*)

A124. The auditor's evaluation of the appropriateness of the entity's risk assessment process is based on the understanding obtained in accordance with paragraph 22*a*.

Scalability

A125. Whether the entity's risk assessment process is appropriate to the entity's circumstances, considering the nature and complexity of the entity, is a matter of the auditor's professional judgment. For example, in some less complex entities, and particularly owner-managed entities, an appropriate risk assessment may be performed through the direct involvement of management or the owner-manager (for example, the manager or owner-manager may routinely devote time to monitoring the activities of competitors and other developments in the market place to identify emerging business risks). The evidence of this risk assessment occurring in these types of entities is often not formally documented, but it may be evident from, for example, discussions the auditor has with management, corroborated by e-mails or other correspondence between management and other personnel, that management is, in fact, performing risk assessment procedures.

Obtaining an Understanding of the Entity's Process to Monitor the Entity's System of Internal Control (Ref: par. 24)

Scalability

A126. In less complex entities, and in particular, owner-manager entities, the auditor's understanding of the entity's process to monitor the system of internal control is often focused on how management or the owner-manager is directly involved in operations because there may not be any other monitoring activities. For example, management may receive complaints from customers about inaccuracies in their monthly statement that alerts the owner-manager to issues with the timing of when customer payments are being recognized in the accounting records.

A127. For entities in which there is no formal process for monitoring the system of internal control, understanding the process to monitor the system of internal control may include understanding periodic reviews of management accounting information that are designed to contribute to how the entity prevents or detects misstatements.

Understanding the Entity's Process to Monitor the System of Internal Control (Ref: par. 24*a*(i))

A128. Matters that may be relevant for the auditor to consider when understanding how the entity monitors its system of internal control include the following:

- The design of the monitoring activities, for example, whether it is periodic or ongoing monitoring
- The performance and frequency of the monitoring activities

- The evaluation of the results of the monitoring activities, on a timely basis, to determine whether the controls have been effective
- How identified deficiencies have been addressed through appropriate remedial actions, including timely communication of such deficiencies to those responsible for taking remedial action

A129. The auditor may also consider how the entity's process to monitor the system of internal control addresses monitoring information-processing controls that involve the use of IT. This may include, for example

- controls to monitor complex IT environments that
  - — evaluate the continuing design effectiveness of information-processing controls and modify them, as appropriate, for changes in conditions or
  - — evaluate the operating effectiveness of information-processing controls.
- controls that monitor the permissions applied in automated information-processing controls that enforce the segregation of duties.
- controls that monitor how errors or control deficiencies related to the automation of financial reporting are identified and addressed.

Understanding the Entity's Internal Audit Function (Ref: par. 24*a*(ii))

A130. Appendix D sets out further considerations for understanding the entity's internal audit function.

A131. The auditor's inquiries of appropriate individuals within the internal audit function help the auditor obtain an understanding of the nature of the internal audit function's responsibilities. If the auditor determines that the function's responsibilities are related to the entity's financial reporting, the auditor may obtain further understanding of the activities performed, or to be performed, by the internal audit function by reviewing the internal audit function's audit plan for the period, if any, and discussing that plan with the appropriate individuals within the function. This understanding, together with the information obtained from the auditor's inquiries, may also provide information that is directly relevant to the auditor's identification and assessment of the risks of material misstatement. If, based on the auditor's preliminary understanding of the internal audit function, the auditor expects to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed, AU-C section 610, *Using the Work of Internal Auditors*, applies.

Other Sources of Information Used in the Entity's Process to Monitor the System of Internal Control

Understanding the Sources of Information (Ref: par. 24*b*)

A132. Management's monitoring activities may use information in communications from external parties, such as customer complaints or regulator comments, that may indicate problems or highlight areas in need of improvement.

Why the Auditor Is Required to Understand the Sources of Information Used for the Entity's Monitoring of the System of Internal Control

A133. The auditor's understanding of the sources of information used by the entity in monitoring the entity's system of internal control, including whether the information used is relevant and reliable, assists the auditor in evaluating whether the entity's process to monitor the entity's system of internal control is appropriate. If management assumes that information used for monitoring is relevant and reliable without having a basis for that assumption, errors that may exist in the information could potentially lead management to draw incorrect conclusions from its monitoring activities.

Evaluating The Entity's Process to Monitor The System of Internal Control

Why the Auditor Evaluates Whether the Entity's Process to Monitor the System of Internal Control Is Appropriate (Ref: par. 24*c*)

A134. The auditor's evaluation about how the entity undertakes ongoing and separate evaluations for monitoring the effectiveness of controls assists the auditor in understanding whether the other components of the entity's system of internal control are present and functioning and, therefore, assists with understanding the other components of the entity's system of internal control. This evaluation may also assist the auditor with identifying and assessing financial-statement-level and assertion-level risks of material misstatement (see paragraph A107) and with designing tests of controls.[34]

Evaluating Whether the Entity's Process to Monitor the System of Internal Control Is Appropriate (Ref: par. 24*c*)

A135. The auditor's evaluation of the appropriateness of the entity's process to monitor the system of internal control is based on the auditor's understanding of the entity's process to monitor the system of internal control.

Information System and Communication, and Control Activities (Ref: par. 25–26)

A136. The controls in the information system and communication, and control activities components are primarily direct controls (that is, controls that are sufficiently precise to prevent, detect, or correct misstatements at the assertion level).

Why the Auditor Is Required to Understand the Information System and Communication and Controls in the Control Activities Component

A137. The auditor is required to understand the entity's information system and communication because understanding the entity's policies that define the flows of transactions and other aspects

[34] Paragraph .08 of section 330.

of the entity's information-processing activities relevant to the preparation of the financial statements, and evaluating whether the component appropriately supports the preparation of the entity's financial statements, supports the auditor's identification and assessment of risks of material misstatement at the assertion level. This understanding and evaluation may also result in the identification of risks of material misstatement at the financial statement level when the results of the auditor's procedures are inconsistent with expectations about the entity's system of internal control that may have been set based on information obtained during the engagement acceptance or continuance process (see paragraph A107).

A138. The auditor is required to identify specific controls in the control activities component, and evaluate the design and determine whether the controls have been implemented, because it assists the auditor's understanding about management's approach to addressing certain risks; therefore, it provides a basis for the design and performance of further audit procedures responsive to these risks as required by AU-C section 330. The higher on the spectrum of inherent risk a risk is assessed, the more persuasive the audit evidence needs to be. Even when the auditor does not plan to test the operating effectiveness of identified controls, the auditor's understanding may still affect the design of the nature, timing, and extent of substantive procedures that are responsive to the related risks of material misstatement.

The Iterative Nature of the Auditor's Understanding and Evaluation of the Information System and Communication, and Control Activities

A139. As explained in paragraph A55, the auditor's understanding of the entity and its environment, and the applicable financial reporting framework, may assist the auditor in developing initial expectations about the classes of transactions, account balances, and disclosures that may be significant classes of transactions, account balances, and disclosures. In obtaining an understanding of the information system and communication component in accordance with paragraph 25*a*, the auditor may use these initial expectations for the purpose of determining the extent of understanding of the entity's information-processing activities to be obtained.

A140. The auditor's understanding of the information system includes understanding the policies that define flows of information relating to the entity's significant classes of transactions, account balances, and disclosures, and other related aspects of the entity's information-processing activities. This information and the information obtained from the auditor's evaluation of the information system may confirm or further influence the auditor's expectations about the significant classes of transactions, account balances, and disclosures initially identified (see paragraph A140).

A141. In obtaining an understanding of how information relating to significant classes of transactions, account balances, and disclosures flows into, through, and out of the entity's information system, the auditor may also identify controls in the control activities component that are required to be identified in accordance with paragraph 26*a*. For example, the auditor's identification and evaluation of controls in the control activities component may first focus on controls over journal entries and controls that the auditor plans to test the operating effectiveness of in designing the nature, timing, and extent of substantive procedures.

A142. The auditor's assessment of inherent risk may also influence the identification of controls in the control activities component. For example, controls that address significant risks may be identifiable only when the auditor has assessed inherent risk at the assertion level in accordance with paragraph 31. Furthermore, controls addressing risks for which the auditor has determined that substantive procedures alone do not provide sufficient appropriate audit evidence (in accordance with paragraph 33) may also be identifiable only once the auditor's inherent risk assessments have been undertaken.

A143. The auditor's identification and assessment of risks of material misstatement at the assertion level is influenced by both of the following:

- The auditor's understanding of the entity's policies for its information-processing activities in the information system and communication component
- The auditor's identification and evaluation of controls in the control activities component

Obtaining an Understanding of the Information System and Communication (Ref: par. 25)

A144. Appendix C[35] sets out further considerations relating to the information system and communication.

Scalability

A145. The information system, and related business processes, in less complex entities are likely to be less sophisticated than in larger entities and are likely to involve a less complex IT environment; however, the role of the information system is just as important. Less complex entities with direct management involvement may not need extensive descriptions of accounting procedures, sophisticated accounting records, or written policies. Understanding the relevant aspects of the entity's information system may, therefore, require less effort in an audit of a less complex entity and may involve a greater amount of inquiry than observation or inspection of documentation. The need to obtain an understanding, however, remains important to provide a basis for the design of further audit procedures in accordance with AU-C section 330 and may further assist the auditor in identifying or assessing risks of material misstatement (see paragraph A107).

Obtaining an Understanding of the Information System (Ref: par. 25*a*)

A146. Included within the entity's system of internal control are aspects that relate to the entity's reporting objectives, including its financial reporting objectives, but may also include aspects that relate to its operations or compliance objectives, when such aspects are relevant to financial reporting. Understanding how the entity initiates transactions and captures information as part of the auditor's understanding of the information system may include information about the entity's systems (its policies) designed to address compliance and operations objectives because such information is relevant to the preparation of the financial statements. Further, some entities may have information systems that are highly integrated such that controls may be designed in a manner

[35] Paragraphs 11–15 of appendix C, "Understanding the Entity's System of Internal Control."

to simultaneously achieve financial reporting, compliance and operational objectives, and combinations thereof.

A147. The auditor's understanding of the entity's information system and communication required under paragraph 25*a* results in obtaining an understanding of the process of reconciling detailed records to the general ledger.

A148. Understanding the entity's information system also includes an understanding of the resources to be used in the entity's information-processing activities. Information about the human resources involved that may be relevant to understanding risks to the integrity of the information system include the following:

- The competence of the individuals undertaking the work
- Whether there are adequate resources
- Whether there is appropriate segregation of duties

A149. Matters the auditor may consider when understanding the policies that define the flows of information relating to the entity's significant classes of transactions, account balances, and disclosures in the information system and communication component include the nature of

a. the data or information relating to transactions, other events, and conditions to be processed;

b. the information processing to maintain the integrity of that data or information; and

c. the information processes, personnel, and other resources used in processing information.

A150. Obtaining an understanding of the entity's business processes, which include how transactions are originated, assists the auditor in obtaining an understanding of the entity's information system in a manner that is appropriate to the entity's circumstances.

A151. The auditor's understanding of the information system may be obtained in various ways and may include some or all of the following:

- Inquiries of relevant personnel about the procedures used to initiate, record, process, and report transactions or about the entity's financial reporting process
- Inspection of policy or process manuals or other documentation of the entity's information system
- Observation of the performance of the policies or procedures by entity's personnel
- Selecting transactions and tracing them through the applicable process in the information system (that is, performing a walk-through)

Automated Tools and Techniques

A152. The auditor may also use automated techniques to obtain direct access to, or a digital download from, the databases in the entity's information system that store accounting records of transactions. By applying automated tools or techniques to this information, the auditor may confirm the understanding obtained about how transactions flow through the information system by tracing journal entries, or other digital records related to a particular transaction, or an entire population of transactions from initiation in the accounting records through to recording in the general ledger. Analysis of complete or large sets of transactions may also result in the identification of variations from the normal, or expected, processing procedures for these transactions, which may result in the identification of risks of material misstatement.

Information Obtained From Outside of the General and Subsidiary Ledgers

A153. Financial statements may contain information that is obtained from outside of the general and subsidiary ledgers. Examples of such information that the auditor may consider are as follows:

- Information obtained from lease agreements relevant to disclosures in the financial statements
- Information disclosed in the financial statements that is produced by an entity's risk management system
- Fair value information produced by management's specialists and disclosed in the financial statements
- Information disclosed in the financial statements that has been obtained from models or from other calculations used to develop accounting estimates recognized or disclosed in the financial statements, including information relating to the underlying data and assumptions used in those models, such as
  - assumptions developed internally that may affect an asset's useful life, or
  - data such as interest rates that are affected by factors outside the control of the entity
- Information disclosed in the financial statements about sensitivity analyses derived from financial models that demonstrates that management has considered alternative assumptions
- Information recognized or disclosed in the financial statements that has been obtained from an entity's tax returns and records
- Information disclosed in the financial statements that has been obtained from analyses prepared to support management's assessment of the entity's ability to continue as a going concern, such as disclosures, if any, related to events or conditions that have been identified that may cast significant doubt on the entity's ability to continue as a going concern[36]

[36] Paragraphs .21–.22 of AU-C section 570, *The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern*.

A154. Certain amounts or disclosures in the entity's financial statements (such as disclosures about credit risk, liquidity risk, and market risk) may be based on information obtained from the entity's risk management system. However, the auditor is not required to understand all aspects of the risk management system and uses professional judgment in determining the necessary understanding.

The Entity's Use of IT in the Information System

Why Does the Auditor Understand the IT Environment Relevant to the Information System

A155. The auditor's understanding of the information system includes the IT environment relevant to the flows of transactions and processing of information in the entity's information system because the entity's use of IT applications or other aspects in the IT environment may give rise to risks arising from the use of IT.

A156. The understanding of the entity's business model and how it integrates the use of IT may also provide useful context to the nature and extent of IT expected in the information system.

Understanding the Entity's Use of IT

A157. The auditor's understanding of the IT environment may focus on identifying, and understanding the nature and number of, the specific IT applications and other aspects of the IT environment that are relevant to the flows of transactions and processing of information in the information system. Changes in the flow of transactions, or information within the information system, may result from program changes to IT applications or direct changes to data in databases involved in processing or storing those transactions or information.

A158. The auditor may identify the IT applications and supporting IT infrastructure concurrently with the auditor's understanding of how information relating to significant classes of transactions, account balances, and disclosures flow into, through, and out of the entity's information system.

Obtaining an Understanding of the Entity's Communication (Ref: par. 25*b*)

Scalability

A159. In larger, more complex entities, information the auditor may consider when understanding the entity's communication may come from policy manuals and financial reporting manuals.

A160. In less complex entities, communication may be less structured (for example, formal manuals may not be used) due to fewer levels of responsibility and management's greater visibility and availability. Regardless of the size of the entity, open communication channels facilitate the reporting of exceptions and acting on them.

Evaluating Whether the Relevant Aspects of the Information System Support the Preparation of the Entity's Financial Statements (Ref: par. 25*c*)

A161. The auditor's evaluation of whether the entity's information system and communication appropriately supports the preparation of the financial statements is based on the understanding obtained in paragraph 25*a–b*.

Control Activities (Ref: par. 26)

Controls in the Control Activities Component (Ref: par. 26)

A162. Appendix C[37] sets out further considerations relating to control activities.

A163. The control activities component includes controls that are designed to ensure the proper application of policies (which are also controls) in all the other components of the entity's system of internal control and includes both direct and indirect controls. For example, the controls that an entity has established to ensure that its personnel are properly counting and recording the annual physical inventory relate directly to the risks of material misstatement relevant to the existence and completeness assertions for the inventory account balance.

A164. The auditor's identification and evaluation of controls in the control activities component is focused on information-processing controls, which are controls applied during the processing of information in the entity's information system that directly address the risks of material misstatement. This may include risks arising from IT such as risk relating to the integrity of information (that is, the completeness, accuracy, and validity of transactions and other information). However, the auditor is not required to identify and evaluate all information-processing controls related to the entity's policies that define the flows of transactions and other aspects of the entity's information-processing activities for the significant classes of transactions, account balances, and disclosures.

A165. Direct controls may exist in the control environment, the entity's risk assessment process, or the entity's process to monitor the system of internal control, which may be identified in accordance with paragraph 26. An example is a management review control designed to detect misstatements by using key performance indicators or other types of information to develop sufficiently precise expectations of reported amounts. The more indirect the relationship between controls that support other controls and the control that is being considered, the less effective that control may be in preventing, or detecting and correcting, related misstatements. For example, a sales manager's review of a summary of sales activity for specific stores by region ordinarily is indirectly related only to the risks of material misstatement relevant to the completeness assertion for sales revenue. Accordingly, it may be less effective in addressing those risks than controls more directly related thereto, such as matching shipping documents with billing documents.

A166. Paragraph 26 also requires the auditor to identify and evaluate general IT controls for IT applications and other aspects of the IT environment that the auditor has determined to be subject to risks arising from the use of IT because general IT controls support the continued effective functioning of information-processing controls. A general IT control alone is typically not sufficient to address a risk of material misstatement at the assertion level.

---

[37] Paragraphs 15–16 of appendix C.

A167. The controls that the auditor is required to identify and evaluate the design, and determine the implementation of, in accordance with paragraph 26 are as follows:

- Controls that the auditor plans to test the operating effectiveness of in determining the nature, timing, and extent of substantive procedures. The evaluation of such controls provides the basis for the auditor's design of test of control procedures in accordance with AU-C section 330. These controls also include controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.
- Controls that address significant risks and controls over journal entries. The auditor's identification and evaluation of such controls may also influence the auditor's identification and assessment of the risks of material misstatement, including the identification of additional risks of material misstatement (see paragraph A107). This understanding also provides the basis for the auditor's design of the nature, timing, and extent of substantive procedures that are responsive to the related assessed risks of material misstatement.
- Other controls that the auditor considers appropriate to enable the auditor to meet the objectives of paragraph 13 with respect to risks at the assertion level, based on the auditor's professional judgment.

A168. Controls in the control activities component are required to be identified when such controls meet one or more of the criteria included in paragraph 26*a*. However, when multiple controls each achieve the same objective, it is unnecessary to identify each of the controls related to such objective.

Types of Controls in the Control Activities Component (Ref: par. 26)

A169. Examples of controls in the control activities component include authorizations and approvals, reconciliations, verifications (such as edit and validation checks or automated calculations), segregation of duties, and physical or logical controls, including those addressing safeguarding of assets.

A170. Controls in the control activities component may also include controls established by management that address risks of material misstatement related to disclosures not being prepared in accordance with the applicable financial reporting framework. Such controls may relate to information included in the financial statements that is obtained from outside of the general and subsidiary ledgers.

A171. Regardless of whether controls are within the IT environment or manual systems, controls may have various objectives and may be applied at various organizational and functional levels.

Scalability (Ref: par. 26)

A172. Controls in the control activities component for less complex entities are likely to be similar to those in larger entities, but the formality with which they operate may vary. Further, in less complex entities, more controls may be directly applied by management. For example,

management's sole authority for granting credit to customers and approving significant purchases can provide strong control over important account balances and transactions.

A173. It may be less practicable to establish segregation of duties in less complex entities that have fewer employees. However, in an owner-managed entity, the owner-manager may be able to exercise more effective oversight through direct involvement than in a larger entity, which may compensate for the generally more limited opportunities for segregation of duties. Although, as also explained in AU-C section 240, domination of management by a single individual can be a potential control deficiency because there is an opportunity for management override of controls.[38]

*Controls That Address Risks of Material Misstatement at the Assertion Level (Ref: par. 26*a*)*

Controls That Address Risks That Are Determined to Be a Significant Risk (Ref: par. 26*a*(i))

A174. Regardless of whether the auditor plans to test the operating effectiveness of controls that address significant risks, the understanding obtained about management's approach to addressing those risks may provide a basis for the design and performance of substantive procedures responsive to significant risks as required by AU-C section 330.[39] Although risks relating to significant nonroutine or judgmental matters are often less likely to be subject to routine controls, management may have other responses intended to deal with such risks. For example, when there are nonroutine events, such as a significant business acquisition, consideration of the entity's response may include such matters as whether it has been referred to appropriate specialists (such as internal or external valuation specialists), whether an assessment has been made of the potential effect, and how it is proposed that the circumstances are to be disclosed in the financial statements. The auditor's understanding of whether the entity has designed and implemented controls for significant risks arising from nonroutine or judgmental matters may include whether and how management responds to the risks. Such responses may include the following:

- Controls, such as a review of assumptions by senior management or specialists
- Documented processes for accounting estimations
- Approval by those charged with governance

A175. AU-C section 240[40] requires the auditor to understand controls related to assessed risks of material misstatement due to fraud (which are treated as significant risks) and further explains that it is important for the auditor to obtain an understanding of the controls that management has designed, implemented, and maintained to prevent and detect fraud.

Controls Over Journal Entries (Ref: par. 26*a*(ii))

A176. Controls that address risks of material misstatement at the assertion level that are expected to be identified for all audits are controls over journal entries because the manner in which an

---

38 Paragraph .A33 of AU-C section 240.

39 Paragraph .22 of AU-C section 330.

40 Paragraphs .27 and .A37 of AU-C section 240.

entity incorporates information from transaction processing into the general ledger ordinarily involves the use of journal entries, whether standard or nonstandard, or automated or manual. Paragraph 25*a* requires the auditor to obtain an understanding of the flows of information in the entity's information system for significant classes of transactions, account balances, and disclosures. The understanding required by paragraph 26*a*(ii) includes controls over adjustments to significant classes of transactions, account balances, and disclosures that may not be subject to controls over processing of routine transactions. Further, the auditor may have identified no related party transactions that meet the definition of *significant unusual transactions* in accordance with AU-C section 240,[41] other significant risks, or other risks of material misstatement for which it is necessary for the auditor to evaluate the design of controls and determine that they have been implemented. In such an audit, the auditor may determine that there are no identified controls other than the entity's controls over journal entries.

Automated Tools and Techniques

A177. In manual general ledger systems, nonstandard journal entries may be identified through inspection of ledgers, journals, and supporting documentation. When automated procedures are used to maintain the general ledger and prepare financial statements, such entries may exist only in electronic form and, therefore, may be more easily identified through the use of automated techniques. For example, in the audit of a less complex entity, the auditor may be able to extract a total listing of all journal entries into a simple spreadsheet. It may then be possible for the auditor to sort the journal entries by applying a variety of filters such as currency amount, name of the preparer or reviewer, journal entries that gross up the balance sheet and income statement only, or to view the listing by the date the journal entry was posted to the general ledger, to assist the auditor in designing responses to the risks identified relating to journal entries.

Controls for Which the Auditor Plans to Test the Operating Effectiveness (Ref: par. 26*a*(iii))

A178. The auditor determines whether there are any risks of material misstatement at the assertion level for which it is not possible to obtain sufficient appropriate audit evidence through substantive procedures alone. The auditor is required, in accordance with AU-C section 330,[42] to design and perform tests of controls that address such risks of material misstatement when substantive procedures alone do not provide sufficient appropriate audit evidence at the assertion level. As a result, when such controls exist that address these risks, they are required to be identified and evaluated.

A179. In other cases, when the auditor plans to take into account the operating effectiveness of controls in determining the nature, timing, and extent of substantive procedures in accordance with AU-C section 330, such controls are also required to be identified because AU-C section 330[43] requires the auditor to design and perform tests of those controls. For example, the auditor may plan to test the operating effectiveness of controls

---

41 Paragraph .11 of AU-C section 240.

42 Paragraph .08*b* of AU-C section 330.

43 Paragraph .08*a* of AU-C section 330.

- over routine classes of transactions because such testing may be more effective or efficient for large volumes of homogenous transactions.
- over the completeness and accuracy of information produced by the entity (for example, controls over the preparation of system-generated reports) to determine the reliability of that information, when the auditor intends to take into account the operating effectiveness of those controls in designing and performing further audit procedures.
- relating to operations and compliance objectives when they relate to data the auditor evaluates or uses in applying audit procedures.

A180. The auditor's decision whether to test the operating effectiveness of controls may also be influenced by the identified risks of material misstatement at the financial statement level. For example, if deficiencies are identified related to the control environment, this may affect the auditor's overall expectations about the operating effectiveness of direct controls.

Other Controls That the Auditor Considers Appropriate (Ref: par. 26*a*(iv))

A181. Other controls that the auditor may consider appropriate to identify and evaluate the design and determine the implementation of may include some or all of the following:

- Controls that address risks assessed as higher on the spectrum of inherent risk but have not been determined to be a significant risk
- Controls related to reconciling detailed records to the general ledger
- Controls related to accounting estimates
- Complementary user entity controls, if using a service organization[44]

Identifying IT Applications and Other Aspects of the IT Environment, Risks Arising From the Use of IT, and General IT Controls (Ref: par. 26*b*–*c*)

A182. Appendix E includes example characteristics of IT applications and other aspects of the IT environment, and guidance related to those characteristics, that may be relevant in identifying IT applications and other aspects of the IT environment subject to risks arising from the use of IT.

Identifying IT Applications and Other Aspects of the IT Environment (Ref: par. 26*b*)

Why the Auditor Identifies Risks Arising From the Use of IT and General IT Controls Related to Identified IT Applications and Other Aspects of the IT Environment

A183. For controls listed in paragraph 26*a*, paragraph 26*b* requires the auditor to identify related IT applications and other aspects of the IT environment that are subject to the risks described in paragraph 26*c*(i). Paragraph 26*b*(ii) then requires the auditor to identify general IT controls that address such risks. Such identification is necessary in order for the auditor to effectively perform the evaluation of design and determination of implementation of identified controls in accordance

[44] AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization*.

with paragraph 26*d* because general IT controls that address these risks may affect the design and implementation of the controls listed in paragraph 26*a*.

A184. Understanding the risks arising from the use of IT and the general IT controls implemented by the entity to address those risks may affect some or all of the following:

- The auditor's decision about whether to test the operating effectiveness of controls to address risks of material misstatement at the assertion level. For example, when general IT controls are not designed effectively or appropriately implemented to address risks arising from the use of IT (for example, controls do not appropriately prevent or detect unauthorized program changes or unauthorized access to IT applications), this may affect the auditor's decision to rely on automated controls within the affected IT applications.
- The auditor's assessment of control risk at the assertion level. For example, the ongoing operating effectiveness of an information-processing control may depend on certain general IT controls that prevent or detect unauthorized program changes to the IT information-processing control (that is, program change controls over the related IT application). In such circumstances, the expected operating effectiveness (or lack thereof) of the general IT control may affect the auditor's assessment of control risk (for example, control risk may be higher when such general IT controls are expected to be ineffective or if the auditor does not plan to test the general IT controls).
- The auditor's strategy for testing information produced by the entity that is produced by or involves information from the entity's IT applications. For example, when information produced by the entity to be used as audit evidence is produced by IT applications, the auditor may determine to test controls over system-generated reports, including identification and testing of the general IT controls that address risks of inappropriate or unauthorized program changes or the integrity of the data that appears in the reports.
- The auditor's assessment of inherent risk at the assertion level. For example, when there are significant or extensive programming changes to an IT application to address new or revised reporting requirements of the applicable financial reporting framework, this may be indicative of the complexity of the new requirements and their effect on the entity's financial statements. When such extensive programming or data changes occur, the IT application is also likely to be subject to risks arising from the use of IT.
- The design of further audit procedures. For example, if information-processing controls depend on general IT controls, the auditor may determine to test the operating effectiveness of the general IT controls, which will then require the design of tests of controls for such general IT controls. If, in the same circumstances, the auditor determines not to test the operating effectiveness of the general IT controls, or the general IT controls are expected to be ineffective, the related risks arising from the use of IT may need to be addressed through the design of substantive procedures. However, the risks arising from the use of IT may not be able to be addressed when such risks relate to risks for which substantive procedures alone do not provide sufficient

appropriate audit evidence. In such circumstances, the auditor may need to consider the implications for the audit opinion.

Identifying IT Applications That Are Subject to Risks Arising From the Use of IT

A185. For the IT applications relevant to the information system, understanding the nature and complexity of the specific IT processes and general IT controls that the entity has in place may assist the auditor in determining which IT applications the entity is relying upon to accurately process and maintain the integrity of information in the entity's information system. Such IT applications may be subject to risks arising from the use of IT.

A186. Identifying the IT applications that are subject to risks arising from the use of IT involves taking into account controls identified by the auditor because such controls may involve the use of IT or rely on IT. The auditor may focus on whether an IT application includes automated controls that management is relying on and that the auditor has identified, including controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. The auditor may also consider how information is stored and processed in the information system relating to significant classes of transactions, account balances, and disclosures and whether management is relying on general IT controls to maintain the integrity of that information.

A187. The controls identified by the auditor may depend on system-generated reports, in which case, the IT applications that produce those reports may be subject to risks arising from the use of IT. In other cases, the auditor may plan not to rely on controls over the system-generated reports and plan to directly test the inputs and outputs of the report generation process, in which case, the auditor may identify the related IT applications as not being subject to risks arising from IT and, thus, these controls may not be subject to the requirements in paragraphs 26*c*–*d*.

Scalability

A188. The extent of the auditor's understanding of the IT processes, including the extent to which the entity has general IT controls in place, will vary with the nature and circumstances of the entity and its IT environment and will also be based on the nature and extent of controls identified by the auditor. The number of IT applications that are subject to risks arising from the use of IT also will vary based on these factors. Examples are as follows:

- An entity that uses commercial software and does not have access to the source code to make any program changes is unlikely to have a process for program changes but may have a process or procedures to configure the software (for example, the chart of accounts, reporting parameters, or thresholds). In addition, the entity may have a process or procedures to manage access to the application (for example, a designated individual with administrative access to the commercial software). In such circumstances, the entity is unlikely to have or need formalized general IT controls.
- In contrast, a larger entity may rely on IT to a great extent. In such cases, the IT environment may involve multiple IT applications, and the IT processes to manage the IT environment may be complex (for example, a dedicated IT department exists that develops and implements program changes and manages access rights), including that the entity has implemented formalized general IT controls over its IT processes.

- When management is not relying on automated controls or general IT controls to process transactions or maintain the data, and the auditor has not identified any automated controls or other information-processing controls (or any that depend on general IT controls), the auditor may plan to directly test any information produced by the entity involving IT and may not identify any IT applications that are subject to risks arising from the use of IT.
- When management relies on an IT application to process or maintain data and the volume of data is significant, and management relies upon the IT application to perform automated controls that the auditor has also identified, the IT application is likely to be subject to risks arising from the use of IT.

A189. When an entity has greater complexity in its IT environment, identifying the IT applications and other aspects of the IT environment, determining the related risks arising from the use of IT, and identifying general IT controls is likely to require the involvement of team members with specialized skills or knowledge in IT. Such involvement is likely to be essential and may need to be extensive for complex IT environments.

Identifying Other Aspects of the IT Environment That Are Subject to Risks Arising From the Use of IT

A190. The other aspects of the IT environment that may be subject to risks arising from the use of IT include the network, operating system and databases, and, in certain circumstances, interfaces between IT applications. Other aspects of the IT environment are generally not identified when the auditor does not identify IT applications that are subject to risks arising from the use of IT. When the auditor has identified IT applications that are subject to risks arising from IT, other aspects of the IT environment (for example, database, operating system, network) are likely to be identified because such aspects support and interact with the identified IT applications.

Identifying Risks Arising From the Use of IT and General IT Controls (Ref: par. 26*c*)

A191. Appendixes E–F set out considerations for understanding general IT controls.

A192. In identifying the risks arising from the use of IT, the auditor may consider the nature of the identified IT application or other aspect of the IT environment and the reasons for it being subject to risks arising from the use of IT. For some identified IT applications or other aspects of the IT environment, the auditor may identify applicable risks arising from the use of IT that relate primarily to unauthorized access or unauthorized program changes as well as risks related to inappropriate data changes (for example, the risk of inappropriate changes to the data through direct database access or the ability to directly manipulate information).

A193. The extent and nature of the applicable risks arising from the use of IT vary depending on the nature and characteristics of the identified IT applications and other aspects of the IT environment. Applicable IT risks may result when the entity uses external or internal service providers for identified aspects of its IT environment (for example, outsourcing the hosting of its IT environment to a third party or using a shared service center for central management of IT processes in a group). It is more likely that there will be more risks arising from the use of IT when the volume or complexity of automated application controls is higher and management is placing

greater reliance on those controls for effective processing of transactions or the effective maintenance of the integrity of underlying information. Applicable risks arising from the use of IT may also be identified related to cybersecurity.

*Evaluating the Design and Determining Implementation of Identified Controls in the Control Activities Component (Ref: par. 26*d*)*

A194. Evaluating the design of an identified control involves the auditor's consideration of whether the control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting, material misstatements.

A195. The auditor determines the implementation of an identified control by establishing that the control exists and that the entity is using it. There is little point in the auditor assessing the implementation of a control that is not designed effectively. Therefore, the auditor evaluates the design of a control first. An improperly designed control may represent a control deficiency.

A196. Risk assessment procedures to obtain audit evidence about the design and implementation of identified controls in the control activities component may include

- inquiring of entity personnel.
- observing the performance of specific controls.
- inspecting documents and reports.

Inquiry alone, however, is not sufficient for such purposes.

A197. The auditor may perform walk-throughs in evaluating the design of controls that address the risks of material misstatement and determining whether those controls have been implemented. Such walk-throughs, as described in paragraph A198, ordinarily are sufficient to evaluate design and determine implementation. A walk-through involves following a transaction from origination through the entity's processes, including information systems, until it is reflected in the entity's financial records, using the same documents and IT that entity personnel use. Walk-through procedures usually include a combination of inquiry, observation, inspection of relevant documentation, and reperformance of controls.

A198. In performing a walk-through, at the points at which important processing procedures occur, the auditor inquires of the entity's personnel about their understanding of what is required by the entity's prescribed procedures and controls particularly for the application of manual controls. These inquiries, combined with the other walk-through procedures, allow the auditor to gain a sufficient understanding of the process and to be able to identify important points at which a necessary control is missing or not designed effectively. Additionally, inquiries that go beyond a narrow focus on the single transaction used as the basis for the walk-through allow the auditor to gain an understanding of the different types of significant transactions handled by the process.

A199. The auditor may expect, based on experience from the previous audit or based on current period risk assessment procedures, that management does not have effectively designed or implemented controls to address a significant risk. In such instances, the procedures performed to

address the requirement in paragraph 26*d* may consist of determining that such controls have not been effectively designed or implemented. If the results of the procedures indicate that controls have been newly designed or implemented, the auditor is required to perform the procedures in paragraph 26*b–d* on the newly designed or implemented controls.

A200. The auditor may conclude that a control, which is effectively designed and implemented, may be appropriate to test in order to take its operating effectiveness into account in designing substantive procedures. However, when a control is not designed or implemented effectively, there is no benefit in testing it. When the auditor plans to test a control, the information obtained about the extent to which the control addresses the risk or risks of material misstatement is an input to the auditor's control risk assessment at the assertion level.

A201. Evaluating the design and determining the implementation of identified controls in the control activities component is not sufficient to test their operating effectiveness. However, for automated controls, if the procedures performed to evaluate the design of the controls and determine whether they have been implemented meets the requirements of a test of operating effectiveness in AU-C section 330,[45] the auditor may use the results of these procedures as a test of the operating effectiveness of the automated controls by identifying and testing general IT controls that provide for the consistent operation of the automated controls. Obtaining audit evidence about the implementation of a manual control at a point in time does not provide audit evidence about the operating effectiveness of the control at other times during the period under audit. Tests of the operating effectiveness of controls, including tests of indirect controls, are further described in AU-C section 330.[46]

A202. When the auditor does not plan to test the operating effectiveness of identified controls, the auditor's evaluation of the design and determination of the implementation of certain controls may still assist in the design of the nature, timing, and extent of substantive procedures that are responsive to the related risks of material misstatement. Examples are as follows:

- The results of these risk assessment procedures may provide a basis for the auditor's consideration of possible deviations in a population when designing substantive procedures.
- Performance of these risk assessment procedures may lead the auditor to identify a fraud risk related to inadequate segregation of duties in the payroll function, and the auditor may decide to perform certain substantive procedures to address the risk of fictitious employees as a result.
- During the process of evaluating the design of certain controls related to sales, the auditor may become aware that the entity enters into bill-and-hold transactions with customers, and the auditor may design specific substantive procedures related to the agreements with the customers to test appropriateness of revenue recognition under the applicable financial reporting framework.

---

45 Paragraph .08 of AU-C section 330.

46 Paragraphs .08–.11 of AU-C section 330.

Control Deficiencies Within the Entity's System of Internal Control (Ref: par. 27)

A203. In performing the evaluations of each of the components of the entity's system of internal control, as described in paragraphs .21*b*, .22*b*, .24*c*, .25*c*, and .26*d*, the auditor may determine that certain of the entity's policies in a component are not appropriate to the nature and circumstances of the entity. Such a determination may be an indicator that assists the auditor in identifying control deficiencies.

A204. If the auditor has identified one or more control deficiencies, AU-C section 265, *Communicating Internal Control Related Matters Identified in an Audit*,[47] requires the auditor to determine whether, individually or in combination, the deficiencies constitute a material weakness or a significant deficiency. The auditor uses professional judgment in determining whether a deficiency represents a material weakness or a significant control deficiency.[48]

Identifying and Assessing the Risks of Material Misstatement (Ref: par. 28–37)

Why the Auditor Identifies and Assesses the Risks of Material Misstatement

A205. Risks of material misstatement are identified and assessed by the auditor in order to determine the nature, timing, and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence. This evidence enables the auditor to express an opinion on the financial statements at an acceptably low level of audit risk.

A206. Information gathered by performing risk assessment procedures is used as audit evidence to provide the basis for the identification and assessment of the risks of material misstatement. For example, the audit evidence obtained when evaluating the design of identified controls and determining whether those controls have been implemented in the control activities component is used as audit evidence to support the risk assessment. Such evidence also provides a basis for the auditor to design overall responses to address the assessed risks of material misstatement at the financial statement level as well as designing and performing further audit procedures whose nature, timing, and extent are responsive to the assessed risks of material misstatement at the assertion level, in accordance with AU-C section 330.

Identifying Risks of Material Misstatement (Ref: par. 28)

A207. The identification of risks of material misstatement is performed before consideration of any related controls (that is, the inherent risk) and is based on the auditor's preliminary consideration of misstatements that have a reasonable possibility of both occurring and being material if they were to occur.

---

[47] Paragraph .08 of AU-C section 265, *Communicating Internal Control Related Matters Identified in an Audit*.

[48] Paragraphs .A6–.A7 of AU-C section 265 set out indicators of significant deficiencies and matters to be considered in determining whether a deficiency, or a combination of deficiencies, in internal control constitute a significant deficiency.

A208. Identifying the risks of material misstatement also provides the basis for the auditor's determination of relevant assertions, which assists the auditor's determination of the significant classes of transactions, account balances, and disclosures.

Assertions

Why the Auditor Uses Assertions

A209. In identifying and assessing the risks of material misstatement, the auditor uses assertions to consider the different types of potential misstatements that may occur. Assertions for which the auditor has identified related risks of material misstatement are relevant assertions.

The Use of Assertions

A210. In identifying and assessing the risks of material misstatement, the auditor may use the categories of assertions as described in subsequent paragraph A211*a–b* or may express them differently, provided all aspects described in paragraphs A211*a–b* have been covered. The auditor may choose to combine the assertions about classes of transactions and events, and related disclosures, with the assertions about account balances and related disclosures.

A211. Assertions used by the auditor in considering the different types of potential misstatements that may occur may fall into the following categories:

a. Assertions about classes of transactions and events, and related disclosures, for the period under audit:

i. *Occurrence*. Transactions and events that have been recorded or disclosed have occurred, and such transactions and events pertain to the entity.

ii. *Completeness*. All transactions and events that should have been recorded have been recorded, and all related disclosures that should have been included in the financial statements have been included.

iii. *Accuracy*. Amounts and other data relating to recorded transactions and events have been recorded appropriately, and related disclosures have been appropriately measured and described.

iv. *Cutoff*. Transactions and events have been recorded in the correct accounting period.

v. *Classification*. Transactions and events have been recorded in the proper accounts.

vi. *Presentation*. Transactions and events are appropriately aggregated or disaggregated and clearly described, and related disclosures are relevant and understandable in the context of the requirements of the applicable financial reporting framework.

b. Assertions about account balances, and related disclosures, at the period end:

i. *Existence*. Assets, liabilities, and equity interests exist.

ii. *Rights and obligations*. The entity holds or controls the rights to assets, and liabilities are the obligations of the entity.

iii. *Completeness*. All assets, liabilities, and equity interests that should have been recorded have been recorded, and all related disclosures that should have been included in the financial statements have been included.

iv. *Accuracy, valuation, and allocation*. Assets, liabilities, and equity interests have been included in the financial statements at appropriate amounts and any resulting valuation or allocation adjustments have been appropriately recorded, and related disclosures have been appropriately measured and described.

v. *Classification*. Assets, liabilities, and equity interests have been recorded in the proper accounts.

vi. *Presentation*. Assets, liabilities, and equity interests are appropriately aggregated or disaggregated and clearly described, and related disclosures are relevant and understandable in the context of the requirements of the applicable financial reporting framework.

A212. The assertions described in preceding paragraph A211*a–b*, adapted as appropriate, may also be used by the auditor in considering the different types of misstatements that may occur in disclosures not directly related to recorded classes of transactions, events, or account balances. For example, such a disclosure may be a description, required by the applicable financial reporting framework, of an entity's exposure to risks arising from financial instruments, including how the risks arise; the objectives, policies, and processes for managing the risks; and the methods used to measure the risks.

Considerations Specific to Governmental Entities

A213. When making assertions about the financial statements of governmental entities, in addition to those assertions set out in paragraph A211*a–b*, management may often assert that transactions and events have been carried out in accordance with law, regulation, or other authority. Such assertions may fall within the scope of the financial statement audit.

Risks of Material Misstatement at the Financial Statement Level (Ref: par. 28a and 29)

Why the Auditor Identifies and Assesses Risks of Material Misstatement at the Financial Statement Level

A214. The auditor identifies risks of material misstatement at the financial statement level to determine whether the risks have a pervasive effect on the financial statements and, therefore, would require an overall response in accordance with AU-C section 330.[49]

A215. In addition, risks of material misstatement at the financial statement level may also affect individual assertions, and identifying these risks may assist the auditor in assessing risks of

[49] Paragraph .05 of AU-C section 330.

material misstatement at the assertion level and in designing further audit procedures to address the identified risks.

Identifying and Assessing Risks of Material Misstatement at the Financial Statement Level

A216. Risks of material misstatement at the financial statement level refer to risks that relate pervasively to the financial statements as a whole and potentially affect many assertions. Risks of this nature are not necessarily risks identifiable with specific assertions at the class of transactions, account balance, or disclosure level (for example, risk of management override of controls). Rather, they represent circumstances that may pervasively increase the risks of material misstatement at the assertion level. The auditor's evaluation of whether risks identified relate pervasively to the financial statements supports the auditor's assessment of the risks of material misstatement at the financial statement level. In other cases, a number of assertions may also be identified as susceptible to the risk and, therefore, may affect the auditor's risk identification and assessment of risks of material misstatement at the assertion level. For example, the entity faces operating losses and liquidity issues and is reliant on funding that has not yet been secured. In such a circumstance, the financial reporting framework may require management to evaluate whether there is substantial doubt about the entity remaining a going concern, and the auditor may determine that there is a significant risk associated with this determination.

A217. The auditor's identification and assessment of risks of material misstatement at the financial statement level is influenced by the auditor's understanding of the entity's system of internal control, in particular, the auditor's understanding of the control environment, the entity's risk assessment process, and the entity's process to monitor the system of internal control, in addition to the following:

- The outcome of the related evaluations required by paragraphs 21*b*, 22*b*, 24*c*, and 26*c*
- Any control deficiencies identified in accordance with paragraph 27

In particular, risks at the financial statement level may arise from deficiencies in the control environment or from external events or conditions such as declining economic conditions.

A218. Risks of material misstatement due to fraud may be particularly relevant to the auditor's consideration of the risks of material misstatement at the financial statement level. For example, the auditor understands from inquiries of management that the entity's financial statements are to be used in discussions with lenders in order to secure further financing to maintain working capital. The auditor also understands from such inquiries and other procedures that current loan agreements with these lenders contain financial covenants that the entity is at risk of failing to meet and identifies this condition as a fraud risk factor. Therefore, the auditor may determine that there is a greater susceptibility to misstatement due to this identified fraud risk factor, which affects inherent risk (that is, the susceptibility of the financial statements to material misstatement because of the risk of fraudulent financial reporting, such as overstatement of assets and revenue and understatement of liabilities and expenses to ensure that the covenants are met). The auditor may then identify assertion-level risks with respect to existence, accuracy, or valuation of certain assets and completeness of certain liabilities that are susceptible to material misstatement as a result of this financial-statement-level risk.

A219. The auditor's understanding, including the related evaluations, of the control environment and other components of the system of internal control may raise doubts about the auditor's ability to obtain audit evidence on which to base the audit opinion or be cause for withdrawal from the engagement when withdrawal is possible under applicable law or regulation. Examples are as follows:

- As a result of evaluating the entity's control environment, the auditor has concerns about the integrity of the entity's management, which may be so serious that it could cause the auditor to conclude that the risk of intentional misrepresentation by management in the financial statements is such that an audit cannot be conducted.
- As a result of evaluating the entity's information system and communication, the auditor determines that significant changes in the IT environment have been poorly managed, with little oversight from management and those charged with governance. The auditor concludes that there are significant concerns about the condition and reliability of the entity's accounting records. In such circumstances, the auditor may determine that it is unlikely that sufficient appropriate audit evidence will be available to support an unmodified opinion on the financial statements.

A220. AU-C section 705, *Modifications to the Opinion in the Independent Auditor's Report,* establishes requirements and provides guidance in determining whether there is a need for the auditor to express a qualified opinion or disclaim an opinion or, as may be required in some cases, to withdraw from the engagement when withdrawal is possible under applicable law or regulation.

Considerations Specific to Governmental Entities

A221. For governmental entities, the identification of risks at the financial statement level may include consideration of matters related to the political climate, public interest, and program sensitivity.

*Risks of Material Misstatement at the Assertion Level (Ref: par. 28*b*)*

A222. Appendix B sets out examples, in the context of inherent risk factors, of events or conditions that may indicate susceptibility to misstatement that may be material.

A223. Risks of material misstatements that do not relate pervasively to the financial statements are risks of material misstatement at the assertion level.

Relevant Assertions and Significant Classes of Transactions, Account Balances, and Disclosures (Ref: par. 29)

Why Relevant Assertions and Significant Classes of Transactions, Account Balances, and Disclosures Are Determined

A224. Determining relevant assertions and the significant classes of transactions, account balances, and disclosures provides the basis for the scope of the auditor's understanding of the entity's information system required to be obtained in accordance with paragraph 25*a*. This

understanding may further assist the auditor in identifying and assessing risks of material misstatement (see paragraph A93).

Automated Tools and Techniques

A225. The auditor may use automated techniques to assist in the identification of significant classes of transactions, account balances, and disclosures. Examples are as follows:

- An entire population of transactions may be analyzed using automated tools and techniques to understand their nature, source, size, and volume. By applying automated techniques, the auditor may, for example, identify that an account with a zero balance at period end comprised numerous offsetting transactions and journal entries occurring during the period, indicating that the account balance or class of transactions may be significant (for example, a payroll clearing account). This same payroll clearing account may also identify expense reimbursements to management (and other employees), which could be a significant disclosure due to these payments being made to related parties.
- By analyzing the flows of an entire population of revenue transactions, the auditor may more easily identify a significant class of transactions that had not previously been identified.

Disclosures That May Be Significant

A226. Significant disclosures include both quantitative and qualitative disclosures for which there is one or more relevant assertions. Examples of disclosures that have qualitative aspects and that may have relevant assertions and, therefore, may be considered significant by the auditor include disclosures about the following:

- Accounting and reporting complexities associated with an account
- Exposure to losses in an account
- Significant contingent liabilities arising from the activities reflected in an account
- Liquidity and debt covenants of an entity in financial distress
- Events or circumstances that have led to the recognition of an impairment loss
- Key sources of estimation uncertainty, including assumptions about the future
- The nature of a change in accounting policy, and other relevant disclosures required by the applicable financial reporting framework, where, for example, new financial reporting requirements are expected to have a significant impact on the financial position and financial performance of the entity
- Share-based payment arrangements, including information about how any amounts recognized were determined, and other relevant disclosures
- Related parties and related party transactions

- Sensitivity analysis, including the effects of changes in assumptions used in the entity's valuation techniques intended to enable users to understand the underlying measurement uncertainty of a recorded or disclosed amount

Assessing Risks of Material Misstatement at the Assertion Level

Assessing Inherent Risk (Ref: par. 31–33)

Assessing the Likelihood and Magnitude of Misstatement (Ref: par. 31)

Why the Auditor Assesses Likelihood and Magnitude of Misstatement

A227. The auditor assesses the likelihood and magnitude of misstatement for identified risks of material misstatement because the significance of the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement were the misstatement to occur determines where on the spectrum of inherent risk the identified risk is assessed, which informs the auditor's design of further audit procedures to address the risk.

A228. Assessing the inherent risk of identified risks of material misstatement also assists the auditor in determining significant risks. The auditor determines significant risks because specific responses to significant risks are required in accordance with AU-C section 330 and other AU-C sections.

A229. Inherent risk factors influence the auditor's assessment of the likelihood and magnitude of misstatement for the identified risks of material misstatement at the assertion level. The greater the degree to which a class of transactions, account balance, or disclosure is susceptible to material misstatement, the higher the inherent risk assessment is likely to be. Considering the degree to which inherent risk factors affect the susceptibility of an assertion to misstatement assists the auditor in appropriately assessing inherent risk for risks of material misstatement at the assertion level and in designing a more precise response to such a risk.

Spectrum of Inherent Risk

A230. In assessing inherent risk, the auditor uses professional judgment in determining the significance of the combination of the likelihood and magnitude of a misstatement.

A231. The assessed inherent risk relating to a particular risk of material misstatement at the assertion level represents a judgment within a range, from lower to higher, on the spectrum of inherent risk. The judgment about where in the range inherent risk is assessed may vary based on the nature, size, and complexity of the entity and takes into account the assessed likelihood and magnitude of the misstatement and inherent risk factors.

A232. In considering the likelihood of a misstatement, the auditor considers the possibility that a misstatement may occur based on consideration of the inherent risk factors.

A233. In considering the magnitude of a misstatement, the auditor considers the qualitative and quantitative aspects of the possible misstatement (that is, misstatements in assertions about classes

of transactions, account balances, or disclosures may be judged to be material due to size, nature, or circumstances).

A234. The auditor uses the significance of the combination of the likelihood and magnitude of a possible misstatement in determining where on the spectrum of inherent risk (that is, the range) inherent risk is assessed. The higher the combination of likelihood and magnitude, the higher the assessment of inherent risk; the lower the combination of likelihood and magnitude, the lower the assessment of inherent risk.

A235. For a risk to be assessed as higher on the spectrum of inherent risk, it does not mean that both the magnitude and likelihood need to be assessed as high. Rather, it is the intersection of the magnitude and likelihood of the material misstatement on the spectrum of inherent risk that will determine whether the assessed inherent risk is higher or lower on the spectrum of inherent risk. A higher inherent risk assessment may also arise from different combinations of likelihood and magnitude, for example, a higher inherent risk assessment could result from a lower likelihood but a very high magnitude.

A236. In order to develop appropriate strategies for responding to risks of material misstatement, the auditor may designate risks of material misstatement within categories along the spectrum of inherent risk, based on their assessment of inherent risk. These categories may be described in different ways. Regardless of the method of categorization used, the auditor's assessment of inherent risk is appropriate when the design and implementation of further audit procedures to address the identified risks of material misstatement at the assertion level is appropriately responsive to the assessment of inherent risk and the reasons for that assessment.

Pervasive Risks of Material Misstatement at the Assertion Level (Ref: par. 31*b*)

A237. In assessing the identified risks of material misstatement at the assertion level, the auditor may conclude that some risks of material misstatement relate more pervasively to the financial statements as a whole and potentially affect many assertions, in which case, the auditor may update the identification of risks of material misstatement at the financial statement level.

A238. In circumstances in which risks of material misstatement are identified as financial-statement-level risks due to their pervasive effect on a number of assertions and are identifiable with specific assertions, the auditor is required to take into account those risks when assessing inherent risk for risks of material misstatement at the assertion level.

Considerations Specific to Governmental Entities

A239. In exercising professional judgment regarding the assessment of the risk of material misstatement, governmental auditors may consider the complexity of laws and regulations, and the risks of noncompliance therewith.

Significant Risks (Ref: par. 32)

Why Significant Risks Are Determined and the Implications for the Audit

A240. The determination of significant risks allows for the auditor to focus more attention on those risks that are on the upper end of the spectrum, through the performance of certain required responses, including the following:

- Controls that address significant risks are required to be identified in accordance with paragraph 26*a*(i) of this proposed SAS, with a requirement to evaluate whether the control has been designed effectively and implemented in accordance with paragraph 26*d* of this proposed SAS.
- AU-C section 330 requires controls that address significant risks to be tested in the current period (when the auditor intends to rely on the operating effectiveness of such controls) and substantive procedures to be planned and performed that are specifically responsive to the identified significant risk.[50]
- AU-C section 330 requires the auditor to obtain more persuasive audit evidence the higher the auditor's assessment of risk.[51]
- AU-C section 260 requires communicating with those charged with governance about the significant risks identified by the auditor.[52]
- AU-C section 701, *Communicating Key Audit Matters in the Independent Auditor's Report,* requires the auditor to take into account significant risks when determining those matters that required significant auditor attention, which are matters that may be key audit matters.[53]
- Timely review of audit documentation by the engagement partner at the appropriate stages during the audit allows significant matters, including significant risks, to be resolved on a timely basis to the engagement partner's satisfaction on or before the date of the auditor's report.[54]
- AU-C section 600 requires more involvement by the group engagement partner if the significant risk relates to a component in a group audit and for the group engagement team to direct the work required at the component by the component auditor.[55]

Determining Significant Risks

A241. In determining significant risks, the auditor may first identify those assessed risks of material misstatement that have been assessed higher on the spectrum of inherent risk to form the basis for considering which risks may be close to the upper end. Being close to the upper end of the spectrum of inherent risk will differ from entity to entity and will not necessarily be the same

---

50 Paragraphs .15 and. 22 of AU-C section 330.

51 Paragraph .07*b* of AU-C section 330.

52 Paragraph .15 of AU-C section 260.

53 Paragraph .08 of AU-C section 701, *Communicating Key Audit Matters in the Independent Auditor's Report*.

54 Paragraphs .19 and .A17 of AU-C section 220.

55 Paragraphs .57–.58 of AU-C section 600, *Special Considerations — Audits of Group Financial Statements (Including the Work of Component Auditors)*.

for an entity period on period. It may depend on the nature and circumstances of the entity for which the risk is being assessed.

A242. The determination of which of the assessed risks of material misstatement are close to the upper end of the spectrum of inherent risk and, therefore, are significant risks, is a matter of professional judgment, unless the risk is of a type specified to be treated as a significant risk in accordance with the requirements of another AU-C section. AU-C section 240 and AU-C section 550 provide further requirements and guidance in relation to the identification and assessment of the risks of material misstatement due to fraud and transactions with related parties.[56,57] Examples are as follows:

- Cash at a supermarket retailer would ordinarily be determined to be a high likelihood of possible misstatement (due to the risk of cash being misappropriated); however, the magnitude would typically be very low (due to the low levels of physical cash handled in the stores). The combination of these two factors on the spectrum of inherent risk would be unlikely to result in the existence of cash being determined to be a significant risk.
- An entity is in negotiations to sell a business segment. The auditor considers the effect on goodwill impairment and may determine there is a higher likelihood of possible misstatement and a higher magnitude due to the impact of inherent risk factors of subjectivity, uncertainty, and susceptibility to management bias or other fraud risk factors. This may result in goodwill impairment being determined to be a significant risk.

A243. The auditor also takes into account the relative effects of inherent risk factors when assessing inherent risk. The lower the effect of inherent risk factors, the lower the assessed risk is likely to be. Risks of material misstatement that may be assessed as having higher inherent risk and, therefore, may be determined to be a significant risk, may arise from matters such as the following:

- Transactions for which there are multiple acceptable accounting treatments such that subjectivity is involved
- Accounting estimates that have high estimation uncertainty or complex models[58]
- Accounting for unusual or complex transactions, including those in controversial or emerging areas (for example, accounting for revenue with multiple performance obligations that are difficult to value)
- Complexity in data collection and processing to support account balances
- Account balances or quantitative disclosures that involve complex calculations
- Accounting principles that may be subject to differing interpretation

---

56 Paragraphs .25–.27 of AU-C section 240.

57 Paragraph .19 of AU-C section 550.

58 Paragraphs .10–.11 of AU-C section 540, *Auditing Accounting Estimates and Related Disclosures*.

- Changes in the entity's business that involve changes in accounting, for example, mergers and acquisitions

Risks for Which Substantive Procedures Alone Do Not Provide Sufficient Appropriate Audit Evidence (Ref: par. 33)

Why Risks for Which Substantive Procedures Alone Do Not Provide Sufficient Appropriate Audit Evidence Are Required to Be Identified

A244. Due to the nature of a risk of material misstatement, and the control activities that address that risk, in some circumstances, the only way to obtain sufficient appropriate audit evidence is to test the operating effectiveness of controls. Accordingly, there is a requirement for the auditor to identify any such risks because of the implications for the design and performance of further audit procedures in accordance with AU-C section 330 to address risks of material misstatement at the assertion level.

A245. Paragraph 26*a*(iii) also requires the identification of controls that address risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence because the auditor is required, in accordance with AU-C section 330,[59] to design and perform tests of such controls. Determining risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.

A246. When routine business transactions are subject to highly automated processing with little or no manual intervention, it may not be possible to perform only substantive procedures in relation to the risk. This may be the case in circumstances in which a significant amount of an entity's information is initiated, recorded, processed, or reported only in electronic form, such as in an information system that involves a high degree of integration across its IT functions. For example, it is typically not possible to obtain sufficient appropriate audit evidence relating to revenue for a telecommunications entity based on substantive procedures alone. This is because the evidence of call or data activity does not exist in a form that is observable. Instead, controls testing is typically performed to determine that the origination and completion of calls and data activity is correctly captured (for example, minutes of a call or volume of a download) and recorded correctly in the entity's billing system. In such cases

- audit evidence may be available only in electronic form, and its sufficiency and appropriateness usually depend on the effectiveness of controls over its accuracy and completeness.
- the potential for improper initiation or alteration of information to occur and not be detected may be greater if appropriate controls are not operating effectively.

A247. AU-C section 540 provides further guidance related to accounting estimates about risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.[60] In

---

[59] Paragraph .08 of AU-C section 330.

[60] Paragraphs .A87–.A89 of AU-C section 540.

relation to accounting estimates, this may not be limited to automated processing but may also be applicable to complex models.

Assessing Control Risk (Ref: par. 34)

A248. The auditor's plans to test the operating effectiveness of controls is based on the expectation that controls are operating effectively, and this will form the basis of the auditor's assessment of control risk. The initial expectation of the operating effectiveness of controls is based on the auditor's evaluation of the design and the determination of implementation of the identified controls in the control activities component. Once the auditor has tested the operating effectiveness of the controls in accordance with AU-C section 330, the auditor will be able to confirm the initial expectation about the operating effectiveness of controls. If the controls are not operating effectively as expected, then the auditor will need to revise the control risk assessment in accordance with paragraph 37.

A249. The auditor's assessment of control risk may be performed in different ways, depending on preferred audit techniques or methodologies, and may be expressed in different ways.

A250. If the auditor plans to test the operating effectiveness of controls, it may be necessary to test a combination of controls to confirm the auditor's expectation that the controls are operating effectively. The auditor may plan to test both direct and indirect controls, including general IT controls and, if so, take into account the combined expected effect of the controls when assessing control risk. To the extent that the control to be tested does not fully address the assessed inherent risk, the auditor determines the implications on the design of further audit procedures to reduce audit risk to an acceptably low level.

A251. When the auditor plans to test the operating effectiveness of an automated control, the auditor may also plan to test the operating effectiveness of the relevant general IT controls that support the continued functioning of that automated control to address the risks arising from the use of IT, and to provide a basis for the auditor's expectation that the automated control operated effectively throughout the period. When the auditor expects related general IT controls to be ineffective, this determination may affect the auditor's assessment of control risk at the assertion level, and the auditor's further audit procedures may need to include substantive procedures to address the applicable risks arising from the use of IT. Further guidance about the procedures that the auditor may perform in these circumstances is provided in AU-C section 330.[61]

A252. Regardless of whether the auditor plans to test the operating effectiveness of controls for the purpose of assessing control risk, the auditor's understanding of the entity and its environment, the financial reporting framework, and the entity's internal control informs the auditor's design of further audit procedures. Examples follow:

- The auditor's understanding of internal control may indicate that controls are not designed or implemented appropriately, or the entity's control environment does not support the effective operation of control. In this case, there is no point in testing controls; the further audit procedures will consist solely of substantive procedures. If

[61] Paragraphs .A32–.A33 of AU-C section 330.

the auditor determines, pursuant to paragraph 33, that substantive procedures alone cannot provide sufficient appropriate audit evidence, the auditor may need to consider the effect on the auditor's report, as described in AU-C section 330.[62]

- The auditor's understanding of the entity's information system and communication will inform the auditor about the nature of documentation available for testing. For example, if the entity's records are all electronic, the auditor may design audit procedures differently than if the entity's records are in paper format.

Evaluating the Audit Evidence Obtained From the Risk Assessment Procedures (Ref: par. 35)

Why the Auditor Evaluates the Audit Evidence From the Risk Assessment Procedures

A253. Audit evidence obtained from performing risk assessment procedures provides the basis for the identification and assessment of the risks of material misstatement. This provides the basis for the auditor's design of the nature, timing, and extent of further audit procedures responsive to the assessed risks of material misstatement, at the assertion level, in accordance with AU-C section 330. Accordingly, the audit evidence obtained from the risk assessment procedures provides a basis for the identification and assessment of risks of material misstatement whether due to fraud or error at the financial statement and assertion levels.

The Evaluation of the Audit Evidence

A254. Audit evidence from risk assessment procedures comprises both information that supports and corroborates management's assertions, and any information that contradicts such assertions.[63]

Professional Skepticism

A255. In evaluating the audit evidence from the risk assessment procedures, the auditor considers whether sufficient understanding about the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control has been obtained to be able to identify the risks of material misstatement as well as whether there is any evidence that is contradictory that may indicate a risk of material misstatement.

Classes of Transactions, Account Balances, and Disclosures That Are Not Significant but Are Material (Ref: par. 36)

A256. As explained in AU-C section 320,[64] materiality and audit risk are considered when identifying and assessing the risks of material misstatement in classes of transactions, account balances, and disclosures. The auditor's determination of materiality is a matter of professional judgment and is affected by the auditor's perception of the financial information needs of users of the financial statements.[65] For purposes of this proposed SAS, classes of transactions, account

---

62 Paragraph .29 of AU-C section 330.

63 Paragraph .A1 of AU-C section 500.

64 Paragraph .A1 of AU-C section 320

65 Paragraph .04 of AU-C section 320.

balances, or disclosures are material if there is a substantial likelihood that omitting, misstating, or obscuring information about them would influence the judgment made by a reasonable user based on the financial statements.

A257. There may be classes of transactions, account balances, or disclosures that are material but have not been determined to be significant classes of transactions, account balances, or disclosures (that is, there are no relevant assertions identified). For example, the entity may have a disclosure about executive compensation for which the auditor has not identified a risk of material misstatement. However, the auditor may determine that this disclosure is material based on the considerations in paragraph A256.

Revision of Risk Assessment (Ref: par. 37)

A258. During the audit, new or other information may come to the auditor's attention that differs significantly from the information on which the risk assessment was based. For example, the entity's risk assessment may be based on an expectation that certain controls are operating effectively. In performing tests of those controls, the auditor may obtain audit evidence that they were not operating effectively at relevant times during the audit. Similarly, in performing substantive procedures, the auditor may detect misstatements in amounts or frequency greater than is consistent with the auditor's risk assessments. In such circumstances, the risk assessment may not appropriately reflect the true circumstances of the entity, and the further planned audit procedures may not be effective in detecting material misstatements. AU-C section 330[66] provides further guidance about evaluating the operating effectiveness of controls.

Documentation (Ref: par. 38)

A259. For recurring audits, certain documentation may be carried forward, updated as necessary to reflect changes in the entity's business or processes.

A260. AU-C section 230, *Audit Documentation*, notes that among other considerations, although there may be no single way in which the auditor's exercise of professional skepticism is documented, the audit documentation may, nevertheless, provide evidence of the auditor's exercise of professional skepticism.[67] For example, when the audit evidence obtained from risk assessment procedures includes evidence that both corroborates and contradicts management's assertions, the documentation may include how the auditor evaluated that evidence, including the professional judgments made in evaluating whether the audit evidence provides an appropriate basis for the auditor's identification and assessment of the risks of material misstatement. Examples of other requirements in this proposed SAS for which documentation may provide evidence of the exercise of professional skepticism by the auditor include the following:

- Paragraph 13, which requires the auditor to design and perform risk assessment procedures in a manner that is not biased toward obtaining audit evidence that may corroborate the existence of risks or toward excluding audit evidence that may contradict the existence of risks

---

66 Paragraphs .16–.17 of AU-C section 330.

67 Paragraph .A9 of AU-C section 230.

- Paragraph 17, which requires a discussion among key engagement team members of the application of the applicable financial reporting framework and the susceptibility of the entity's financial statements to material misstatement
- Paragraphs 19*b* and 20, which require the auditor to obtain an understanding of the reasons for any changes to the entity's accounting policies and to evaluate whether the entity's accounting policies are appropriate and consistent with the applicable financial reporting framework
- Paragraphs 21*b*, 22*b*, 23*b*, 24*c,* 26*c*, 26*d*, and 27, which require the auditor to evaluate, based on the required understanding obtained, whether the components of the entity's system of internal control are appropriate to the entity's circumstances considering the nature and complexity of the entity, and to determine whether one or more control deficiencies have been identified
- Paragraph 35, which requires the auditor to take into account all audit evidence obtained from the risk assessment procedures, whether corroborative or contradictory to assertions made by management, and to evaluate whether the audit evidence obtained from the risk assessment procedures provides an appropriate basis for the identification and assessment of the risks of material misstatement
- Paragraph 36, which requires the auditor to evaluate, when applicable, whether the auditor's determination that there are no risks of material misstatement for a material class of transactions, account balance, or disclosure remains appropriate

Scalability (Ref: par. 38)

A261. The manner in which the requirements of paragraph 38 are documented is for the auditor to determine using professional judgment.

A262. More detailed documentation that is sufficient to enable an experienced auditor having no previous experience with the audit to understand the nature, timing, and extent of the audit procedures performed and a conclusion or the basis for a conclusion not otherwise readily determinable from the documentation of the work performed or audit evidence obtained[68] may be required to support the rationale for difficult judgments made. An example of such a circumstance may be the rationale for significant judgments related to the inherent risk of an identified risk of material misstatement, when such rationale is not otherwise evident from the audit documentation.

A263. For the audits of less complex entities, the form and extent of documentation may be simple and relatively brief. The form and extent of the auditor's documentation is influenced by the nature, size, and complexity of the entity and its system of internal control, availability of information from the entity, and the audit methodology and technology used in the course of the audit. It is not necessary to document the entirety of the auditor's understanding of the entity and matters related to it. Key elements[69] of understanding documented by the auditor may include those on which the auditor based the assessment of the risks of material misstatement. However, the auditor is not

---

[68] See paragraph .A4 of AU-C section 230.

[69] Paragraph .08 of AU-C section 230.

required to document every inherent risk factor that was taken into account in identifying and assessing the risks of material misstatement at the assertion level. In audits of less complex entities, audit documentation may be incorporated in the auditor's documentation of the overall strategy and audit plan.[70] Similarly, for example, the results of the risk assessment may be documented separately or as part of the auditor's documentation of further audit procedures.[71]

[70] Paragraphs .07, .09, and .A12 of AU-C section 300, *Planning an Audit*.

[71] Paragraph .30 of AU-C section 330.

A264.

Appendix A — Considerations for Understanding the Entity and Its Business Model (Ref: par. A67–A74)

This appendix explains the objectives and scope of the entity's business model and provides examples of matters that the auditor may consider in understanding the activities of the entity that may be included in the business model. The auditor's understanding of the entity's business model, and how it is affected by its business strategy and business objectives, may assist the auditor in identifying business risks that may have an effect on the financial statements. In addition, this may assist the auditor in identifying risks of material misstatement.

Objectives and Scope of an Entity's Business Model

1. An entity's business model describes how an entity considers, for example, its organizational structure, operations or scope of activities, business lines (including competitors and customers thereof), processes, growth opportunities, globalization, regulatory requirements, and technologies. The entity's business model describes how the entity creates, preserves, and captures financial or broader value for its stakeholders.

2. *Strategies* are the approaches by which management plans to achieve the entity's objectives, including how the entity plans to address the risks and opportunities that it faces. An entity's strategies are changed over time by management to respond to changes in its objectives and in the internal and external circumstances in which it operates.

3. A description of a business model typically includes the following:

- The scope of the entity's activities and why it does them
- The entity's structure and scale of its operations
- The markets or geographical or demographic spheres, and parts of the value chain, in which it operates, how it engages with those markets or spheres (main products, customer segments, and distribution methods), and the basis on which it competes
- The entity's business or operating processes (for example, investment, financing, and operating processes) employed in performing its activities, focusing on those parts of the business processes that are important in creating, preserving, or capturing value
- The resources (for example, financial, human, intellectual, environmental, and technological) and other inputs and relationships (for example, customers, competitors, suppliers, and employees) that are necessary or important to its success
- How the entity's business model integrates the use of IT in its interactions with customers, suppliers, lenders, and other stakeholders through IT interfaces and other technologies

4. A business risk may have an immediate consequence for the risk of material misstatement for classes of transactions, account balances, and disclosures at the assertion level or the financial

statement level. For example, the business risk arising from a significant fall in real estate market values may increase the risk of material misstatement associated with the valuation assertion for a lender of medium-term real-estate-backed loans. However, the same risk, particularly in combination with a severe economic downturn that concurrently increases the underlying risk of lifetime credit losses on its loans, may also have a longer-term consequence. The resulting net exposure to credit losses may cast significant doubt on the entity's ability to continue as a going concern. If so, this could have implications for management's, and the auditor's, conclusion regarding the appropriateness of the entity's use of the going concern basis of accounting and determination about whether a material uncertainty exists; therefore, whether a business risk may result in a risk of material misstatement is considered in light of the entity's circumstances. Examples of events and conditions that may give rise to the existence of risks of material misstatement are indicated in appendix B, "Understanding Inherent Risk Factors."

Activities of the Entity

5. The following are some examples of matters that the auditor may consider when obtaining an understanding of the activities of the entity (included in the entity's business model):

a. Business operations:

i. Nature of revenue sources, products or services, and markets, including involvement in electronic commerce such as internet sales and marketing activities

ii. Conduct of operations (for example, stages and methods of production or activities exposed to environmental risks)

iii. Alliances, joint ventures, and outsourcing activities

iv. Geographic dispersion and industry segmentation

v. Location of production facilities, warehouses, and offices, and location and quantities of inventories

vi. Key customers and important suppliers of goods and services, employment arrangements (including the existence of union contracts, pension and other post-employment benefits, stock options or incentive bonus arrangements, and government regulation related to employment matters)

vii. Research and development activities and expenditures

viii. Transactions with related parties

b. Investments and investment activities:

i. Planned or recently executed acquisitions or divestitures

ii. Investments and dispositions of securities and loans

iii. Capital investment activities

iv. Investments in nonconsolidated entities, including noncontrolled partnerships, joint ventures, and noncontrolled variable interest entities

c. Financing and financing activities:

i. Ownership structure of major subsidiaries and associated entities, including consolidated and nonconsolidated structures

ii. Debt structure and related terms, including off-balance-sheet financing arrangements and leasing arrangements

iii. Beneficial owners (local, foreign, business reputation, and experience) and related parties

iv. Use of derivative financial instruments

Nature of Variable Interest Entities

6. A *variable interest entity* is an entity that is generally established for a narrow and well-defined purpose, such as to effect a lease or a securitization of financial assets or to carry out research and development activities. It may take the form of a corporation, trust, partnership, or unincorporated entity. The entity on behalf of which the variable interest entity has been created may often transfer assets to the latter (for example, as part of a derecognition transaction involving financial assets), obtain the right to use the latter's assets, or perform services for the latter, whereas other parties may provide the funding to the latter. As AU-C section 550, *Related Parties*, indicates, in some circumstances, a variable interest entity may be a related party of the entity.[1]

7. Financial reporting frameworks often specify detailed conditions that are deemed to amount to control or circumstances under which the variable interest entity should be considered for consolidation. The interpretation of the requirements of such frameworks often demands a detailed knowledge of the relevant agreements involving the variable interest entity.

[1] Paragraph .A12 of AU-C section 550, *Related Parties.*

A265.

Appendix B — Understanding Inherent Risk Factors (Ref: par. 12, 19, A8–A10, A67, A92–A97, and A222)

This appendix provides further explanation about inherent risk factors as well as matters that the auditor may consider in understanding and applying the inherent risk factors in identifying and assessing the risks of material misstatement at the assertion level.

The Inherent Risk Factors

1. *Inherent risk factors* are characteristics of events or conditions that affect susceptibility of an assertion about a class of transactions, account balance, or disclosure, to misstatement, whether due to fraud or error, and before consideration of controls. Such factors may be qualitative or quantitative and include complexity, subjectivity, change, uncertainty, or susceptibility to misstatement due to management bias or other fraud risk factors[1] insofar as they affect inherent risk. In obtaining the understanding of the entity and its environment, and the applicable financial reporting framework and entity's accounting policies, in accordance with paragraph 19*a–b*, the auditor also understands how inherent risk factors affect susceptibility of assertions to misstatement in the preparation of the financial statements.

2. Inherent risk factors relating to the preparation of information required by the applicable financial reporting framework (referred to in this paragraph as *required information*) include the following:

- *Complexity.* Arises either from the nature of the information or in the way that the required information is prepared, including when such preparation processes are more inherently difficult to apply. For example, complexity may arise in one of the following circumstances:
  - — In calculating supplier rebate provisions because it may be necessary to take into account different commercial terms with many different suppliers or many interrelated commercial terms that are all relevant in calculating the rebates due.
  - — When there are many potential data sources with different characteristics used in making an accounting estimate, the processing of that data involves many interrelated steps and, therefore, the data is inherently more difficult to identify, capture, access, understand, or process.
- *Subjectivity*. Arises from inherent limitations in the ability to prepare required information in an objective manner, due to limitations in the availability of knowledge or information, such that management may need to make an election or subjective judgment about the appropriate approach to take and about the resulting information to include in the financial statements. Because of different approaches to preparing the required information, different outcomes could result from appropriately applying the requirements of the applicable financial reporting framework. As limitations in knowledge or data increase, the subjectivity in the judgments that could be made by

[1] Paragraphs .A28–.A32 of AU-C section 240, *Consideration of Fraud in a Financial Statement Audit*.

reasonably knowledgeable and independent individuals and the diversity in possible outcomes of those judgments will also increase.

- *Change*. Results from events or conditions that, over time, affect the entity's business or the economic, accounting, regulatory, industry, or other aspects of the environment in which it operates, when the effects of those events or conditions are reflected in the required information. Such events or conditions may occur during, or between, financial reporting periods. For example, change may result from developments in the requirements of the applicable financial reporting framework, in the entity and its business model, or in the environment in which the entity operates. Such change may affect management's assumptions and judgments, including as they relate to management's selection of accounting policies or how accounting estimates are made or related disclosures are determined.
- *Uncertainty*. Arises when the required information cannot be prepared based only on sufficiently precise and comprehensive data that is verifiable through direct observation. In these circumstances, an approach may need to be taken that applies the available knowledge to prepare the information using sufficiently precise and comprehensive observable data, to the extent available, and reasonable assumptions supported by the most appropriate available data, when it is not. Constraints on the availability of knowledge or data, which are not within the control of management (subject to cost constraints where applicable) are sources of uncertainty, and their effect on the preparation of the required information cannot be eliminated. For example, estimation uncertainty arises when the required monetary amount cannot be determined with precision, and the outcome of the estimate is not known before the date the financial statements are finalized.
- *Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk.* Susceptibility to management bias results from conditions that create susceptibility to intentional or unintentional failure by management to maintain neutrality in preparing the information. Management bias is often associated with certain conditions that have the potential to give rise to management not maintaining neutrality in exercising judgment (indicators of potential management bias), which could lead to a material misstatement of the information that would be fraudulent if intentional. Such indicators include incentives or pressures insofar as they affect inherent risk (for example, as a result of motivation to achieve a desired result, such as a desired profit target or capital ratio) and opportunity, not to maintain neutrality. Factors relevant to the susceptibility to misstatement due to fraud in the form of fraudulent financial reporting or misappropriation of assets are described in AU-C section 240, *Consideration of Fraud in a Financial Statement Audit*.[2]

3. When complexity is an inherent risk factor, there may be an inherent need for more complex processes in preparing the information, and such processes may be inherently more difficult to apply. As a result, applying them may require specialized skills or knowledge and may require the use of a management's specialists.

---

[2] Paragraphs .A1–.A5 of AU-C section 240.

4. When management judgment is more subjective, the susceptibility to misstatement due to management bias, whether unintentional or intentional, may also increase. For example, significant management judgment may be involved in making accounting estimates that have been identified as having high estimation uncertainty, and conclusions regarding methods, data, and assumptions may reflect unintentional or intentional management bias.

Examples of Events or Conditions That May Give Rise to the Existence of Risks of Material Misstatement

5. The following are examples of events (including transactions) and conditions that may indicate the existence of risks of material misstatement in the financial statements at the financial statement level or the assertion level. The examples, grouped by inherent risk factor, cover a broad range of events and conditions; however, not all events and conditions are relevant to every audit engagement, and the list of examples is not necessarily complete. The events and conditions have been categorized by the inherent risk factor that may have the greatest effect in the circumstances. Importantly, due to the interrelationships among inherent risk factors, the example events and conditions also are likely to be subject to, or affected by, other inherent risk factors to varying degrees.

Relevant inherent risk factor	Examples of events and conditions that may indicate the existence of risks of material misstatement at the assertion level
Complexity	Regulatory: • Operations that are subject to a high degree of complex regulation. Business model: • The existence of complex alliances and joint ventures Applicable financial reporting framework: • Accounting measurements that involve complex processes Transactions: • Use of off-balance-sheet financing, variable interest entities, and other complex financing arrangements
Subjectivity	Applicable financial reporting framework: • A wide range of possible measurement criteria of an accounting estimate, for example, management's recognition of depreciation or construction income and expenses • Management's selection of a valuation technique or model for a noncurrent asset, such as investment properties
Change	Economic conditions:

Relevant inherent risk factor	Examples of events and conditions that may indicate the existence of risks of material misstatement at the assertion level
	• Operations in regions that are economically unstable, for example, countries with significant currency devaluation or highly inflationary economies Markets: • Operations exposed to volatile markets, for example, futures trading Customer loss: • Going concern and liquidity issues, including loss of significant customers Industry model: • Changes in the industry in which the entity operates Business model: • Changes in the supply chain • Developing or offering new products or services, or moving into new lines of business Geography: • Expanding into new locations Entity structure: • Changes in the entity, such as large acquisitions or reorganizations or other unusual events • Entities or business segments likely to be sold Human resources competence: • Changes in key personnel, including departure of key executives IT: • Changes in the IT environment • Installation of significant new IT systems related to financial reporting Applicable financial reporting framework: • Application of new accounting pronouncements Capital: • New constraints on the availability of capital and credit

Relevant inherent risk factor	Examples of events and conditions that may indicate the existence of risks of material misstatement at the assertion level
	Regulatory: • Investigations into the entity's operations or financial results by regulatory or government bodies • Impact of new legislation related to environmental protection
Uncertainty	Reporting: • Events or transactions that involve significant measurement uncertainty, including accounting estimates, and related disclosures • Pending litigation and contingent liabilities, for example, sales warranties, financial guarantees, and environmental remediation
Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk	Reporting: • Opportunities for management and employees to engage in fraudulent financial reporting, including omission or obscuring, of significant information in disclosures Transactions: • Significant transactions with related parties • Significant amount of nonroutine or nonsystematic transactions, including intercompany transactions and large revenue transactions at period end • Transactions that are recorded based on management's intent, for example, debt refinancing, assets to be sold, and classification of marketable securities

Other events or conditions that may indicate risks of material misstatement at the financial statement level:

- Lack of personnel with appropriate accounting and financial reporting skills
- Control deficiencies, particularly in the control environment, risk assessment process and process for monitoring, and especially those not addressed by management
- Past misstatements, history of errors, or a significant amount of adjustments at period end

A266.

Appendix C — Understanding the Entity's System of Internal Control (Ref: par. 12, 21–26, A98–A202)

1. The entity's system of internal control may be reflected in policy and procedures manuals, systems and forms, and the information embedded therein, and is effected by people. The entity's system of internal control is implemented by management, those charged with governance, and other personnel based on the structure of the entity. The entity's system of internal control can be applied based on the decisions of management, those charged with governance, or other personnel and in the context of legal or regulatory requirements to the operating model of the entity, the legal entity structure, or a combination of these.

2. This appendix further explains the components of, as well as the limitations of, the entity's system of internal control as set out in paragraphs 12(l), 21–26, and A98–A202 as they relate to a financial statement audit.

3. Included within the entity's system of internal control are aspects that relate to the entity's reporting objectives, including its financial reporting objectives, but it may also include aspects that relate to its operations or compliance objectives, when such aspects are relevant to financial reporting. For example, controls over compliance with laws and regulations may be relevant to financial reporting when such controls are relevant to the entity's preparation of disclosures of contingencies in the financial statements.

Components of the Entity's System of Internal Control

Control Environment

4. The control environment includes the governance and management functions and the attitudes, awareness, and actions of those charged with governance and management concerning the entity's system of internal control and its importance in the entity. The control environment sets the tone of an organization, influencing the control consciousness of its people, and provides the overall foundation for the operation of the other components of the entity's system of internal control.

5. An entity's control consciousness is influenced by those charged with governance because one of their roles is to counterbalance pressures on management in relation to financial reporting that may arise from market demands or remuneration schemes. Therefore, the effectiveness of the design of the control environment in relation to participation by those charged with governance is influenced by such matters as the following:

- Their independence from management and their ability to evaluate the actions of management
- Whether they understand the entity's business transactions
- The extent to which they evaluate whether the financial statements are prepared in accordance with the applicable financial reporting framework, including whether the financial statements include adequate disclosures

6. The control environment encompasses the following elements:

a. How management's responsibilities are carried out, such as creating and maintaining the entity's culture and demonstrating management's commitment to 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 behavior are the product of the entity's ethical and behavioral standards or codes of conduct, how they are communicated (for example, through policy statements), and how they are reinforced in practice (for example, through management actions to eliminate or mitigate incentives or temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts). The communication of entity policies on integrity and ethical values may include the communication of behavioral standards to personnel through policy statements and codes of conduct and by example.

b. When those charged with governance are separate from management, how those charged with governance demonstrate independence from management and exercise oversight of the entity's system of internal control. An entity's control consciousness is influenced by those charged with governance. Considerations may include whether there are sufficient individuals who are independent from management and objective in their evaluations and decision making; how those charged with governance identify and accept oversight responsibilities and whether those charged with governance retain oversight responsibility for management's design, implementation, and conduct of the entity's system of internal control. The importance of the responsibilities of those charged with governance is recognized in codes of practice and other laws and regulations or guidance produced for the benefit of those charged with governance. Other responsibilities of those charged with governance include oversight of the design and effective operation of whistle-blower procedures.

c. How the entity assigns authority and responsibility in pursuit of its objectives. This may include the following considerations:

- Key areas of authority and responsibility and appropriate lines of reporting
- Policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties
- 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

d. How the entity attracts, develops, and retains competent individuals in alignment with its objectives. This includes how the entity ensures the individuals have the knowledge and skills necessary to accomplish the tasks that define the individual's job, such as the following:

- Standards for recruiting the most qualified individuals, with an emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior

- Training policies that communicate prospective roles and responsibilities, including practices such as training schools and seminars that illustrate expected levels of performance and behavior
- Periodic performance appraisals driving promotions that demonstrate the entity's commitment to the advancement of qualified personnel to higher levels of responsibility

e. How the entity holds individuals accountable for their responsibilities in pursuit of the objectives of the entity's system of internal control. This may be accomplished through some of the following examples:

- Mechanisms to communicate and hold individuals accountable for performance of controls responsibilities and implement corrective actions as necessary
- Establishing performance measures, incentives, and rewards for those responsible for the entity's system of internal control, including how the measures are evaluated and maintain their relevance
- How pressures associated with the achievement of control objectives affect the individual's responsibilities and performance measures
- How the individuals are disciplined as necessary

The appropriateness of the preceding matters will be different for every entity depending on its size, the complexity of its structure, and the nature of its activities.

The Entity's Risk Assessment Process

7. The entity's risk assessment process is an iterative process for identifying and analyzing risks to achieving the entity's objectives and forms the basis for how management or those charged with governance determine the risks to be managed.

8. For financial reporting purposes, the entity's risk assessment process includes how management identifies business risks relevant to the preparation of financial statements in accordance with the entity's applicable financial reporting framework, estimates their significance, assesses the likelihood of their occurrence, and decides upon actions to manage them and the results thereof. For example, the entity's risk assessment process may address how the entity considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements or considers risks of fraud.

9. Risks relevant to reliable financial reporting include external and internal events, transactions, or circumstances that may occur and adversely affect an entity's ability to initiate, record, process, and report financial information consistent with the assertions of management in the financial statements. Management may initiate plans, programs, or actions to address specific risks, or it may decide to assume 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, economic, 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 the entity's system of internal control.
- *New or revamped information system*. Significant and rapid changes in the information system can change the risk relating to the entity's system of 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 the information system may change the risk associated with the entity's system of internal control.
- *New business models, products, or activities*. Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with the entity's system of 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 the entity's system of internal control.
- *Expanded foreign operations*. The expansion or acquisition of foreign operations carries new and often unique risks that may affect internal control, for example, additional or changed risks from foreign currency transactions.
- *New accounting pronouncements*. Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.
- *Use of IT*. Risks relating to
  - — maintaining the integrity of data and information processing;
  - — risks to the entity business strategy that arise if the entity's IT strategy does not effectively support the entity's business strategy; or
  - — changes or interruptions in the entity's IT environment or turnover of IT personnel or when the entity does not make necessary updates to the IT environment or such updates are not timely.

The Entity's Process to Monitor the System of Internal Control

10. The entity's process to monitor the system of internal control is a continual process to evaluate the effectiveness of the entity's system of internal control and to take necessary remedial actions on a timely basis. The entity's process to monitor the entity's system of internal control may consist of ongoing activities, separate evaluations (conducted periodically), or some combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of an entity and may include regular management and supervisory activities. The entity's

process will likely vary in scope and frequency depending on the assessment of the risks by the entity.

11. The objectives and scope of internal audit functions typically include activities designed to evaluate or monitor the effectiveness of the entity's system of internal control.[1] The entity's process to monitor the entity's system of internal control may include activities such as management's review of whether bank reconciliations are being prepared on a timely basis, internal auditors' evaluation of sales personnel's compliance with the entity's policies on terms of sales contracts, and a legal department's oversight of compliance with the entity's ethical or business practice policies. Monitoring is done also to ensure that controls continue to operate effectively over time. For example, if the timeliness and accuracy of bank reconciliations are not monitored, personnel are likely to stop preparing them.

12. Controls related to the entity's process to monitor the entity's system of internal control, including those that monitor underlying automated controls, may be automated or manual, or a combination of both. For example, an entity may use automated monitoring controls over access to certain technology with automated reports of unusual activity to management, who manually investigate identified anomalies.

13. When distinguishing between a monitoring activity and a control related to the information system, the underlying details of the activity are considered, especially when the activity involves some level of supervisory review. Supervisory reviews are not automatically classified as monitoring activities, and it may be a matter of judgment whether a review is classified as a control related to the information system or a monitoring activity. For example, the intent of a monthly completeness control would be to detect and correct errors, whereas a monitoring activity would determine why errors are occurring and assign management the responsibility of fixing the process to prevent future errors. In simple terms, a control related to the information system responds to a specific risk, whereas a monitoring activity assesses whether controls within each of the five components of the entity's system of internal control are operating as intended.

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

The Information System and Communication

15. The information system relevant to the preparation of the financial statements consists of activities and policies, and accounting and supporting records, designed and established to do the following:

[1] AU-C section 610, "The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements," and appendix D, "Considerations for Understanding an Entity's Internal Audit Function," of this proposed SAS provide further guidance related to internal audit.

- Initiate, record, and process entity transactions (as well as to capture, process, and disclose information about events and conditions other than transactions, such as changes in fair values or indicators of impairment) and to maintain accountability for the related assets, liabilities, and equity
- Resolve incorrect processing of transactions, for example, automated suspense files and procedures followed to clear suspense items out on a timely basis
- Process and account for system overrides or bypasses to controls
- Incorporate information from transaction processing in the general ledger (for example, transferring of accumulated transactions from various data tables)
- Capture and process information relevant to the preparation of the financial statements for events and conditions other than transactions, such as the depreciation and amortization of assets and changes in the recoverability of assets
- Ensure information required to be disclosed by the applicable financial reporting framework is accumulated, recorded, processed, summarized, and appropriately reported in the financial statements

16. An entity's business processes include the activities designed to

- develop, purchase, produce, sell, and distribute an entity's products and services;
- ensure compliance with laws and regulations; and
- record information, including accounting and financial reporting information.

Business processes result in the transactions that are recorded, processed, and reported by the information system.

17. The quality of information affects management's ability to make appropriate decisions in managing and controlling the entity's activities and to prepare reliable financial reports.

18. Communication, which involves providing an understanding of individual roles and responsibilities pertaining to the entity's system of internal control, may take 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.

19. Communication by the entity of the financial reporting roles and responsibilities and of significant matters relating to financial reporting involves providing an understanding of individual roles and responsibilities pertaining to the entity's system of internal control relevant to financial reporting. It may include such matters as the extent to which personnel understand how their activities in the information system relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity.

Control Activities

20. Controls in the control activities component are identified in accordance with paragraph 26. Such controls include information-processing controls and general IT controls, both of which may be manual or automated in nature. The greater the extent of automated controls, or controls

involving automated aspects, that management uses and relies on in relation to its financial reporting, the more important it may become for the entity to implement general IT controls that address the continued functioning of the automated aspects of information-processing controls. Controls in the control activities component may pertain, for example, to the following:

- *Authorization and approvals*. An authorization affirms that a transaction is valid (that is, it represents an actual economic event or is within an entity's policy). An authorization typically takes the form of an approval by a higher level of management or of verification and a determination if the transaction is valid. For example, a supervisor approves an expense report after reviewing whether the expenses seem reasonable and within policy. An example of an automated approval is when an invoice unit cost is automatically compared with the related purchase order unit cost within a pre-established tolerance level. Invoices within the tolerance level are automatically approved for payment. Those invoices outside the tolerance level are flagged for additional investigation.

- *Reconciliations*. Reconciliations compare two or more data elements. If differences are identified, action is taken to bring the data into agreement. Reconciliations generally address the completeness or accuracy of processing transactions.

- *Verifications*. Verifications compare two or more items with each other or compare an item with a policy and will likely involve a follow-up action when the two items do not match or the item is not consistent with policy. Verifications generally address the completeness, accuracy, or validity of processing transactions.

- *Physical or logical controls, including those that address security of assets against unauthorized access, acquisition, use, or disposal.* Controls that encompass the following:

  — The physical security of assets, including adequate safeguards such as secured facilities over access to assets and records

  — The authorization for access to computer programs and data files (that is, logical access)

  — The periodic counting and comparison with amounts shown on control records (for example, comparing the results of cash, security, and inventory counts with accounting records)

  The extent to which physical controls intended to prevent theft of assets are relevant to the reliability of financial statement preparation depends on circumstances such as when assets are highly susceptible to misappropriation.

- *Segregation of duties.* Assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets. Segregation of duties is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud in the normal course of the person's duties.

For example, a manager authorizing credit sales is not responsible for maintaining accounts receivable records or handling cash receipts. If one person is able to perform all these activities he

or she could, for example, create a fictitious sale that could go undetected. Similarly, salespersons should not have the ability to modify product price files or commission rates.

Sometimes, segregation is not practical, cost effective, or feasible. For example, smaller and less complex entities may lack sufficient resources to achieve ideal segregation, and the cost of hiring additional staff may be prohibitive. In these situations, management may institute alternative controls. In the preceding example, if the salesperson can modify product price files, a detective control activity can be put in place to have personnel unrelated to the sales function periodically review whether and under what circumstances the salesperson changed prices.

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

Limitations of Internal Control

22. The entity's system of internal control, no matter how effective, can provide an entity with only reasonable assurance about achieving the entity's financial reporting objectives. The likelihood of their achievement is affected by the inherent limitations of internal control. These include the realities that human judgment in decision making can be faulty, and that breakdown in the entity's system of internal control can occur because of human error. For example, there may be an error in the design of, or in the change to, a control. Equally, the operation of a control may not be effective, such as when information produced for the purposes of the entity's system of internal control (for example, an exception report) is not effectively used because the individual responsible for reviewing the information does not understand its purpose or fails to take appropriate action.

23. Additionally, controls can be circumvented by the collusion of two or more people or inappropriate management override of controls. For example, management may enter into side agreements with customers that alter the terms and conditions of the entity's standard sales contracts, which may result in improper revenue recognition. Also, edit checks in an IT application that are designed to identify and report transactions that exceed specified credit limits may be overridden or disabled.

24. Further, in designing and implementing controls, management may make judgments on the nature and extent of the controls it chooses to implement, and the nature and extent of the risks it chooses to assume.

A267.

Appendix D — Considerations for Understanding an Entity's Internal Audit Function (Ref: par. A29–A30 and A130)

This appendix provides further considerations relating to understanding the entity's internal audit function when such a function exists.

Objectives and Scope of the Internal Audit Function

1. The objectives and scope of an internal audit function, the nature of its responsibilities, and its status within the organization, including the function's authority and accountability, vary widely and depend on the size, complexity, and structure of the entity and the requirements of management and, when applicable, those charged with governance. These matters may be set out in an internal audit charter or terms of reference.

2. The responsibilities of an internal audit function may include performing procedures and evaluating the results to provide assurance to management and those charged with governance regarding the design and effectiveness of risk management, the entity's system of internal control, and governance processes. If so, the internal audit function may play an important role in the entity's process to monitor the entity's system of internal control. However, the responsibilities of the internal audit function may be focused on evaluating the economy, efficiency, and effectiveness of operations and, if so, the work of the function may not directly relate to the entity's financial reporting.

Inquiries of the Internal Audit Function

3. If an entity has an internal audit function, inquiries of the appropriate individuals within the function may provide information that is useful to the auditor in obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control, and in identifying and assessing risks of material misstatement at the financial statement and assertion levels. In performing its work, the internal audit function is likely to have obtained insight into the entity's operations and business risks and may have findings based on its work, such as identified control deficiencies or risks, that may provide valuable input into the auditor's understanding of the entity and its environment, the applicable financial reporting framework, the entity's system of internal control, the auditor's risk assessments, or other aspects of the audit. Therefore, the auditor's inquiries are made regardless of whether the auditor expects to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed.[1] Inquiries of particular relevance may be about matters the internal audit function has raised with those charged with governance and the outcomes of the function's own risk assessment process.

4. If, based on responses to the auditor's inquiries, it appears that there are findings that may be relevant to the entity's financial reporting and the audit of the financial statements, the auditor may consider it appropriate to read related reports of the internal audit function.

---

[1] The relevant requirements are contained in AU-C section 610, *Using the Work of Internal Auditors*.

Examples of reports of the internal audit function that may be relevant include the function's strategy and planning documents and reports that have been prepared for management or those charged with governance describing the findings of the internal audit function's examinations.

5. In addition, in accordance with AU-C section 240, *Consideration of Fraud in a Financial Statement Audit*,[2] if the internal audit function provides information to the auditor regarding any actual, suspected, or alleged fraud, the auditor takes this into account in the auditor's identification of risk of material misstatement due to fraud.

6. Appropriate individuals within the internal audit function with whom inquiries are made are those who, in the auditor's judgment, have the appropriate knowledge, experience, and authority, such as the chief internal audit executive or, depending on the circumstances, other personnel within the function. The auditor may also consider it appropriate to have periodic meetings with these individuals.

Consideration of the Internal Audit Function in Understanding the Control Environment

7. In understanding the control environment, the auditor may consider how management has responded to the findings and recommendations of the internal audit function regarding identified control deficiencies relevant to the preparation of the financial statements, including whether and how such responses have been implemented, and whether they have been subsequently evaluated by the internal audit function.

Understanding the Role That the Internal Audit Function Plays in the Entity's Process to Monitor the System of Internal Control

8. If the nature of the internal audit function's responsibilities and assurance activities are related to the entity's financial reporting, the auditor may also be able to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed directly by the auditor in obtaining audit evidence. Auditors may be more likely to be able to use the work of an entity's internal audit function when it appears, for example, based on experience in previous audits or the auditor's risk assessment procedures, that the entity has an internal audit function that is adequately and appropriately resourced relative to the complexity of the entity and the nature of its operations and has a direct reporting relationship to those charged with governance.

9. If, based on the auditor's preliminary understanding of the internal audit function, the auditor expects to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed, AU-C section 610 applies.

10. As is further discussed in AU-C section 610, the activities of an internal audit function are distinct from other monitoring controls that may be relevant to financial reporting, such as reviews of management accounting information that are designed to contribute to how the entity prevents or detects misstatements.

---

[2] Paragraph .19 of AU-C section 240, *Consideration of Fraud in a Financial Statement Audit*.

11. Establishing communications with the appropriate individuals within an entity's internal audit function early in the engagement, and maintaining such communications throughout the engagement, can facilitate effective sharing of information. It creates an environment in which the auditor can be informed of significant matters that may come to the attention of the internal audit function when such matters may affect the work of the auditor. AU-C section 200 discusses the importance of the auditor planning and performing the audit with professional skepticism, including being alert to information that brings into question the reliability of documents and responses to inquiries to be used as audit evidence. Accordingly, communication with the internal audit function throughout the engagement may provide opportunities for internal auditors to bring such information to the auditor's attention. The auditor is then able to take such information into account in the auditor's identification and assessment of risks of material misstatement.

A268.

Appendix E — Considerations for Understanding Information Technology (Ref: par. 12, 25*a*, 26*b*–*c*, A105, and A182)

This appendix provides further matters that the auditor may consider in understanding the entity's use of information technology (IT) in its system of internal control.

Understanding the Entity's Use of IT in the Components of the Entity's System of Internal Control

1. An entity's system of internal control contains manual elements and automated elements (that is, manual and automated controls and other resources used in the entity's system of internal control). An entity's mix of manual and automated elements varies with the nature and complexity of the entity's use of IT. An entity's use of IT affects the manner in which the information relevant to the preparation of the financial statements in accordance with the applicable financial reporting framework is processed, stored, and communicated and, therefore, affects the manner in which the entity's system of internal control is designed and implemented. Each component of the entity's system of internal control may use some extent of IT.

Generally, IT benefits an entity's system of internal control by enabling an entity to do the following:

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

2. The characteristics of manual or automated elements are relevant to the auditor's identification and assessment of the risks of material misstatement and further audit procedures based thereon. Automated controls may be more reliable than manual controls because they cannot be as easily bypassed, ignored, or overridden, and they are also less prone to simple errors and mistakes. Automated controls may be more effective than manual controls in the following circumstances:

    - High volume of recurring transactions, or in situations in which errors that can be anticipated or predicted can be prevented, or detected and corrected, through automation

- Controls in which the specific ways to perform the control can be adequately designed and automated

Understanding the Entity's Use of IT in the Information System (Ref: par. 25a)

3. The entity's information system may include the use of manual and automated elements, which also affect the manner in which transactions are initiated, recorded, processed, and reported. In particular, procedures to initiate, record, process, and report transactions may be enforced through the IT applications used by the entity and how the entity has configured those applications. In addition, records in the form of digital information may replace or supplement records in the form of paper documents.

4. In obtaining an understanding of the IT environment relevant to the flows of transactions and information processing in the information system, the auditor gathers information about the nature and characteristics of the IT applications used as well as the supporting IT infrastructure and IT. The following table includes examples of matters that the auditor may consider in obtaining the understanding of the IT environment and includes examples of typical characteristics of IT environments based on the complexity of IT applications used in the entity's information system. However, such characteristics are directional and may differ depending on the nature of the specific IT applications in use by an entity.

	Examples of typical characteristics of specific types of IT applications		
	Purchased applications with no customization	Purchased applications or simple legacy or low-end enterprise resource planning (ERP) applications with little or no customization	Custom-developed applications or more complex ERP applications with significant customization
Matters related to extent of automation and use of data:			
• The extent of automated procedures for processing, and the complexity of those procedures, including whether there is highly automated, paperless processing	N/A	N/A	Extensive and often complex automated procedures

• The extent of the entity's reliance on system-generated reports in the processing of information	Simple automated report logic	Simple relevant automated report logic	Complex automated report logic; report-writer software
• How data is input (that is, manual input, customer or vendor input, or file load)	Manual data inputs	Small number of data inputs or simple interfaces	Large number of data inputs or complex interfaces
• How IT facilitates communication between applications, databases, or other aspects of the IT environment, internally and externally, as appropriate, through system interfaces	No automated interfaces (manual inputs only)	Small number of data inputs or simple interfaces	Large number of data inputs or complex interfaces
• The volume and complexity of data in digital form being processed by the information system, including whether accounting records or other information are stored in digital form and the location of stored data	Low volume of data or simple data that is able to be verified manually; data available locally	Low volume of data or simple data	Large volume of data or complex data; data warehouses;[1] use of internal or external IT service providers (for example, third-party storage or hosting of data)
Matters related to IT applications and IT infrastructure:			
• The complexity of the nature of the IT applications and the underlying IT infrastructure	Small, simple laptop or client-server-based solution	Mature and stable mainframe, small or simple client server, software as a service cloud	Complex mainframe, large or complex client server, web-facing,

[1] A *data warehouse* is a central repository of integrated data from one or more disparate sources (such as multiple databases) from which reports may be generated or that may be used by the entity for other data analysis activities. A *report-writer* is an IT application that is used to extract data from one or more sources (such as a data warehouse, a database, or an IT application) and present the data in a specified format.

			infrastructure as a service cloud
• Whether there is third-party hosting or outsourcing of IT	If outsourced, competent, mature, proven provider (for example, cloud provider)	If outsourced, competent, mature, proven provider (for example, cloud provider)	Competent, mature, proven provider for certain applications and new or start-up provider for others
• Whether the entity is using emerging technologies that affect its financial reporting	No use of emerging technologies	Limited use of emerging technologies in some applications	Mixed use of emerging technologies across platforms
Matters related to IT processes:			
• The personnel involved in maintaining the IT environment (the number and skill level of the IT support resources that manage security and changes to the IT environment)	Few personnel with limited IT knowledge to process vendor upgrades and manage access	Limited personnel with IT skills/dedicated to IT	Dedicated IT departments with skilled personnel, including programming skills
• The complexity of processes to manage access rights	Single individual with administrative access manages access rights	Few individuals with administrative access manages access rights	Complex processes managed by IT department for access rights
• The complexity of the security over the IT environment, including vulnerability of the IT applications, databases, and other aspects of the IT environment to cyber risks, particularly when there are web-based transactions or transactions involving external interfaces	Simple on-premise access with no external web-facing elements	Some web-based applications with primarily simple, role-based security	Multiple platforms with web-based access and complex security models

• Whether program changes have been made to the manner in which information is processed and the extent of such changes during the period	Commercial software with no source code installed	Some commercial applications with no source code and other mature applications with a small number or simple changes; traditional systems development life cycle	New or large number of complex changes, several development cycles each year
• The extent of change within the IT environment (for example, new aspects of the IT environment or significant changes in the IT applications or the underlying IT infrastructure)	Changes limited to version upgrades of commercial software	Changes consist of commercial software upgrades, ERP version upgrades, or legacy enhancements	New or large number of complex changes, several development cycles each year, heavy ERP customization
• Whether there was a major data conversion during the period and, if so, the nature and significance of the changes made, and how the conversion was undertaken	Software upgrades provided by vendor; no data conversion features for upgrade	Minor version upgrades for commercial software applications with limited data being converted	Major version upgrade, new release, platform change

Emerging Technologies

5. Entities may use emerging technologies (for example, blockchain, robotics, or artificial intelligence) because such technologies may present specific opportunities to increase operational efficiencies or enhance financial reporting. When emerging technologies are used in the entity's information system relevant to the preparation of the financial statements, the auditor may include such technologies in the identification of IT applications and other aspects of the IT environment that are subject to risks arising from the use of IT. Although emerging technologies may be seen to be more sophisticated or more complex compared to existing technologies, the auditor's responsibilities in relation to IT applications and identified general IT controls in accordance with paragraph 26 remain unchanged.

Scalability

6. Obtaining an understanding of the entity's IT environment may be more easily accomplished for a less complex entity that uses commercial software and when the entity does not have access to the source code to make any program changes. Such entities may not have dedicated

IT resources but may have a person assigned in an administrator role for the purpose of granting employee access or installing vendor-provided updates to the IT applications. Specific matters that the auditor may consider in understanding the nature of a commercial accounting software package, which may be the single IT application used by a less complex entity in its information system, may include the following:

- The extent to which the software is well established and has a reputation for reliability.
- The extent to which it is possible for the entity to modify the source code of the software to include additional modules (that is, add-ons) to the base software or to make direct changes to data.
- The nature and extent of modifications that have been made to the software. Although an entity may not be able to modify the source code of the software, many software packages allow for configuration (for example, setting or amending reporting parameters). These do not usually involve modifications to source code; however, the auditor may consider the extent to which the entity is able to configure the software when considering the completeness and accuracy of information produced by the software that is used as audit evidence.
- The extent to which data related to the preparation of the financial statements can be directly accessed (that is, direct access to the database without using the IT application) and the volume of data that is processed. The greater the volume of data, the more likely the entity may need controls that address maintaining the integrity of the data, which may include general IT controls over unauthorized access and changes to the data.

7. Complex IT environments may include highly customized or highly integrated IT applications and, therefore, may require more effort to understand. Financial reporting processes or IT applications may be integrated with other IT applications. Such integration may involve IT applications that are used in the entity's business operations and that provide information to the IT applications relevant to the flows of transactions and information processing in the entity's information system. In such circumstances, certain IT applications used in the entity's business operations may also be relevant to the preparation of the financial statements. Complex IT environments also may require dedicated IT departments that have structured IT processes supported by personnel that have software development and IT environment maintenance skills. In other cases, an entity may use internal or external service providers to manage certain aspects of, or IT processes within, its IT environment (for example, third-party hosting).

Identifying IT Applications That Are Subject to Risks Arising From the Use of IT

8. Through understanding the nature and complexity of the entity's IT environment, including the nature and extent of information-processing controls, the auditor may determine which IT applications the entity is relying upon to accurately process and maintain the integrity of financial information. The identification of IT applications on which the entity relies, may affect the auditor's decision to test the automated controls within such IT applications, assuming that such automated controls address identified risks of material misstatement.

Conversely, if the entity is not relying on an IT application, the automated controls within such IT application are unlikely to be appropriate or sufficiently precise for purposes of operating effectiveness tests. Automated controls that may be identified in accordance with paragraph 26*a* may include, for example, automated calculations or input and processing and output controls, such as a three-way match of a purchase order, vendor shipping document, and vendor invoice. When automated controls are identified by the auditor and the auditor determines through the understanding of the IT environment that the entity is relying on the IT application that includes those automated controls, it may be more likely for the auditor to identify the IT application as one that is subject to risks arising from the use of IT.

9. In considering whether the IT applications for which the auditor has identified automated controls are subject to risks arising from the use of IT, the auditor is likely to consider whether, and the extent to which, the entity may have access to source code that enables management to make program changes to such controls or the IT applications. The extent to which the entity makes program or configuration changes and the extent to which the IT processes over such changes are formalized may also be relevant considerations. The auditor is also likely to consider the risk of inappropriate access or changes to data.

10. System-generated reports that the auditor may intend to use as audit evidence may include, for example, a trade receivable aging report or an inventory valuation report. For such reports, the auditor may obtain audit evidence about the completeness and accuracy of the reports by substantively testing the inputs and outputs of the report. In other cases, the auditor may plan to test the operating effectiveness of the controls over the preparation and maintenance of the report, in which case, the IT application from which it is produced is likely to be subject to risks arising from the use of IT. In addition to testing the completeness and accuracy of the report, the auditor may plan to test the operating effectiveness of general IT controls that address risks related to inappropriate or unauthorized program changes to, or data changes in, the report.

11. Some IT applications may include report-writing functionality within them, whereas some entities may also use separate report-writing applications (that is, report writers). In such cases, the auditor may need to determine the sources of system-generated reports (that is, the application that prepares the report and the data sources used by the report) to determine the IT applications subject to risks arising from the use of IT.

12. The data sources used by IT applications may be databases that, for example, can be accessed only through the IT application or by IT personnel with database administration privileges. In other cases, the data source may be a data warehouse that may itself be considered to be an IT application subject to risks arising from the use of IT.

13. The auditor may have identified a risk for which substantive procedures alone are not sufficient because of the entity's use of highly automated and paperless processing of transactions, which may involve multiple integrated IT applications. In such circumstances, the controls identified by the auditor are likely to include automated controls. Further, the entity may be relying on general IT controls to maintain the integrity of the transactions processed and other information used in processing. In such cases, the IT applications involved in the processing and storage of the information are likely subject to risks arising from the use of IT.

End-User Computing

14. Although audit evidence may also come in the form of system-generated output that is used in a calculation performed in an end-user computing tool (for example, spreadsheet software or simple databases), such tools are not typically identified as IT applications in the context of paragraph 26*b*. Designing and implementing controls around access and change to end-user computing tools may be challenging, and such controls are rarely equivalent to, or as effective as, general IT controls. Rather, the auditor may consider a combination of information-processing controls, taking into account the purpose and complexity of the end-user computing involved, such as some or all of the following:

    - Information-processing controls over the initiation and processing of the source data, including relevant automated or interface controls to the point from which the data is extracted (that is, the data warehouse)
    - Controls to check that the logic is functioning as intended, for example, controls that "prove" the extraction of data, such as reconciling the report to the data from which it was derived, comparing the individual data from the report to the source and vice versa, and controls that check the formulas or macros
    - Use of validation software tools, which systematically check formulas or macros, such as spreadsheet integrity tools

Scalability

15. The entity's ability to maintain the integrity of information stored and processed in the information system may vary based on the complexity and volume of the related transactions and other information. The greater the complexity and volume of data that supports a significant class of transactions, account balance, or disclosure, the less likely it may become for the entity to maintain integrity of that information through information-processing controls alone (for example, input and output controls or review controls). It also becomes less likely that the auditor will be able to obtain audit evidence about the completeness and accuracy of such information through substantive testing alone when such information is used as audit evidence. In some circumstances, when volume and complexity of transactions are lower, management may have an information-processing control that is sufficient to verify the accuracy and completeness of the data (for example, individual sales orders processed and billed may be reconciled to the hard copy originally entered into the IT application). When the entity relies on general IT controls to maintain the integrity of certain information used by IT applications, the auditor may determine that the IT applications that maintain that information are subject to risks arising from the use of IT.

Example characteristics of an IT application that is likely not subject to risks arising from IT	Example characteristics of an IT application that is likely subject to risks arising from IT
• Stand-alone applications. • The volume of data (transactions) is not significant.	• Applications are interfaced. • The volume of data (transactions) is significant.

• The application's functionality is not complex. • Each transaction is supported by original hard copy documentation.	• The application's functionality is complex because – the application automatically initiates transactions, and – there are a variety of complex calculations underlying automated entries.
IT application is likely not subject to risks arising from IT because of the following: • The volume of data is not significant and, therefore, management is not relying upon general IT controls to process or maintain the data. • Management does not rely on automated controls or other automated functionality. The auditor has not identified automated controls in accordance with paragraph 26*a*. • Although management uses system-generated reports in their controls, they do not rely on these reports. Instead, they reconcile the reports back to the hard copy documentation and verify the calculations in the reports. • The auditor will directly test information produced by the entity used as audit evidence.	IT application is likely subject to risks arising from IT because • management relies on an application system to process or maintain data because the volume of data is significant. • management relies upon the application system to perform certain automated controls that the auditor has also identified.

Other Aspects of the IT Environment That Are Subject to Risks Arising From the Use of IT

16. When the auditor identifies IT applications that are subject to risks arising from the use of IT, other aspects of the IT environment are also typically subject to risks arising from the use of IT. The IT infrastructure includes databases, operating system, and network. Databases store the data used by IT applications and may consist of many interrelated data tables. Data in databases may also be accessed directly through database management systems by IT or other personnel with database administration privileges. The operating system is responsible for managing communications between hardware, IT applications, and other software used in the network. As such, IT applications and databases may be directly accessed through the operating system. A network is used in the IT infrastructure to transmit data and to share information, resources, and services through a common communications link. The network also typically establishes a layer of logical security (enabled through the operating system) for access to the underlying resources.

17. When IT applications are identified by the auditor to be subject to risks arising from IT, the databases that store the data processed by an identified IT application is typically also identified. Similarly, because an IT application's ability to operate is often dependent on the operating system and IT applications and databases may be directly accessed from the operating system, the operating system is typically subject to risks arising from the use of IT. The network may be identified when it is a central point of access to the identified IT applications and related databases, when an IT application interacts with vendors or external parties through the internet, or when web-facing IT applications are identified by the auditor.

Identifying Risks Arising From the Use of IT and General IT Controls

18. Examples of risks arising from the use of IT include risks related to inappropriate reliance on IT applications that are inaccurately processing data, processing inaccurate data, or both, as follows:

    - 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. Particular risks may arise when multiple users access a common database.
    - The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.
    - Unauthorized changes to data in master files.
    - Unauthorized changes to IT applications or other aspects of the IT environment.
    - Failure to make necessary changes to IT applications or other aspects of the IT environment.
    - Inappropriate manual intervention.
    - Potential loss of data or inability to access data as required.

19. The auditor's consideration of unauthorized access may include risks related to unauthorized access by internal or external parties (often referred to as *cybersecurity risks*). Such risks may not necessarily affect financial reporting, as an entity's IT environment may also include IT applications and related data that address operational or compliance needs. It is important to note that cyber incidents usually first occur through the perimeter and internal network layers, which tend to be further removed from the IT application, database, and operating systems that affect the preparation of the financial statements. Accordingly, if information about a security breach has been identified, the auditor ordinarily considers the extent to which such a breach had the potential to affect financial reporting. If financial reporting may be affected, the auditor may decide to understand, and test the related controls to determine the possible impact or scope of potential misstatements in the financial statements or may determine that the entity has provided adequate disclosures in relation to such security breach.

20. In addition, laws and regulations that may have a direct or indirect effect on the entity's financial statements may include data protection legislation. Considering an entity's

compliance with such laws or regulations, in accordance with AU-C section 250, *Consideration of Laws and Regulations in an Audit of Financial Statements*, may involve understanding the entity's IT processes and general IT controls that the entity has implemented to address the relevant laws or regulations.

21. General IT controls are implemented to address risks arising from the use of IT. Accordingly, the auditor uses the understanding obtained about the identified IT applications and other aspects of the IT environment and the applicable risks arising from the use of IT in determining the general IT controls to identify. In some cases, an entity may use common IT processes across its IT environment or across certain IT applications, in which case, common risks arising from the use of IT and common general IT controls may be identified.

22. In general, a greater number of general IT controls related to IT applications and databases are likely to be identified than for other aspects of the IT environment. This is because these aspects are the most closely concerned with the information processing and storage of information in the entity's information system. In identifying general IT controls, the auditor may consider controls over actions of both end users and of the entity's IT personnel or IT service providers.

23. Appendix F provides further explanation of the nature of the general IT controls typically implemented for different aspects of the IT environment. In addition, examples of general IT controls for different IT processes are provided.

A269.

Appendix F — Considerations for Understanding General IT Controls (Ref: par. 26*c*(ii) and A184–A190)

This appendix provides further matters that the auditor may consider in understanding general IT controls.

1. The nature of the general IT controls typically implemented for each of the aspects of the IT environment

    a. *Applications*. General IT controls at the IT application layer will correlate to the nature and extent of application functionality and the access paths allowed in the technology. For example, more controls will be relevant for highly integrated IT applications with complex security options than a legacy IT application supporting a small number of account balances with access methods only through transactions.

    b. *Database*. General IT controls at the database layer typically address risks arising from the use of IT related to unauthorized updates to financial reporting information in the database through direct database access or execution of a script or program.

    c. *Operating system*. General IT controls at the operating system layer typically address risks arising from the use of IT related to administrative access, which can facilitate the override of other controls. This includes actions such as compromising other user's credentials; adding new, unauthorized users; loading malware; or executing scripts or other unauthorized programs.

    d. *Network*. General IT controls at the network layer typically address risks arising from the use of IT related to network segmentation, remote access, and authentication. Network controls may be relevant when an entity has web-facing applications used in financial reporting. Network controls may be relevant when the entity has significant business partner relationships or third-party outsourcing, which may increase data transmissions and the need for remote access.

2. Examples of general IT controls that may exist, organized by IT process, include the following:

    a. Process to manage access:

        i. *Authentication*. Controls that ensure a user accessing the IT application or other aspect of the IT environment is using their own log-in credentials (that is, the user is not using another user's credentials).

        ii. *Authorization*. Controls that allow users to access the information necessary for their job responsibilities and nothing further, which facilitates appropriate segregation of duties.

        iii. *Provisioning*. Controls to authorize new users and modifications to existing users' access privileges.

iv. *Deprovisioning*. Controls to remove user access upon termination or transfer.

v. *Privileged access*. Controls over administrative or powerful users' access.

vi. *User-access reviews*. Controls to recertify or evaluate user access for ongoing authorization over time.

vii. *Security configuration controls*. Each technology generally has key configuration settings that help restrict access to the environment.

viii. *Physical access*. Controls over physical access to the data center and hardware because such access may be used to override other controls.

b. Process to manage program or other changes to the IT environment:

i. *Change-management process*. Controls over the process to design, program, test, and migrate changes to a production (that is, end user) environment.

ii. *Segregation of duties over change migration*. Controls that segregate access to make and migrate changes to a production environment.

iii. *Systems development or acquisition or implementation*. Controls over initial IT application development or implementation (or in relation to other aspects of the IT environment).

iv. *Data conversion*. Controls over the conversion of data during development, implementation, or upgrades to the IT environment.

c. Process to manage IT operations:

i. *Job scheduling*. Controls over access to schedule and initiate jobs or programs that may affect financial reporting.

ii. *Job monitoring*. Controls to monitor financial reporting jobs or programs for successful execution.

iii. *Backup and recovery*. Controls to ensure backups of financial reporting data occur as planned and that such data is available and able to be accessed for timely recovery in the event of an outage or attack.

iv. *Intrusion detection*. Controls to monitor for vulnerabilities or intrusions in the IT environment.

3. The following table illustrates examples of general IT controls to address examples of risks arising from the use of IT, including for different IT applications, based on their nature.

Process	Risks	Controls	IT applications		
IT process	**Example risks arising from the use of IT**	**Example general IT controls**	**Purchased applications with no customization – Applicable (yes/no)**	**Purchased applications or simple legacy or low-end ERP applications with little or no customization – Applicable (yes/no)**	**Custom-developed applications or more complex ERP applications with significant customization – Applicable (yes/no)**
Manage access	User-access privileges: Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.	Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles and roles, critical financial reporting transactions, and segregation of duties.	Yes – instead of user-access reviews noted below	Yes	Yes
		Access for terminated or transferred users is removed or modified in a timely manner.	Yes – instead of user-access reviews noted below	Yes	Yes
		User access is periodically reviewed.	Yes – instead of provisioning and deprovisioning controls above	Yes for certain applications	Yes

		Segregation of duties is monitored, and conflicting access is either removed or mapped to mitigating controls, which are documented and tested.	N/A – no system-enabled segregation	Yes for certain applications	Yes
		Privileged-level access (for example, configuration, data and security administrators) is authorized and appropriately restricted.	Yes – likely at IT application layer only	Yes at IT application and certain layers of IT environment for platform	Yes at all layers of IT environment for platform
Manage access	Direct data access: Inappropriate changes are made directly to financial data through means other than application transactions.	Access to application data files or database objects/tables/data is limited to authorized personnel, based on their job responsibilities and assigned roles, and such access is approved by management.	N/A	Yes for certain applications and databases	Yes
Manage access	System settings: Systems are not adequately configured or updated to restrict system access to properly authorized and appropriate users.	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (for example,	Yes – password authentication only	Yes – mix of password and multifactor authentication	Yes

		password minimum length and complexity, expiration, account lockout).			
		The key attributes of the security configuration are appropriately implemented.	N/A – no technical security configurations exist	Yes for certain applications and databases	Yes
Manage change	Application changes: Inappropriate changes are made to application systems or programs that contain relevant automated controls (that is, configurable settings, automated algorithms, automated calculations, and automated data extraction) or report logic.	Application changes are appropriately tested and approved before being moved into the production environment.	N/A – would verify no source code installed	Yes for noncommercial software	Yes
		Access to implement changes into the application production environment is appropriately restricted and segregated from the development environment.	N/A	Yes for noncommercial software	Yes
Manage change	Database changes: Inappropriate changes are made to the database structure and relationships between the data.	Database changes are appropriately tested and approved before being moved into the production environment.	N/A – no database changes made at entity	Yes for noncommercial software	Yes

Manage change	System software changes: Inappropriate changes are made to system software (for example, operating system, network, change-management software, access-control software).	System software changes are appropriately tested and approved before being moved to production.	N/A – no system software changes are made at entity	Yes	Yes
Manage change	Data conversion: Data converted from legacy systems or previous versions introduces data errors if the conversion transfers incomplete, redundant, obsolete, or inaccurate data.	Management approves the results of the conversion of data (for example, balancing and reconciliation activities) from the old application system or data structure to the new application system or data structure and monitors that the conversion is performed in accordance with established conversion policies and procedures.	N/A – Addressed through manual controls	Yes	Yes
IT operations	Network: The network does not adequately prevent unauthorized users from gaining inappropriate access	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system.	N/A – no separate network authentication method exists	Yes	Yes

	to information systems.	Password parameters meet company or professional policies and standards (for example, password minimum length and complexity, expiration, account lockout).			
		Network is architected to segment web-facing applications from the internal network, where internal control over financial reporting relevant applications are accessed.	N/A – no network segmentation employed	Yes – with judgment	Yes – with judgment
		On a periodic basis, vulnerability scans of the network perimeter are performed by the network management team, which also investigates potential vulnerabilities.	N/A	Yes – with judgment	Yes – with judgment
		On a periodic basis, alerts are generated to provide notification of threats identified by the intrusion detection systems. These threats are investigated by the network management team.	N/A	Yes – with judgment	Yes – with judgment

		Controls are implemented to restrict virtual private network (VPN) access to authorized and appropriate users.	N/A – no VPN	Yes – with judgment	Yes – with judgment
IT operations	Data backup and recovery: Financial data cannot be recovered or accessed in a timely manner when there is a loss of data.	Financial data is backed up on a regular basis according to an established schedule and frequency.	N/A – relying on manual backups by finance team	Yes	Yes
IT operations	Job scheduling: Production systems, programs, or jobs result in inaccurate, incomplete, or unauthorized processing of data.	Only authorized users have access to update batch jobs (including interface jobs) in the job-scheduling software.	N/A – no batch jobs	Yes for certain applications	Yes
		Critical systems, programs, or jobs are monitored, and processing errors are corrected to ensure successful completion.	N/A – no job monitoring	Yes for certain applications	Yes

A270.

Appendix G — Amendments to Various Statements on Auditing Standards (SAS), as Amended, and to Various Sections in SAS No. 122, *Statements on Auditing Standards: Clarification and Recodification,* as Amended

(***Boldface italics*** denotes new language. Deleted text is shown in ~~strikethrough~~.)

Amendment to SAS No. 117, *Compliance Audits*, as Amended (AICPA, *Professional Standards*, AU-C sec. 935)

1. The amendment to AU-C section 935 in this appendix is effective for audits of financial statements for periods ending on or after December 15, 2023.

AU-C section 935, *Compliance Audits*

[No amendment to paragraphs .01–.A13.]

.A14 Performing risk assessment procedures to obtain an understanding of the entity's internal control over compliance includes an evaluation of the design of controls and whether the controls have been implemented. Internal control consists of the following five interrelated components: the control environment, the entity's risk assessment ***process***, information and communication systems, control activities, and ***the entity's process to*** monitor~~ing~~ ***the system of internal control***. [fn 12] Section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, contains a detailed discussion of these components.

[fn 12] [Footnote omitted for purposes of this proposed SAS.]

[No further amendment to AU-C section 935.]

Amendments to Various Sections in SAS No. 122, as Amended (AICPA, *Professional Standards*, AU-C secs. 200, 210, 230, 240, 250, 260, 265, 330, 402, 501, 530, 550, 600, 620, and 930)

2. The amendment to each section is effective for audits of financial statements for periods ending on or after December 15, 2023.

AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards*

[No amendment to paragraphs .01–.07.]

.08 GAAS contain objectives, requirements, and application and other explanatory material that are designed to support the auditor in obtaining reasonable assurance. GAAS require that the auditor exercise professional judgment and maintain professional skepticism throughout the planning and performance of the audit and, among other things

- identify and assess risks of material misstatement, whether due to fraud or error, based on an understanding of the entity and its environment, ***the applicable financial reporting framework, and*** ~~including~~ the entity's ***system of*** internal control.

- obtain sufficient appropriate audit evidence about whether material misstatements exist, through designing and implementing appropriate responses to the assessed risks.

- form an opinion on the financial statements, or determine that an opinion cannot be formed, based on an evaluation of the audit evidence obtained.

[No amendment to paragraphs .09–.12.]

Definitions

.13 For purposes of GAAS, the following terms have the meanings attributed below:

…

Risk of material misstatement. The risk that the financial statements are materially misstated prior to audit. This consists of two components, described as follows at the assertion level: ***(Ref: par. .A15)***

Inherent risk – The susceptibility of an assertion about a class of transaction, account balance**,** or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls.

Control risk – The risk that a misstatement that could occur in an assertion about a class of transactions, account balance**,** or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's ~~internal~~ control***s***.

[No further amendment to paragraph .13; no amendment to paragraphs .14–.A14.]

Definitions (Ref: par. .14)

Risk of Material Misstatement

.A15 For purposes of GAAS, a risk of material misstatement exists when

a. there is a reasonable possibility of a misstatement occurring (that is, its likelihood), and

b. if it were to occur, there is a reasonable possibility of the misstatement being material (that is, its magnitude).

[No amendment to paragraphs .A15–.A41.]

[Paragraphs .A15–.A44 are renumbered as .A16–.A45.]

~~.A42~~ *.A43* Inherent risk is ***influenced by inherent risk factors.*** ~~higher for some assertions and related classes of transactions, account balances, and disclosures than for others.~~ ***Depending on the degree to which the inherent risk factors affect the susceptibility to misstatement of an assertion, the level of inherent risk varies on a scale that is referred to as the* spectrum of inherent risk*. The auditor determines significant classes of transactions, account balances, and disclosures, and their relevant assertions, as part of the process of identifying and assessing the risks of material misstatement.*** For example, ~~it may be higher for complex calculations or for~~ accounts ***balances*** consisting of amounts derived from accounting estimates that are subject to significant estimation uncertainty ***may be identified as significant account balances, and the auditor's assessment of inherent risk for the related risks at the assertion level may be higher because of the high estimation uncertainty***. External circumstances giving rise to business risks may also influence inherent risk. For example, technological developments might make a particular product obsolete, thereby causing inventory to be more susceptible to overstatement. Factors in the entity and its environment that relate to several or all of the classes of transactions, account balances, or disclosures may also influence the inherent risk related to a specific assertion. Such factors may include, for example, a lack of sufficient working capital to continue operations or a declining industry characterized by a large number of business failures.

~~A43~~ *.A44* Control risk is a function of the effectiveness of the design, implementation, and maintenance of ~~internal~~ control***s*** by management to address identified risks that threaten the achievement of the entity's objectives relevant to preparation and fair presentation of the entity's financial statements. However, internal control, no matter how well designed and operated, can only reduce, but not eliminate, risks of material misstatement in the financial statements, because of the inherent limitations of ~~internal~~ control***s***. These include, for example, the possibility of human errors or mistakes, or of controls being circumvented by collusion or inappropriate management override. Accordingly, some control risk will always exist. GAAS provide the conditions under which the auditor is required to, or may choose to, test the operating effectiveness of controls in determining the nature, timing, and extent of substantive procedures to be performed. [fn 14]

[fn 14] [Footnote omitted for purposes of this proposed SAS.]

~~.A44~~ .A45 GAAS ***typically*** ~~do not ordinarily~~ refer to ~~inherent risk and control risk separately~~, ~~but rather to a combined assessment~~ ~~of~~ the risks of material misstatement***, rather than inherent risk and control risk separately***. However***, AU-C section 315 requires inherent risk to be assessed separately from control risk to provide a basis for designing and performing audit procedures to respond to the assessed risks of material misstatement at the assertion level.*** ~~the auditor may make separate or combined assessments of inherent and control risk depending on preferred audit techniques or methodologies and practical considerations.~~ The assessment of the risks of material misstatement may be expressed in quantitative terms, such as in percentages or in nonquantitative terms. In any case, the need for the auditor to make appropriate risk assessments is more important than the different approaches by which they may be made.

.A46 Risks of material misstatement are assessed at the assertion level in order to determine the nature, timing, and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence.[fn 15]

[fn 15] Paragraph .06 of AU-C section 330.

[Former paragraphs .A45–.A67 are renumbered as paragraphs .A47–.A68. Subsequent footnotes renumbered.]

[No amendment to former paragraphs .A45–.A63.]

~~.A64~~ .A65 When necessary, the application and other explanatory material provides further explanation of the requirements of an AU-C section and guidance for carrying them out.

- In particular, it may explain more precisely what a requirement means or is intended to cover~~.~~***, including, in some AU-C sections, such as AU-C section 315, why a procedure is required***.

- Include examples of procedures that may be appropriate in the circumstances***.***

Although such guidance does not in itself impose a requirement, it is relevant to the proper application of the requirements of an AU-C section. The auditor is required by paragraph .21 to understand the application and other explanatory material; how the auditor applies the guidance in the engagement depends on the exercise of professional judgment in the circumstances consistent with the objective of the AU-C section. The words "may," "might," and "could" are used to describe these actions and procedures. The application and other explanatory material may also provide background information on matters addressed in an AU-C section.

[No amendment to paragraphs .A64–.A68.]

~~*Considerations Specific to Smaller, Less Complex Entities*~~ ***Scalability Considerations***

.A70 Scalability considerations have been included in some AU-C sections (for example, AU-C section 315) to illustrate the application of the requirements to all

entities, ~~whose~~ regardless of ~~whether~~ their nature and circumstances are less complex, ~~as well as those that are~~ or more complex. Less complex entities are entities for which the characteristics in paragraph .A66 apply.

[Paragraphs .A69–.A85 are renumbered as paragraphs .A71–.A88.]

~~.A69~~ .A71. For purposes of specifying additional considerations to audits of smaller, less complex entities, a *smaller, less complex entity* refers to an entity that typically possesses qualitative characteristics, such as the following:

a. Concentration of ownership and management in a small number of individuals

b. One or more of the following:

i. Straightforward or uncomplicated transactions

ii. Simple record keeping

iii. Few lines of business and few products within business lines

iv. ***Simpler systems of*** ~~Few~~ internal control

v. Few levels of management with responsibility for a broad range of controls

vi. Few personnel, many having a wide range of duties

These qualitative characteristics are not exhaustive, they are not exclusive to smaller, less complex entities, and smaller, less complex entities do not necessarily display all of these characteristics.

Considerations Specific to Automated Tools and Techniques

.A72 The considerations specific to "automated tools and techniques" included in some AU-C sections (for example, AU-C section 315) have been developed to explain how the auditor may apply certain requirements when using automated tools and techniques in performing audit procedures.

[No further amendment to AU-C section 200.]

AU-C section 210*, Terms of the Engagement*

[No amendment to paragraphs .01–.A15.]

.A16 Management has the responsibility to determine what internal control is necessary to enable the preparation and fair presentation of the financial statements. The term *internal control* encompasses a wide range of activities within components ***of the system of internal control*** that may be described as the control environment; the entity's risk

assessment process; ***the entity's process to monitor the system of internal control,*** the information system~~, including the related business processes relevant to financial reporting,~~ and communication; ***and*** control activities~~; and monitoring of controls~~. This division, however, does not necessarily reflect how a particular entity may design, implement, and maintain its internal control or how it may classify any particular component. [fn 9] An entity's internal control will reflect the needs of management, the complexity of the business, the nature of the risks to which the entity is subject, and relevant laws or regulations.

[fn 9] [Footnote omitted for purposes of this proposed SAS.]

[No further amendment to section 210.]

AU-C section 230, ***Audit Documentation***

[No amendment to paragraphs .01–.A19.]

.A20 When preparing audit documentation, the auditor of a smaller, less complex entity may also find it helpful and efficient to record various aspects of the audit together in a single document, with cross-references to supporting working papers as appropriate. Examples of matters that may be documented together in the audit of a smaller, less complex entity include the understanding of the entity and its ***environment, the applicable financial reporting framework, and the entity's system of*** internal control; the overall audit strategy and audit plan; materiality; assessed risks, significant findings or issues noted during the audit; and conclusions reached.

[No further amendment to AU-C section 230.]

AU-C section 240, ***Consideration of Fraud in a Financial Statement Audit***

[No amendment to paragraphs .01–.06.]

.07 Furthermore, the risk of the auditor not detecting a material misstatement resulting from management fraud is greater than for employee fraud because management is frequently in a position to directly or indirectly manipulate accounting records, present fraudulent financial information, or override control***s*** ~~procedures~~ designed to prevent similar frauds by other employees.

[No amendment to paragraphs .08–.15.]

.16 When performing risk assessment procedures and related activities to obtain an understanding of the entity and its environment, ***the applicable financial reporting framework and*** ~~including~~ the entity's ***system of*** internal control, required by section 315,

the auditor should perform the procedures in paragraphs .17–.24 to obtain information for use in identifying the risks of material misstatement due to fraud. [fn 5]

[fn 5] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .17–.19.]

Those Charged With Governance

.20 Unless all of those charged with governance are involved in managing the entity, [fn 7] the auditor should obtain an understanding of how those charged with governance exercise oversight of management's processes for identifying and responding to the risks of fraud in the entity and the ~~internal~~ control***s*** that management has established to mitigate these risks. (Ref: par. .A21–.A23)

[fn 7] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .21–.26.]

.27 The auditor should treat those assessed risks of material misstatement due to fraud as significant risks and, accordingly, to the extent not already done so, the auditor should ~~obtain an understanding of the entity's related~~ ***identify the entity's*** controls~~, including control activities, relevant to~~ ***that address*** such risks ***and evaluate their design and determine whether they have been implemented.*** [***fn 10***] ~~including the evaluation of whether such controls have been suitably designed and implemented to mitigate such fraud risks.~~

[***fn 10***] ***Paragraphs 26a(i) and (d) of proposed SAS*** **Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.**

[No amendment to paragraphs .28–.42. Subsequent footnotes renumbered.]

.43 The auditor should include in the audit documentation [fn 13] ~~of the auditor's understanding of the entity and its environment~~ ***the identification*** and the assessment of the risks of material misstatement required by AU-C section 315***, which includes*** the following***:*** [fn 14]

a. The significant decisions reached during the discussion among the engagement team regarding the susceptibility of the entity's financial statements to material misstatement due to fraud, and how and when the discussion occurred and the audit team members who participated

b. The identified and assessed risks of material misstatement due to fraud at the financial statement level and at the assertion level (See paragraphs .16–.27.)

c. ***Identified controls in the control activities component that address assessed risks of material misstatement due to fraud.***

[fn 13 and fn 14] [Footnotes omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .44–.A8.]

Professional Skepticism *(Ref: par. .12–.14)*

.A9 Maintaining professional skepticism requires an ongoing questioning of whether the information and audit evidence obtained suggests that a material misstatement due to fraud may exist. It includes considering the reliability of the information to be used as audit evidence and ~~the~~ ***identified*** controls ***in the control activities, if any,*** over its preparation and maintenance ~~when relevant~~. Due to the characteristics of fraud, the auditor's professional skepticism is particularly important when considering the risks of material misstatement due to fraud.

[No amendment to paragraphs .A10–.A20.]

.A21 Those charged with governance of an entity oversee the entity's systems for monitoring risk, financial control, and compliance with the law. In some circumstances, governance practices are well-developed, and those charged with governance play an active role in oversight of the entity's assessment of the risks of fraud and ~~of the relevant internal control~~ ***the controls that address such risks***. Because the responsibilities of those charged with governance and management may vary by entity, it is important that the auditor understands the respective responsibilities of those charged with governance and management to enable the auditor to obtain an understanding of the oversight exercised by the appropriate individuals.[fn 18]

[fn 18] [Footnote omitted for purposes of this proposed SAS.]

.A22 An understanding of the oversight exercised by those charged with governance may provide insights regarding the susceptibility of the entity to management fraud, the adequacy of ~~internal~~ control***s that address*** ~~over~~ risks of fraud, and the competency and integrity of management. The auditor may obtain this understanding in a number of ways, such as by attending meetings during which such discussions take place, reading the minutes from such meetings, or making inquiries of those charged with governance.

[No amendment to paragraphs .A23–.A26.]

.A27 In addition to information obtained from applying analytical procedures, other information obtained about the entity and its environment***, the applicable financial reporting framework, and the entity's system of internal control*** may be helpful in identifying the risks of material misstatement due to fraud. The discussion among team members may provide information that is helpful in identifying such risks. In addition, information obtained from the auditor's client acceptance and retention processes, and experience gained on other engagements performed for the entity, for example, engagements to review interim financial information, may be relevant in the identification of the risks of material misstatement due to fraud.

[No amendment to paragraphs .A27–.A29.]

.A30 Examples of fraud risk factors related to fraudulent financial reporting and misappropriation of assets are presented in appendix A, "Examples of Fraud Risk Factors." These illustrative risk factors are classified based on the three conditions that are generally present when fraud exists:

- An incentive or pressure to commit fraud
- A perceived opportunity to commit fraud
- An ability to rationalize the fraudulent action

The inability to observe one or more of these conditions does not necessarily mean that no risk of material misstatement due to fraud exists.

Fraud risk factors may relate to incentives, pressures, or opportunities ~~may~~ that arise from conditions that create susceptibility to misstatement before consideration of controls. Fraud risk factors, which include intentional management bias, are inherent risk factors insofar as they affect inherent risk. Fraud risk factors may also relate to conditions within the entity's system of internal control that provide opportunity to commit fraud or that may affect management's attitude or ability to rationalize fraudulent actions. Fraud r*~~R~~**isk factors reflective of an attitude that permits rationalization of the fraudulent action may not be susceptible to observation by the auditor. Nevertheless, the auditor may become aware of the existence of such information ***through, for example, the required understanding of the entity's control environment.[fn 20] Although the fraud risk factors described in appendix A cover a broad range of situations that may be faced by auditors, they are only examples, and other risk factors may exist.

fn 20 Paragraph 28 of proposed SAS **Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.**

[No amendment to paragraphs .A31–.A36. Subsequent footnotes renumbered.]

.A37 It is, therefore, important for the auditor to obtain an understanding of the controls that management has designed, implemented, and maintained to prevent and detect fraud. ~~In doing so,~~ ***In identifying the controls that address the risks of material misstatement due to fraud,*** the auditor may learn, for example, that management has consciously chosen to accept the risks associated with a lack of segregation of duties. Information from ~~obtaining this understanding~~ ***identifying these controls and evaluating their design and determining whether they have been implemented*** may also be useful in identifying fraud risks factors that may affect the auditor's assessment of the risks that the financial statements may contain material misstatement due to fraud.

[No amendment to paragraphs .A38–.A47.]

.A48 The auditor's consideration of the risks of material misstatement associated with inappropriate override of controls over journal entries ***fn 20*** is important because automated processes and controls 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 to the financial reporting system. Furthermore, when IT is used to transfer information automatically, there may be little or no visible evidence of such intervention in the information systems.

[fn 20] Paragraph 26a(ii) of the proposed SAS **Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.**

[Subsequent footnotes renumbered.]

.A49 When identifying and selecting journal entries and other adjustments for testing and determining the appropriate method of examining the underlying support for the items selected, the following matters may be relevant:

- *The **identification and** assessment of the risks of material misstatement due to fraud*. The presence of fraud risk factors and other information obtained during the auditor's ***identification and*** assessment of the risks of material misstatement due to fraud may assist the auditor to identify specific classes of journal entries and other adjustments for testing.

- *Controls that have been implemented over journal entries and other adjustments*. Effective controls over the preparation and posting of journal entries and other adjustments may reduce the extent of substantive testing necessary, provided that the auditor has tested the operating effectiveness of the controls.

- *The entity's financial reporting process and the nature of evidence that can be obtained*. For many entities, routine processing of transactions involves a combination of manual and automated ~~steps and procedures~~ control***s***. Similarly, the processing of journal entries and other adjustments may involve both manual and automated procedures and controls. When IT is used in the financial reporting process, journal entries and other adjustments may exist only in electronic form.

- *The characteristics of fraudulent journal entries or other adjustments.* Inappropriate journal entries or other adjustments often have unique identifying characteristics. Such characteristics may include entries (*a*) made to unrelated, unusual, or seldom-used accounts; (*b*) made by individuals who typically do not make journal entries; (*c*) recorded at the end of the period or as post-closing entries that have little or no explanation or description; (*d*) made either before or during the preparation of the financial statements that do not have account numbers; or (*e*) containing round numbers or consistent ending numbers.

- *The nature and complexity of the accounts*. Inappropriate journal entries or adjustments may be applied to accounts that (*a*) contain transactions that are

complex or unusual in nature, (*b*) contain significant estimates and period-end adjustments, (*c*) have been prone to misstatements in the past, (*d*) have not been reconciled on a timely basis or contain unreconciled differences, (*e*) contain intercompany transactions, or (*f*) are otherwise associated with an identified risk of material misstatement due to fraud. In audits of entities that have several locations or components, consideration is given to the need to select journal entries from multiple locations.

- Journal entries or other adjustments processed outside the normal course of *business*. Nonstandard journal entries, and other entries such as consolidating adjustments, may not be subject to the same ~~level of internal~~ ***nature and extent of*** control***s*** as those journal entries used on a recurring basis to record transactions such as monthly sales, purchases, and cash disbursements.

[No amendment to paragraphs .A50–.A74.]

Appendix A — Examples of Fraud Risk Factors (Ref: par. .11, .24, and .A30)

.A75

The fraud risk factors identified in this appendix are examples of such factors that may be faced by auditors in a broad range of situations. Separately presented are examples relating to the two types of fraud relevant to the auditor's consideration — that is, fraudulent financial reporting and misappropriation of assets. For each of these types of fraud, the risk factors are further classified based on the three conditions generally present when material misstatements due to fraud occur: (*a*) incentives and pressures, (*b*) opportunities, and (*c*) attitudes and rationalizations. Although the risk factors cover a broad range of situations, they are only examples and, accordingly, the auditor may identify additional or different risk factors. Not all of these examples are relevant in all circumstances, and some may be of greater or lesser significance in entities of different size or with different ownership characteristics or circumstances. Also, the order of the examples of risk factors provided is not intended to reflect their relative importance or frequency of occurrence.

Fraud risk factors may relate to incentives or pressures, or opportunities that arise from conditions that create susceptibility to misstatement before consideration of controls (that is, the inherent risk). Such factors are inherent risk factors and may be due to susceptibility to management bias. Fraud risk factors related to opportunities may also arise from other identified inherent risk factors (for example, complexity or uncertainty may create opportunities that result in susceptibility to misstatement due to fraud). Fraud risk factors related to opportunities may also relate to conditions within the entity's system of internal control, such as limitations or deficiencies in the entity's internal control that create such opportunities. Fraud risk factors related to attitudes or rationalizations may arise, in particular, from limitations or deficiencies in the entity's control environment.

Risk Factors Relating to Misstatements Arising From Fraudulent Financial Reporting

…

~~Internal control components are deficient~~ ***Deficiencies in internal control are*** ~~as~~ a result of the following:

- Inadequate ~~monitoring of~~ ~~***controls***~~ ***process to monitor the entity's system of internal control***, including automated controls and controls over interim financial reporting (when external reporting is required)

- High turnover rates or employment of staff in accounting, IT, or the internal audit function who are not effective

- Accounting and information systems that are not effective, including situations involving significant deficiencies or material weaknesses in internal control

- Weak controls over budget preparation and development and compliance with law or regulation

Risk Factors Arising From Misstatements Arising From Misappropriation of Assets

...

Opportunities

Certain characteristics or circumstances may increase the susceptibility of assets to misappropriation. For example, opportunities to misappropriate assets increase when the following exist:

- Large amounts of cash on hand or processed

- Inventory items that are small in size, of high value, or in high demand

- Easily convertible assets, such as bearer bonds, diamonds, or computer chips

- Fixed assets that are small in size, marketable, or lack observable identification of ownership

Inadequate ~~internal~~ control***s*** over assets may increase the susceptibility of misappropriation of those assets. For example, misappropriation of assets may occur because the following exist:

- Inadequate segregation of duties or independent checks

- Inadequate oversight of senior management expenditures, such as travel and other reimbursements
- Inadequate management oversight of employees responsible for assets (for example, inadequate supervision or monitoring of remote locations)
- Inadequate job applicant screening of employees with access to assets
- Inadequate record keeping with respect to assets
- Inadequate system of authorization and approval of transactions (for example, in purchasing)
- Inadequate physical safeguards over cash, investments, inventory, or fixed assets
- Lack of complete and timely reconciliations of assets
- Lack of timely and appropriate documentation of transactions (for example, credits for merchandise returns)
- Lack of mandatory vacations for employees performing key control functions
- Inadequate management understanding of IT, which enables IT employees to perpetrate a misappropriation
- Inadequate access controls over automated records, including controls over and review of computer systems event logs

Attitudes and Rationalizations

- Disregard for the need for monitoring or reducing risks related to misappropriations of assets
- Disregard for ~~internal~~ control**s** over misappropriation of assets by overriding existing controls or by failing to take appropriate remedial action on known deficiencies in internal control
- Behavior indicating displeasure or dissatisfaction with the entity or its treatment of the employee
- Changes in behavior or lifestyle that may indicate assets have been misappropriated
- The belief by some government or other officials that their level of authority justifies a certain level of compensation and personal privileges
- Tolerance of petty theft

Appendix B — Examples of Possible Audit Procedures to Address the Assessed Risks of Material Misstatement Due to Fraud (Ref: par. .22 and .A46)

.A76

The following are examples of possible audit procedures to address the assessed risks of material misstatement due to fraud resulting from both fraudulent financial reporting and misappropriation of assets. Although these procedures cover a broad range of situations, they are only examples and, accordingly, they may not be the most appropriate nor necessary in each circumstance. Also the order of the procedures provided is not intended to reflect their relative importance.

Consideration at the Assertion Level

…

- If the work of an expert a specialist becomes particularly significant with respect to a financial statement item for which the assessed risk of ***material*** misstatement due to fraud is high, performing additional procedures relating to some or all of the expert's assumptions, methods, or findings to determine that the findings are not unreasonable, or engaging another expert for that purpose

[No further amendment to section 240.]

AU-C section 250*, Consideration of Laws and Regulations in an Audit of Financial Statements*

[No amendment to paragraphs .01–.A23.]

Evaluating the Implications of Noncompliance (Ref: par. .20)

.A24 As required by paragraph .20, the auditor evaluates the implications of noncompliance with regard to other aspects of the audit, including the auditor's risk assessment and the reliability of written representations. The implications of particular instances of noncompliance identified by the auditor will depend on the relationship of the perpetration and concealment, if any, of the act to specific control***s*** ~~activities~~ and the level of management or employees involved, especially implications arising from the involvement of the highest authority within the entity.

[No further amendment to AU-C section 250.]

AU-C section 260, *The Auditor's Communication With Those Charged With Governance*

[No amendment to paragraphs .01–.A19.]

.A20 Communicating significant risks identified by the auditor helps those charged with governance understand those matters and why they ***were determined to be significant risks*** ~~require special audit consideration~~. The communication about significant risks may assist those charged with governance in fulfilling their responsibility to oversee the financial reporting process.

.A21 Other matters regarding the planned scope and timing of the audit may include the following:

- How the auditor plans to address the significant risks of material misstatement, whether due to fraud or error.
- How the auditor plans to address areas of higher assessed risks of material misstatement.
- The auditor's approach to ***the system of*** internal control***,*** ~~relevant to the audit~~ including, when applicable, whether the auditor will express an opinion on the effectiveness of internal control over financial reporting.
- …

[No further amendment to AU-C section 250.]

AU-C section 265, *Communicating Internal Control Related Matters Identified in an Audit*

.01 This section addresses the auditor's responsibility to appropriately communicate to those charged with governance and management deficiencies in ***the entity's system of*** internal control that the auditor has identified in an audit of financial statements. This section does not impose additional responsibilities on the auditor regarding obtaining an understanding of internal control or designing and performing tests of controls over and above the requirements of section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, and section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*. Section 260, *The Auditor's Communication With Those Charged With Governance*, establishes further requirements and provides guidance regarding the auditor's responsibility to communicate with those charged with governance regarding the audit.

.02 The auditor is required to obtain an understanding of ***the entity's system of*** internal control relevant to the audit when identifying and assessing the risks of material misstatement. [fn 1] In making those risk assessments, the auditor considers ***the entity's***

system of internal control in order to design audit procedures that are appropriate in the circumstances but not for the purpose of expressing an opinion on the effectiveness of internal control. The auditor may identify ***control*** deficiencies ~~in internal control~~ not only during this risk assessment process but also at any other stage of the audit. This section specifies which identified deficiencies the auditor is required to communicate to those charged with governance and management.

[fn 1] [Footnote omitted for purposes of this proposed SAS. Subsequent footnotes renumbered.]

[No amendment to paragraphs .03–.A2.]

.A3 Although the concepts underlying ***controls in the*** control activities ***component*** in smaller entities are likely to be similar to those in larger entities, the formality with which controls operate will vary. Further, smaller entities may find that certain types of control***s*** ~~activities~~ are not necessary because of controls applied by management. For example, management's sole authority for granting credit to customers and approving significant purchases can provide effective control over important account balances and transactions, lessening or removing the need for more detailed control***s*** ~~activities~~.

[No amendment to paragraphs .03–.A9.]

.A10 Controls may be designed to operate individually, or in combination, to effectively prevent, or detect and correct, misstatements. [fn 3] For example, controls over accounts receivable may consist of both automated and manual controls designed to operate together to prevent, or detect and correct, misstatements in the account balance. A deficiency in internal control on its own may not be sufficiently important to constitute a significant deficiency or a material weakness. However, a combination of deficiencies affecting the same class of transactions, account balance, or disclosure, ~~relevant~~ assertion, or component of ***the entity's system of*** internal control may increase the risks of misstatement to such an extent to give rise to a significant deficiency or material weakness.

[fn 3] [Footnote omitted for purposes of this proposed SAS.]

[No further amendment to AU-C section 265.]

AU-C section 300*, Planning an Audit*

[No amendment to paragraphs .01–.A25.]

.A26 As discussed in paragraph .A12, a suitable, brief memorandum may serve as the documented strategy for the audit of a smaller entity. For the audit plan, standard audit programs or checklists (see paragraph .A24) drawn up on the assumption of few ~~relevant~~ control***s*** ~~activities~~, which is likely to be the case in a smaller entity, may be used, provided that they are tailored to the circumstances of the engagement, including the auditor's risk assessments.

[No further amendment to AU-C section 300.]

AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*

[No amendment to paragraphs .01–.07.]

Audit Procedures Responsive to the Assessed Risks of Material Misstatement at the Assertion Level

.07 In designing the further audit procedures to be performed, the auditor should

a. consider the reasons for the assessed risk of material misstatement at the relevant assertion level for each ***significant*** class of transactions, account balance, and disclosure, including

i. the likelihood ***and magnitude*** of material misstatement due to the particular characteristics of the ~~relevant~~ ***significant*** class of transactions, account balance, or disclosure (the inherent risk) and

ii. whether the risk assessment takes account of ~~relevant~~ controls ***that address the risk of material misstatement*** (the control risk), thereby requiring the auditor to obtain audit evidence to determine whether the controls are operating effectively (that is, the auditor ~~intends to rely~~ ***plans to test*** ~~on~~ the operating effectiveness of controls in determining the nature, timing, and extent of substantive procedures), and (Ref: par. .A10–.A19)

b. obtain more persuasive audit evidence the higher the auditor's assessment of risk. (Ref: par. .A20)

Tests of Controls

.08 The auditor should design and perform tests of controls to obtain sufficient appropriate audit evidence about the operating effectiveness of ~~relevant~~ controls if

a. the auditor's assessment of risks of material misstatement at the relevant assertion level includes an expectation that the controls are operating effectively (that is, the auditor ~~intends to rely on~~ ***plans to test*** the operating effectiveness of controls in determining the nature, timing, and extent of substantive procedures) or

b. substantive procedures alone cannot provide sufficient appropriate audit evidence at the relevant assertion level. (Ref: par. .A21–.A26)

[No amendment to paragraph .09.]

.10 In designing and performing tests of controls, the auditor should

a. perform other audit procedures in combination with inquiry to obtain audit evidence about the operating effectiveness of the controls, including

i. how the controls were applied at relevant times during the period under audit;

ii. the consistency with which they were applied; and

iii. by whom or by what means they were applied, including, when applicable, whether the person performing the control possesses the necessary authority and competence to perform the control effectively, and (Ref: par. .A28–.A32)

b. ***to the extent not already addressed,*** determine whether the controls to be tested depend upon other controls (indirect controls) and, if so, whether it is necessary to obtain audit evidence supporting the operating effectiveness of those indirect controls. (Ref: par. .A33–.A34)

[No amendment to paragraphs .11–12.]

.13 In determining whether it is appropriate to use audit evidence about the operating effectiveness of controls obtained in previous audits and, if so, the length of the time period that may elapse before retesting a control, the auditor should consider

a. the effectiveness of other ~~elements~~ ***components*** of ***the entity's system of*** internal control, including the control environment, the entity's ***process to*** monitor~~ing of~~ ***the system of internal*** control~~s~~, and the entity's risk assessment process;

b. the risks arising from the characteristics of the control, including whether the control is manual or automated;

c. the effectiveness of general IT controls;

d. the effectiveness of the control and its application by the entity, including the nature and extent of deviations in the application of the control noted in previous audits and whether there have been personnel changes that significantly affect the application of the control;

e. whether the lack of a change in a particular control poses a risk due to changing circumstances; and

f. the risks of material misstatement and the extent of reliance on the control. (Ref: par. .A38)

[No amendment to paragraph .14.]

Controls Over Significant Risks

.15 If the auditor ~~plans~~ ***intends*** to rely on controls over a risk the auditor has determined to be a significant risk, [fn 1] the auditor should test the operating effectiveness of those controls in the current period.

[fn 1] [Footnote omitted for purposes of this proposed SAS.]

Evaluating the Operating Effectiveness of Controls

.16 When evaluating the operating effectiveness of ~~relevant~~ controls ***upon which the auditor intends to rely***, the auditor should evaluate whether misstatements that have been detected by substantive procedures indicate that controls are not operating effectively. The absence of misstatements detected by substantive procedures, however, does not provide audit evidence that controls related to the relevant assertion being tested are effective. (Ref: par. .A43)

.17 If deviations from controls upon which the auditor intends to rely are detected, the auditor should make specific inquiries to understand these matters and their potential consequences and should determine whether

a. the tests of controls that have been performed provide an appropriate basis for reliance on the controls,

b. additional tests of controls are necessary, or

c. the ~~potential~~ risks of ***material*** misstatement need to be addressed using substantive procedures. (Ref: par. .A44)

.18 ~~Irrespective of the assessed risks of material misstatement,~~ ***T~~t~~he*** auditor should ~~design and perform~~ perform substantive procedures for ***each*** ~~all~~ relevant assertion~~s~~ ~~related~~ ***of*** ~~to~~ each ~~material~~ ***significant*** class of transactions, account balance, and disclosure***, regardless of the assessed level of control risk.*** (Ref: par. .A45–.A50)

[No amendment to paragraphs .19–.28.]

.29 If the auditor has not obtained sufficient appropriate audit evidence ~~about~~ ***related to*** a relevant assertion ***about a significant class of transactions, account balance, or disclosure***, the auditor should attempt to obtain further audit evidence. If the auditor is unable to obtain sufficient appropriate audit evidence, the auditor should express a qualified opinion or disclaim an opinion on the financial statements. [fn 4]

[fn 4] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .30–.33.]

Application and Other Explanatory Material

Overall Responses (Ref: par. .05)

.A1 Overall responses to address the assessed risks of material misstatement at the financial statement level may include [fn 6]

- emphasizing to the audit team the need to maintain professional skepticism.
- assigning more experienced staff or those with specialized skills or using specialists.
- providing ~~more supervision~~ ***changes to the nature, timing, and extent of direction and supervision of members of the engagement team and the review of the work performed***.
- incorporating additional elements of unpredictability in the selection of further audit procedures to be performed.
- ***changes to the overall audit strategy as required by AU-C section 300,*** **Planning an Audit*****, or planned audit procedures, and may include changes to the following:***
  - ***The auditor's determination of performance materiality in accordance with AU-C section 320.***
  - ***The auditor's plans to test the operating effectiveness of controls, and the persuasiveness of audit evidence needed to support the planned reliance on the operating effectiveness of the controls, particularly when deficiencies in the control environment or the entity's monitoring activities are identified.***
  - ***The nature, timing, and extent of substantive procedures. For example, it may be appropriate to perform substantive procedures at or near the date of the financial statements when the risk of material misstatement is assessed as higher.***
- ~~making general changes to the nature, timing, or extent of audit procedures (for~~ ***example***~~, performing substantive procedures at period-end instead of at an interim date or modifying the nature of audit procedures to obtain more persuasive audit evidence).~~

[fn 6] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .A2–.A3.]

Audit Procedures Responsive to the Assessed Risks of Material Misstatement at the Assertion Level

The Nature, Timing, and Extent of Further Audit Procedures (Ref: par. .06)

.A4 The auditor's assessment of the identified risks ***of material misstatement*** at the relevant assertion level provides a basis for considering the appropriate audit approach for designing and performing further audit procedures. For example, the auditor may determine that

a. in addition to the substantive procedures that are required for all relevant assertions, in accordance with paragraph .18, an effective response to the assessed risk of material misstatement for a particular assertion can be achieved only by also performing tests of controls.

b. performing only substantive procedures is appropriate for particular assertions, and therefore, the auditor excludes the effect of controls from the ~~relevant risk~~ assessment ***of the risk of material misstatement***. This may be because the ~~auditor's risk assessment procedures have not identified any effective controls relevant to the assertion or because~~ ***auditor has not identified a risk for which substantive procedures alone cannot provide sufficient appropriate audit evidence and, as a result, is not required to test the operating effectiveness of controls.*** ~~testing controls would be inefficient, and t~~***T***herefor***e***, the auditor ~~does not intend to rely on~~ ***may not plan to test*** the operating effectiveness of controls in determining the nature, timing, and extent of substantive procedures.

c. a combined approach using both tests of controls and substantive procedures is an effective approach.

[No amendment to paragraphs .A5–.A6.]

.A7 Extent of an audit procedure refers to the quantity to be performed (for example, a sample size or the number of observations of a control ~~activity~~).

[No amendment to paragraphs .A8–.A9.]

Responding to the Assessed Risks at the Assertion Level (Ref: par. .07a)

.A10 ***AU-C section 315 requires that the auditor's assessment of the risks of material misstatement at the assertion level is performed by assessing inherent risk and control risk. The auditor assesses inherent risk by assessing the likelihood and magnitude of a*** ~~material~~ ***misstatement, taking into account how and the degree to which the inherent risk factors affect the susceptibility to misstatement of relevant assertions.*** ~~***, identified events or conditions relating to significant classes of transactions, account balances or disclosures are subject to, or affected by, the inherent risk factors.***~~[fn 9] The auditor's assessed risks***, including the reasons for those assessed risks,*** may affect both the types of audit procedures to be performed and their combination. For example, when an assessed risk is higher, the auditor may confirm the completeness of the terms of a contract with the counterparty, in addition to inspecting the document. Further, certain audit procedures may be more appropriate for some assertions than others. For example,

regarding revenue, tests of controls may be most responsive to the assessed risk of ***material*** misstatement of the completeness assertion, whereas substantive procedures may be most responsive to the assessed risk of ***material*** misstatement of the occurrence assertion.

[fn 9] Paragraph .48 of AU-C section 315.

[Subsequent footnotes renumbered.]

.A11 The reasons for the assessment given to a risk are relevant in determining the nature of audit procedures. For example, if an assessed risk is lower because of the particular characteristics of a class of transactions without consideration of the related controls, then the auditor may determine that substantive analytical procedures alone provide sufficient appropriate audit evidence. On the other hand, if the assessed risk is lower because ~~of internal~~ ***the auditor plans to test the operating effectiveness of*** controls ***that are appropriately designed and implemented*** and the auditor intends to base the substantive procedures on that low assessment, then the auditor performs tests of those controls, as required by paragraph .08*a*. This may be the case, for example, for a class of transactions of reasonably uniform, noncomplex characteristics that are routinely processed and controlled by the entity's information system.

[No amendment to paragraphs .A12–.A18.]

.A19 *Considerations specific to smaller, less complex entities*. In the case of smaller entities, the auditor may not identify control***s*** ~~activities~~, or the extent to which their existence or operation have been documented by the entity may be limited. In such cases, it may be more efficient for the auditor to perform further audit procedures that are primarily substantive procedures. In some rare cases, however, the absence of control***s*** ~~activities~~ or ~~other~~ components of ***the system of internal*** control may make it impossible to obtain sufficient appropriate audit evidence.

[No amendment to paragraph .A20.]

Tests of Controls

Designing and Performing Tests of Controls (Ref: par. .08)

.A21 Tests of controls are performed only on those controls that the auditor ***plans to test and*** has determined are suitably designed to prevent, or detect and correct, a material misstatement in a relevant assertion***.*** If substantially different controls were used at different times during the period under audit, each is considered separately.

[No amendment to paragraphs .A22–.A24.]

.A25 In some cases, the auditor may find it impossible to design effective substantive procedures that, by themselves, provide sufficient appropriate audit evidence at the relevant assertion level. [fn 9] This may occur when an entity conducts its business using IT and no documentation of transactions is produced or maintained, other than through the

IT system. In such cases, paragraph .08 requires the auditor to perform tests of ~~relevant~~ controls ***that address the risk for which substantive procedures alone cannot provide sufficient appropriate audit evidence***.

[fn 9] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .A26–.A28.]

.A29 The nature of the particular control influences the type of audit procedure necessary to obtain audit evidence about whether the control was operating effectively. For example, if operating effectiveness is evidenced by documentation, the auditor may decide to inspect such documentation to obtain audit evidence about operating effectiveness. For other controls, however, documentation may not be available or relevant. For example, documentation of operation may not exist for some factors in the control environment, such as assignment of authority and responsibility, or for some types of control***s*** ~~activities~~, such as ***automated*** control***s*** ~~activities performed by a computer~~. In such circumstances, audit evidence about operating effectiveness may be obtained through inquiry in combination with other audit procedures, such as observation or the use of CAATs.

[No amendment to paragraphs .A30–.A31.]

.A32 Because of the inherent consistency of IT processing, it may not be necessary to increase the extent of testing of an automated control. An automated control can be expected to function consistently unless the ~~program~~ ***IT application*** (including the tables, files, or other permanent data used by the ~~program~~ ***IT application***) 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 may consider performing tests to determine that the control continues to function effectively. Such tests ~~might~~ ***may*** include ***testing the general IT controls related to the IT application.*** ~~determining that~~

- ~~changes to the program are not made without being subject to the appropriate program change controls,~~
- ~~the authorized version of the program is used for processing transactions, and~~
- ~~other relevant general controls are effective.~~

~~Such tests also might include determining that changes to the programs have not been made, which may be the case when the entity uses packaged software applications without modifying or maintaining them. For example, the auditor may inspect the record of the administration of IT security to obtain audit evidence that unauthorized access has not occurred during the period.~~

.A33 Similarly, the auditor may perform tests of controls that address risks of material misstatement related to the integrity of the entity's data, or the completeness and accuracy of the entity's system-generated reports, or may determine they are

necessary to address risks of material misstatement because substantive procedures alone cannot provide sufficient appropriate audit evidence. These tests of controls may include tests of general IT controls that address the matters in paragraph .10a. When this is the case, the auditor may not need to perform any further testing to obtain audit evidence about the matters in paragraph .10a.

.A34 When the auditor determines that a general IT control is deficient, the auditor may consider the nature of the related risks arising from the use of IT that were identified in accordance with the proposed SAS [fn 12] to provide the basis for the design of the auditor's additional procedures to address the assessed risk of material misstatement. Such procedures may address determining the following:

- ***Whether the related risks arising from IT have occurred. For example, if users have unauthorized access to an IT application (but cannot access or modify the system logs that track access), the auditor may decide to inspect the system logs to obtain audit evidence that those users did not access the IT application during the period.***

- ***Whether there are any alternate or redundant general IT controls, or any other controls, that address the related risks arising from the use of IT. If so, the auditor may identify such controls (if not already identified) and, therefore, evaluate their design, determine that they have been implemented, and perform tests of their operating effectiveness. For example, if a general IT control related to user access is deficient, the entity may have an alternate control whereby IT management reviews end-user access reports on a timely basis. Circumstances in which an application control may address a risk arising from the use of IT may include when the information that may be affected by the general IT control deficiency can be reconciled to external sources (for example, a bank statement) or internal sources not affected by the general IT control deficiency (for example, a separate IT application or data source).***

[fn 12] Paragraph .41 of AU-C section 315.

[Paragraphs .A33–.A77 renumbered as paragraphs .A35 to .A79. Subsequent footnotes renumbered.]

.A35.~~A33~~ *Testing of indirect controls (Ref: par. .10b)*. In some circumstances, it may be necessary to obtain audit evidence supporting the effective operation of indirect controls ***(for example, general IT controls)***. ***As explained in paragraphs .A33–.A34, general IT controls may have been identified in accordance with the proposed SAS because of their support of the operating effectiveness of automated controls or due to their support in maintaining the integrity of information used in the entity's financial reporting, including system-generated reports. The requirement in paragraph .10b acknowledges that the auditor may have already tested certain indirect controls to address the matters in paragraph .10a.*** ~~For example, when the auditor decides to test the effectiveness of a user review of exception reports detailing sales in excess of authorized credit limits, the user review and related follow up is the control that is of direct~~

~~relevance to the auditor. Controls over the accuracy of the information in the reports (for example, the general IT controls) are described as indirect controls.~~

~~**.A34** Because of the inherent consistency of IT processing, audit evidence about the implementation of an automated application control, when considered in combination with audit evidence about the operating effectiveness of the entity's general IT controls (in particular, change controls), also may provide substantial audit evidence about its operating effectiveness.~~

Timing of Tests of Controls

.A36~~.A35~~ *Intended period of reliance (Ref: par. .11)*. Audit evidence pertaining only to a point in time may be sufficient for the auditor's purpose (for example, when testing controls over the entity's physical inventory counting at the period-end). If, on the other hand, the auditor intends to rely on a control over a period, tests that are capable of providing audit evidence that the control operated effectively at relevant times during that period are appropriate. Such tests may include tests of ***controls in*** the entity's ***process to*** monitor~~ing~~ ***the system of internal*** ~~of~~ control~~s~~.

[No amendment to paragraphs .A36–.A37.]

.A38 *Using audit evidence obtained in previous audits (Ref: par. .13)*. In certain circumstances, audit evidence obtained from previous audits may provide audit evidence, provided that the auditor has determined whether changes have occurred since the previous audit that may affect its relevance ***to the current audit and its reliability***. For example, in performing a previous audit, the auditor may have determined that an automated control was functioning as intended. The auditor may obtain audit evidence to determine whether changes to the automated control have been made that affect its continued effective functioning through, for example, inquiries of management and the inspection of logs to indicate what controls have been changed. Consideration of audit evidence about these changes may support either increasing or decreasing the expected audit evidence to be obtained in the current period about the operating effectiveness of the controls.

.A39 *Controls that have changed from previous audits (Ref: par. .14a)*. Changes may affect the relevance ***and reliability*** of the audit evidence obtained in previous audits such that there may no longer be a basis for continued reliance. For example, changes in a system that enable an entity to receive a new report from the system probably do not affect the relevance of audit evidence from a previous audit; however, a change that causes data to be accumulated or calculated differently does affect it.

[No amendment to paragraph .A40.]

.A41 In general, the higher the risk of material misstatement or the greater the reliance on controls, the shorter the time period elapsed, if any, is likely to be. Factors that may decrease the period for retesting a control or result in not relying on audit evidence obtained in previous audits at all include the following:

- A deficient control environment
- ***A d***~~D~~deficiency~~t~~ ***in the entity's process to*** monitor~~ing~~ ***the system of internal*** controls
- A significant manual element to the relevant controls
- Personnel changes that significantly affect the application of the control
- Changing circumstances that indicate the need for changes in the control
- Deficient general IT controls

[No amendment to paragraphs .A42–.A44.]

Substantive Procedures (Ref: par. .06 and .18)

.A45 Paragraph .18 requires the auditor to design and perform substantive procedures for all relevant assertions related to each ~~material~~ ***significant*** class of transactions, account balance, and disclosure~~, irrespective of the assessed risks of material misstatement~~. ***For such classes of transactions, account balances, and disclosures, substantive procedures may have already been performed because paragraph .06 requires the auditor to design and perform further audit procedures that are responsive to the assessed risks of material misstatement at the assertion level. Accordingly, substantive procedures are required to be designed and performed in accordance with paragraph .18 w***hen the further audit procedures designed and performed in accordance with paragraph .06 for significant classes of transactions, account balances, or disclosures, designed and performed in accordance with paragraph ***.0***6, did not include substantive procedures**.**

This requirement reflects the facts that (i) the auditor's assessment of risk is judgmental and may not identify all risks of material misstatement and (ii) inherent limitations to internal controls exist, including management override.

[No amendment to paragraphs .A46–.A47.]

.A48 The ~~nature~~ ***assessment*** of the risk ~~and~~ ***or the nature of the*** assertion is relevant to the design of tests of details. For example, tests of details related to the existence or occurrence assertion may involve selecting from items contained in a financial statement amount and obtaining the relevant audit evidence. On the other hand, tests of details related to the completeness assertion may involve selecting from items that are expected to be included in the relevant financial statement amount and investigating whether they are included. For example, the auditor might inspect subsequent cash disbursements and compare them with the recorded accounts payable to determine whether any purchases had been omitted from accounts payable.

.A49 Because the assessment of the risks of material misstatement takes account of ~~internal~~ control***s which the auditor plans to test***, the extent of substantive procedures

may need to be increased when the results from tests of controls are unsatisfactory. However, increasing the extent of an audit procedure is appropriate only if the audit procedure itself is relevant to the specific risk.

[No amendment to paragraphs .A50–.A60.]

.A61 Performing substantive procedures at an interim date without undertaking additional procedures at a later date increases the risk that the auditor will not detect misstatements that may exist at the period-end. This risk increases as the remaining period is lengthened. Factors such as the following may influence whether to perform substantive procedures at an interim date:

- The effectiveness of the control environment and other ~~relevant~~ controls
- The availability at a later date of information necessary for the auditor's procedures
- The purpose of the substantive procedure
- The assessed risk of material misstatement
- The nature of the class of transactions or account balance and relevant assertions
- The ability of the auditor to perform appropriate substantive procedures or substantive procedures combined with tests of controls to cover the remaining period in order to reduce the risk that misstatements that may exist at the period-end will not be detected

[No amendment to paragraph .A62]

.A63 Factors such as the following may influence whether to perform substantive analytical procedures with respect to the period between the interim date and the period-end:

- Whether the period-end balances of the particular classes of transactions or account balances are reasonably predictable with respect to amount, relative significance, and composition
- Whether the entity's procedures for analyzing and adjusting such classes of transactions or account balances at interim dates and establishing proper accounting cutoffs are appropriate
- Whether the information system ~~relevant to financial reporting~~ will provide information concerning the balances at the period-end and the transactions in the remaining period that is sufficient to permit investigation of the following:

— Significant unusual transactions or entries (including those at or near the period-end)

— Other causes of significant fluctuations or expected fluctuations that did not occur

— Changes in the composition of the classes of transactions or account balances

[No amendment to paragraphs .A64–.A72.]

.A73 An audit of financial statements is a cumulative and iterative process. As the auditor performs planned audit procedures, the audit evidence obtained may cause the auditor to modify the nature, timing, or extent of other planned audit procedures. Information may come to the auditor's attention that differs significantly from the information on which the risk assessments were based. For example

- the extent of misstatements that the auditor detects by performing substantive procedures may ***alter the auditor's professional judgment about the risk assessments and indicate a significant deficiency or material weakness in internal control.***

- ***the auditor may become aware of discrepancies in accounting records or conflicting or missing evidence.***

- ***analytical*** procedures performed at the overall review stage of the audit may indicate a previously unrecognized risk of material misstatement.

In such circumstances, the auditor may need to reevaluate the planned audit procedures, based on the revised consideration of assessed risks ***of material misstatement*** ~~for all or some~~***and the effect on the*** ~~of~~ ***significant*** classes of transactions, account balances, or disclosures and ~~related~~ ***their relevant*** assertions. Section 315 contains further guidance on revising the auditor's risk assessment. [fn 13]

[fn 13] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraph .A74]

.A75 The auditor's professional judgment about what constitutes sufficient appropriate audit evidence is influenced by such factors as the

- significance of the potential misstatement in the relevant assertion and the likelihood of its having a material effect, individually or aggregated with other potential misstatements, on the financial statements (see section 450, *Evaluation of Misstatements Identified During the Audit*).

- effectiveness of management's responses and controls to address the risks.

- experience gained during previous audits with respect to similar potential misstatements.

- results of audit procedures performed, including whether such audit procedures identified specific instances of fraud or error.

- source and reliability of the available information.

- persuasiveness of the audit evidence.

- understanding of the entity and its environment, ***the applicable financial reporting framework, and*** ~~including~~ ~~it's~~ the ***entity's system of*** internal control.

Documentation (Ref: par. .30)

.A76 The form and extent of audit documentation is a matter of professional judgment and is influenced by the nature, size, and complexity of the entity; ***system of*** internal control of the entity; availability of information from the entity; and the audit methodology and technology used in the audit.

[No further amendment to AU-C section 330.]

AU-C section 402*, Audit Considerations Relating to an Entity Using a Service Organization*

.01 This section addresses the user auditor's responsibility for obtaining sufficient appropriate audit evidence in an audit of the financial statements of a user entity that uses one or more service organizations. Specifically, it expands on how the user auditor applies section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, and section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*, in obtaining an understanding of the user entity, including ***the entity's system of*** internal control relevant to ***the preparation of the financial statements*** ~~the audit~~, sufficient to identify and assess the risks of material misstatement and in designing and performing further audit procedures responsive to those risks.

[No amendment to paragraph .02.]

.03 Services provided by a service organization are relevant to the audit of a user entity's financial statements when those services and the controls over them affect the user entity's information system~~, including related business processes,~~ relevant to ~~financial reporting~~ ***the preparation of the financial statements***. ~~Although m~~***M***ost controls at the service organization are likely to ~~relate to financial reporting~~ ***be part of the user entity's information system relevant to the preparation of the financial statements or*** other ***related*** controls ~~also may be relevant to the audit~~, such as controls over the safeguarding of assets. A service organization's services are part of a user entity's information system~~,~~

~~including related business processes, relevant to financial reporting~~ if these services affect any of the following:

a. ***How information relating to significant classes of transactions, account balances, and disclosures flows through the user entity's information system, whether manually or using IT, and whether obtained from within or outside the general ledger and subsidiary ledgers.*** ~~The classes of transactions in the user entity's operations that are significant to the user entity's financial statements;~~ ***This includes when the service organization affects the following:***

~~*b.*~~***i.*** ~~The procedures within both IT and manual systems by which the user entity's transactions are initiated, authorized, recorded, processed, corrected as necessary, transferred to the general ledger, and reported in the financial statements;~~ ***How transactions of the user entity are initiated and how information about them is recorded, processed, corrected as necessary, and incorporated in the general ledger and reported in the financial statements***

ii. How information about events or conditions, other than transactions, is captured, processed, and disclosed by the user entity in the financial statements

~~*c.*~~ ***b.*** The ~~related~~ accounting records, ~~supporting information, and~~ specific accounts in the user entity's financial statements~~.~~***, and other supporting records relating to the flows of information in paragraph 3a.*** ~~that are used to initiate, authorize, record, process, and report the user entity's transactions. This includes the correction of incorrect information and how information is transferred to the general ledger; the records may be in either manual or electronic form;~~

~~*d.* How the user entity's information system captures events and conditions, other than transactions, that are significant to the financial statements;~~

~~*e c.*~~ The financial reporting process used to prepare the user entity's financial statements ***from the records described in paragraph .03b, including as it relates to disclosures and accounting estimates relating to significant classes of transactions, account balances, and disclosures*** ~~accounting estimates and disclosures; and~~

d. The entity's IT environment relevant to preceding subparagraphs (a)–(c)

~~*f.* Controls surrounding journal entries, including nonstandard journal entries used to record nonrecurring, unusual transactions, or adjustments.~~

[No amendment to paragraph .04–.06.]

.07 The objectives of the user auditor, when the user entity uses the services of a service organization, are to

a. obtain an understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's ***system of*** internal control ~~relevant to the audit~~, sufficient to ***provide an appropriate basis for the identification and assessment of*** ~~identify and assess~~ the risks of material misstatement.

b. design and perform audit procedures responsive to those risks.

[No amendment to paragraph .08–.09.]

.10 When obtaining an understanding of ***the entity's system of*** internal control relevant to the audit in accordance with section 315,[fn 1] the user auditor ***should identify controls in the control activities component*** ~~evaluate~~ ~~the design and implementation of relevant controls~~ at the user entity ***from those*** that relate to the services provided by the service organization, including those that are applied to the transactions processed by the service organization***, and evaluate their design and determine whether they have been implemented.*** [fn 2]

[fn 1] Paragraph .26a of AU-C section 315.

[fn 2] Paragraph .26b of AU-C section 315.

[Subsequent footnotes renumbered.]

.11 The user auditor should determine whether a sufficient understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's ***system of*** internal control ~~relevant to the audit~~ has been obtained to provide an ***appropriate*** basis for the identification and assessment of ***the*** risks of material misstatement.

.12 If the user auditor is unable to obtain a sufficient understanding from the user entity, the user auditor should obtain that understanding from one or more of the following procedures:

a. Obtaining and reading a type 1 or type 2 report, if available

b. Contacting the service organization, through the user entity, to obtain specific information

c. Visiting the service organization and performing procedures that will provide the necessary information about the ~~relevant~~ controls at the service organization

d. Using another auditor to perform procedures that will provide the necessary information about the relevant controls at the service organization (Ref: par. .A15–.A20)

[No amendment to paragraph .13.]

.14 If the user auditor plans to use a type 1 or type 2 report as audit evidence to support the user auditor's understanding about the design and implementation of controls at the service organization, the user auditor should

a. evaluate whether the type 1 report is as of a date, or in the case of a type 2 report, is for a period that is appropriate for the user auditor's purposes;

b. evaluate the sufficiency and appropriateness of the evidence provided by the report for the understanding of ~~the user entity's~~ ~~internal~~ ***controls at the service organization*** ~~relevant to the audit~~; and

c. determine whether complementary user entity controls identified by the service organization are relevant in addressing the risks of material misstatement relating to the relevant assertions in the user entity's financial statements and, if so, obtain an understanding of whether the user entity has designed and implemented such controls. (Ref: par. .A23–.A24)

[No amendment to paragraph .15–.A18.]

.A19 Another auditor may be used to perform procedures that will provide the necessary information about the relevant controls at the service organization ***related to services provided to the user entity***. If a type 1 or type 2 report has been issued, the user auditor may use the service auditor to perform these procedures as the service auditor has an existing relationship with the service organization. The user auditor using the work of another auditor may find the guidance in section 600, *Special Considerations — Audits of Group Financial Statements (Including the Work of Component Auditors)*, useful as it relates to understanding another auditor (including that auditor's independence and professional competence); involvement in the work of another auditor in planning the nature, extent, and timing of such work; and in evaluating the sufficiency and appropriateness of the audit evidence obtained. [fn 6]

[fn 6] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .A20–.A23.]

.A24 A type 1 or type 2 report, along with information about the user entity, may assist the user auditor in obtaining an understanding of the following:

a. The controls at the service organization that may affect the processing of the user entity's transactions, including the use of subservice organizations

b. The flow of significant transactions through the service organization's system to determine the points in the transaction flow where material misstatements in the user entity's financial statements could occur

c. The control objectives stated in the description of the service organization's system that are relevant to the user entity's financial statement assertions

d. Whether controls at the service organization are suitably designed and implemented to prevent, or detect and correct, processing errors that could result in material misstatements in the user entity's financial statements

A type 1 or type 2 report may assist the user auditor in obtaining a sufficient understanding to identify and assess the risks of material misstatement of the user entity's financial statements. A type 1 report, however, does not provide any evidence of the operating effectiveness of the ~~relevant~~ controls.

[No amendment to paragraphs .A25–.A30.]

.A31 The user auditor is required by section 330 to design and perform tests of controls to obtain sufficient appropriate audit evidence concerning the operating effectiveness of ~~relevant~~ controls in certain circumstances. [fn 8] In the context of a service organization, this requirement applies when

a. the user auditor's assessment of risks of material misstatement includes an expectation that the controls at the service organization are operating effectively (that is, the user auditor intends to rely on the operating effectiveness of controls at the service organization in determining the nature, timing, and extent of substantive procedures); or

b. substantive procedures alone, or in combination with tests of the operating effectiveness of controls at the user entity, cannot provide sufficient appropriate audit evidence at the assertion level.

[fn 8] [Footnote omitted for purposes of this proposed SAS.]

.A32 If a type 2 report is not available, a user auditor may contact the service organization through the user entity to request that a service auditor be engaged to perform a type 2 engagement that includes tests of the operating effectiveness of the ~~relevant~~ controls or the user auditor may use another auditor to perform agreed-upon procedures at the service organization that test the operating effectiveness of those controls. A user auditor may also visit the service organization and perform tests of ~~relevant~~ controls if the service organization agrees to it. The user auditor's risk assessments are based on the combined evidence provided by the service auditor's report and the user auditor's own procedures.

[No amendment to paragraphs .A33–.A34.]

.A35 It may also be necessary for the user auditor to obtain additional evidence about significant changes in the ~~relevant~~ controls at the service organization during a period outside the period covered by the type 2 report, or to determine what additional audit procedures need to be performed (for example, when little or no overlap exists between the period covered by the type 2 report and the period covered by the user entity's financial statements). Relevant factors in determining what additional audit evidence to obtain about controls at the service organization that were operating outside the period covered by the service auditor's report may include the following:

- The significance of the assessed risks of material misstatement at the assertion level

- The specific controls that were tested during the interim period and significant changes to them since they were tested including changes in the information systems, processes, and personnel

- The degree to which audit evidence about the operating effectiveness of those controls was obtained

- The length of the remaining period

- The extent to which the user auditor intends to reduce further substantive procedures based on the reliance on controls

- The effectiveness of the control environment and ***the user entity's process to*** monitor~~ing~~ ***the system of internal*** control~~s. at the user entity~~

.A36 Additional audit evidence may be obtained, for example, by performing tests of controls that operated during the remaining period or testing the user entity's ***process to*** monitor~~ing~~ ***the system of internal*** control~~s~~.

[No amendment to paragraphs .A37–.A40.]

.A41 *Communication of significant deficiencies and material weaknesses in internal control identified during the audit*. The user auditor is required by section 265, *Communicating Internal Control Related Matters Identified in an Audit*, to communicate in writing to management and those charged with governance significant deficiencies and material weaknesses identified during the audit. [fn 9] Matters related to the use of a service organization that the user auditor may identify during the audit and may communicate to management and those charged with governance of the user entity include the following:

- Any ***controls within the entity's process to monitor the system of internal control*** ~~needed monitoring controls~~ that could be implemented by the user entity, including those identified as a result of obtaining a type 1 or type 2 report

- Instances when complementary user entity controls identified in the type 1 or type 2 report are not implemented at the user entity

- Controls that may be needed at the service organization that do not appear to have been implemented or that were implemented, but are not operating effectively

[fn 9] [Footnote omitted for purposes of this proposed SAS.]

[No further amendment to AU-C section 402.]

AU-C section 501, *Audit Evidence — Specific Considerations for Selected Items*

[No amendment to paragraphs .01–.A22.]

.A23 Matters relevant in evaluating management's instructions and procedures for recording and controlling the physical inventory counting include whether they address, for example, the following:

- The application of appropriate control***s*** ~~activities~~ (for example, the collection of used physical inventory count records, accounting for unused physical inventory count records, and count and recount procedures)

- The accurate identification of the stage of completion of work in progress; slow moving, obsolete, or damaged items; and inventory owned by a third party (for example, on consignment)

- The procedures used to estimate physical quantities, when applicable, such as may be needed in estimating the physical quantity of a coal pile

- Control over the movement of inventory between areas and the shipping and receipt of inventory before and after the cutoff date

[No further amendment to AU-C section 501.]

AU-C section 530, *Audit Sampling*

[No amendment to paragraphs .01–.A9.]

.A10 In considering the test objective and characteristics of a population for tests of controls, the auditor makes an assessment of the expected rate of deviation based on the auditor's understanding of the ~~relevant~~ controls. This assessment is made in order to design an audit sample and determine sample size. For example, if the expected rate of deviation is unacceptably high, the auditor will normally decide not to perform tests of controls. Similarly, for tests of details, the auditor makes an assessment of the expected misstatement in the population. If the expected misstatement is high, 100 percent examination or increasing the sample size may be appropriate when performing tests of details.

[No further amendment to AU-C section 530.]

AU-C section 550, *Related Parties*

[No amendment to paragraphs .01–.A6.]

.A7 Matters that may be addressed in the discussion among the engagement team include the following:

- The nature and extent of the entity's relationships and transactions with related parties (using, for example, the auditor's record of identified related parties updated after each audit)

- An emphasis on the importance of maintaining professional skepticism throughout the audit regarding the potential for material misstatement associated with related party relationships and transactions

- The circumstances or conditions of the entity that may indicate the existence of related party relationships or transactions that management has not identified or disclosed to the auditor (for example, a complex organizational structure, use of entities formed to accomplish specific purposes, [fn 22] or an inadequate information system)

- The records or documents that may indicate the existence of related party relationships or transactions

- The importance that management and those charged with governance attach to the identification of, appropriate accounting for, and disclosure of related party relationships and transactions and the related risk of management override of ~~relevant~~ controls

[fn 22] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .A8–.A9.]

.A10 However, if the entity does not have such information systems in place, management may not be aware of the existence of all related parties. Nevertheless, the requirement to make the inquiries specified by paragraph .14 still applies because management may be aware of parties that meet the related party definition set out in GAAP. In such a case, however, the auditor's inquiries regarding the identity of the entity's related parties are likely to form part of the auditor's risk assessment procedures and related activities performed in accordance with section 315 to obtain information regarding ***the entity's organizational structure, ownership, governance, and business model.***[23] ~~the following:~~

- ~~The entity's ownership and governance structures~~

- ~~The types of investments that the entity is making and plans to make~~

- ~~The way the entity is structured and how it is financed~~

In the particular case of common control relationships, because management is more likely to be aware of such relationships if they have economic significance to the entity, the auditor's inquiries are likely to be more effective if they are focused on whether parties with which the entity engages in significant transactions or shares resources to a significant degree are related parties.

fn 23 [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .A11–.A20.]

.A21 *Considerations specific to smaller entities.* Control***s*** ~~activities~~ in smaller entities are likely to be less formal, and smaller entities may have no documented processes for dealing with related party relationships and transactions. An owner-manager may mitigate some of the risks arising from related party transactions or potentially increase those risks through active involvement in all the main aspects of the transactions. For such entities, the auditor may obtain an understanding of the related party relationships and transactions, and any controls that may exist over these, through inquiry of management combined with other procedures, such as observation of management's oversight and review activities and inspection of available relevant documentation.

[No amendment to paragraphs .A22–.A29.]

.A30 Relevant related party information shared with the engagement team members may include the following:

- The nature of the related party relationships and transactions
- Significant or complex related party relationships or transactions that may ***be associated with significant risks*** ~~require special audit consideration~~, particularly transactions in which management or those charged with governance are financially involved

The exchange of information is most useful if made at an early stage of the audit.

[No amendment to paragraphs .A31–.A37.]

.A38 Depending upon the results of the auditor's risk assessment procedures, the auditor may consider it appropriate to obtain audit evidence without testing the entity's controls over related party relationships and transactions. In some circumstances, however, it may not be possible to obtain sufficient appropriate audit evidence from substantive audit procedures alone, regarding the risks of material misstatement associated with related party relationships and transactions. For example, when intragroup transactions between the entity and its components are numerous and a significant amount of information regarding these transactions is initiated, authorized, recorded, processed, or reported electronically in an integrated system, the auditor may determine that it is not possible to design effective substantive audit procedures that by themselves would reduce the risks of material misstatement associated with these transactions to an acceptably low level. In such a case, in meeting the requirement of

section 330 to obtain sufficient appropriate audit evidence about the operating effectiveness of ~~relevant~~ controls, the auditor is required to test the entity's controls over the completeness and accuracy of the recording of the related party relationships and transactions.

[No further amendment to AU-C section 550.]

AU-C section 600, *Special Considerations — Audits of Group Financial Statements (Including the Work of Component* Auditors)

[No amendment to paragraphs .01–.19.]

.20 The auditor is required to identify and assess the risks of material misstatement through obtaining an understanding of the entity and its environment, ***the applicable reporting framework, and the system of internal control***.[fn 7] The group engagement team should

a. enhance its understanding of the group, its components, and their environments, including group-wide controls, obtained during the acceptance or continuance stage.

b. obtain an understanding of the consolidation process, including the instructions issued by group management to components. (Ref: par. .A31–.A37)

[fn 7] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .21–.A6.]

.A7 The group engagement team also may identify a component as likely to include significant risks of material misstatement of the group financial statements due to its specific nature or circumstances~~(that is, risks that require special audit consideration [fn14])~~. For example, a component could be responsible for foreign exchange trading and, thus, expose the group to a significant risk of material misstatement, even though the component is not otherwise of individual financial significance to the group.

[fn 14] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .A7–.A93.]

.A94 The examples provided cover a broad range of matters; however, not all matters are relevant to every group audit engagement, and the list of examples is not necessarily complete.

Group-Wide Controls

Group-wide controls may include a combination of the following:

- Regular meetings between group and component management to discuss business developments and review performance

- Monitoring of components' operations and their financial results, including regular reporting routines, which enables group management to monitor components' performance against budgets and take appropriate action

- Group management's risk assessment process (that is, the process for identifying, analyzing, and managing business risks, including the risk of fraud, that may result in material misstatement of the group financial statements)

- Monitoring, controlling, reconciling, and eliminating intragroup account balances, transactions, and unrealized profits or losses at group level

- A process for monitoring the timeliness and assessing the accuracy and completeness of financial information received from components

- A central IT system controlled by the same general IT controls for all or part of the group

- Control***s*** ~~activities~~ within an IT system that are common for all or some components

- ***Controls within the group's process to*** ~~M~~***m***onitor~~ing~~ ***the system of internal*** control~~s~~, including activities of the internal audit function and self-assessment programs

- Consistent policies and procedures, including a group financial reporting procedures manual

- Group-wide programs, such as codes of conduct and fraud prevention programs

- Arrangements for assigning authority and responsibility to component management

- The internal audit function may be regarded as part of group-wide controls, for example, when the function is centralized. Section 610, *Using the Work of Internal Auditors*, addresses the group engagement team's evaluation of whether the internal audit function's organizational status and relevant policies and procedures adequately support the objectivity of internal auditors, the level of competence of the internal audit function, and whether the function applies a systematic and disciplined approach when the group engagement team expects to use the function's work. [fn1]

[fn 1] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraph .A95.]

.A96 The following matters are relevant to the planning of the work of a component auditor:

[*Required matters are italicized.*]

- *A request for the component auditor, knowing the context in which the group engagement team will use the work of the component auditor, to confirm that the component auditor will cooperate with the group engagement team*

- The timetable for completing the audit

- Dates of planned visits by group management and the group engagement team and dates of planned meetings with component management and the component auditor

- A list of key contacts

- *The work to be performed by the component auditor, the use to be made of that work,* and arrangements for coordinating efforts at the initial stage of and during the audit, including the group engagement team's planned involvement in the work of the component auditor

- *The ethical requirements that are relevant to the group audit and, in particular, the independence requirements*

- *In the case of an audit or review of the financial information of the component, component materiality*

- *In the case of an audit or review of, or specified audit procedures performed on, the financial information of the component, the threshold above which misstatements cannot be regarded as clearly trivial to the group financial statements*

- *A list of related parties prepared by group management and any other related parties of which the group engagement team is aware and a request that the component auditor communicates on a timely basis to the group engagement team related parties not previously identified by group management or the group engagement team*

- Work to be performed on intragroup account balances, transactions, and unrealized profits or losses

- Guidance on other statutory reporting responsibilities (for example, reporting on group management's assertion on the effectiveness of internal control)

- When a time lag between completion of the work on the financial information of the components and the group engagement team's conclusion on the group financial statements is likely, specific instructions for a subsequent events review

The following matters are relevant to the conduct of the work of the component auditor:

- The findings of the group engagement team's tests of control***s*** ~~activities~~ of a processing system that is common for all or some components and tests of controls to be performed by the component auditor

…

[No further amendment to section 600.]

AU-C section 620*, Using the Work of an Auditor's Specialist*

[No amendment to paragraphs .01–.A4.]

.A5 An auditor's specialist may be needed to assist the auditor in one or more of the following:

- Obtaining an understanding of the entity and its environment, ***the applicable financial reporting framework, and*** ~~including~~ ***the entity's system of*** internal control

- Identifying and assessing the risks of material misstatement

- Determining and implementing overall responses to assessed risks at the financial statement level

- Designing and performing additional audit procedures to respond to assessed risks at the relevant assertion level, which may comprise tests of controls or substantive procedures

- Evaluating the sufficiency and appropriateness of audit evidence obtained in forming an opinion on the financial statements

[No further amendment to section 620.]

AU-C section 930*, Interim Financial Information*

[No amendment to paragraphs .01–.10.]

Procedures for a Review of Interim Financial Information

Understanding the Entity and Its Environment, ***the Applicable Financial Reporting Framework, and*** ~~Including Its~~ ***the Entity's System of*** Internal Control

.11 To plan and conduct the engagement, the auditor should have an understanding of the entity and its environment, ***the applicable financial reporting framework, and*** ~~including its~~ ***the entity's system of*** internal control as it relates to the preparation and fair presentation of both annual and interim financial information, sufficient to be able

to

a. identify the types of potential material misstatements in the interim financial information and consider the likelihood of their occurrence.

b. select the inquiries and analytical procedures that will provide the auditor with a basis for reporting whether the auditor is aware of any material modifications that should be made to the interim financial information for it to be in accordance with the applicable financial reporting framework.

[No amendment to paragraphs .12–.A6.]

Procedures for a Review of Interim Financial Information

Understanding the Entity and Its Environment, ***the Applicable Financial Reporting Framework,*** ~~Including It's the~~ ***and the Entity's System of*** Internal Control ***(Ref: par. .11–.12)***

.A7 As required by section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, the auditor who has audited the entity's financial statements for one or more annual periods would have obtained an understanding of the entity and its environment, ***the applicable financial reporting framework***, ~~including its~~ ***and the entity's system of*** internal control as it relates to the preparation and fair presentation of annual financial information, that was sufficient to conduct the audit. Internal control over the preparation and fair presentation of interim financial information may differ from internal control over the preparation and fair presentation of annual financial statements because certain accounting principles and practices used for interim financial information may differ from those used for the preparation of annual financial statements (for example, the use of estimated effective income tax rates for the preparation of interim financial information).

[No amendment to paragraphs .A8–.A10.]

Analytical Procedures, Inquiries, and Other Review Procedures

Analytical Procedures (Ref: par. .13)

.A11 Procedures for conducting a review of interim financial information generally are limited to analytical procedures, inquiries, and other procedures that address significant accounting and disclosure matters relating to the interim financial information. The auditor's understanding of the entity and its environment, ***the applicable financial reporting framework***, ***and*** ~~including its~~ ***the entity's*** ~~including its~~ ***system of*** internal control, the results of the risk assessments relating to the preceding audit, and the auditor's consideration of materiality as it relates to the interim financial information, influences the nature and extent of the inquiries made and analytical procedures performed. For example, if the auditor becomes aware of a significant change in the entity's control activities at a particular location, the auditor may consider the following procedures:

- Making additional inquiries, such as whether management monitored the changes and considered whether they were operating as intended

- Employing analytical procedures with a more precise expectation

[No further amendments to AU-C section 930.]

Amendment to SAS No. 128*, Using the Work of Internal Auditors* (AICPA*, Professional Standards*, AU-C sec. 610)

3. The amendment to AU-C section 610 is effective for audits of financial statements for periods ending on or after December 15, 2023.

AU-C section 610*, The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements*

[No amendment to paragraphs .01–.04.]

.05 Many entities establish internal audit functions as part of their internal control and governance structures. The objectives and scope of an internal audit function, the nature of its responsibilities, and its organizational status, including the function's authority and accountability, vary widely and depend on the size and structure of the entity and the requirements of management and those charged with governance. Section 315 addresses how the knowledge and experience of the internal audit function can inform the external auditor's understanding of the entity and its environment***, the applicable financial reporting framework, and the entity's system of internal control*** and identification and assessment of risks of material misstatement. Section 315[fn1] also explains how effective communication between the internal and external auditors creates an environment in which the external auditor can be informed by the internal auditor of significant matters that may affect the external auditor's work.

[fn1] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .06–.A2.]

.A3 However, those in the entity with operational and managerial duties and responsibilities outside of the internal audit function would ordinarily face threats to their objectivity that would preclude them from being treated as part of an internal audit function for the purpose of this section, although they may perform control***s*** ~~activities~~ that can be tested in accordance with section 330.[fn7] For this reason, monitoring controls performed by an owner-manager would not be considered equivalent to an internal audit function.

[fn 7] [Footnote omitted for purposes of the proposed SAS.]

[No amendment to paragraphs .A4–.A11.]

.A12 The application of a systematic and disciplined approach to planning, performing, supervising, reviewing, and documenting its activities distinguishes the activities of the internal audit function from other monitoring control***s*** ~~activities~~ that may be performed within the entity.

[No amendment to paragraphs .A13–.A25.]

.A26 As explained in section 315, [fn 11] significant risks ~~require special audit consideration~~ ***are risks assessed close to the upper end of the spectrum of inherent risk*** and, therefore, the external auditor's ability to use the work of the internal audit function in relation to significant risks will be restricted to procedures that involve limited judgment. In addition, when the risks of material misstatement is other than low, the use of the work of the internal audit function in obtaining audit evidence alone is unlikely to reduce audit risk to an acceptably low level and eliminate the need for the external auditor to perform some tests directly.

[fn 11] [Footnote omitted for purposes of this SAS.]

[No further amendment to section 610.]

Amendment to SAS No. 130*, An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements,* as Amended (AICPA*, Professional Standards,* AU-C sec. 940)

4. The amendment to AU-C section 940 is effective for audits of financial statements for periods ending on or after December 15, 2023.

AU-C section 940*, An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements*

[No amendment to paragraphs .01–.25.]

.26 The auditor should identify significant classes of transactions, account balances, and disclosures, and their relevant assertions. To identify significant classes of transactions, account balances, and disclosures, and their relevant assertions, the auditor should evaluate the ~~qualitative and quantitative~~ ***inherent*** risk factors[fn 6] related to the financial statement line items and disclosures. (Ref: par. .A50–.A52)

[fn 6] See paragraph 12 of the proposed SAS **Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.**

[No amendment to paragraphs .27–.30. Subsequent footnotes renumbered.]

.31 The auditor should understand how IT affects the entity's flow of transactions and, as required by the proposed SAS *Understanding the Entity and Its Environment and*

Assessing the Risks of Material Misstatement, ~~how the entity has responded to~~ ***the entity's general information technology (IT) controls that address the*** risks arising from ***the use of*** IT. [fn 6] (Ref: par. .A58)

[fn 6] Paragraph ~~22~~ ***26c*** of ~~section 315~~ ***the proposed SAS*** *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*.

[No amendment to paragraphs .32–.56.]

.57 In an audit of ICFR, the auditor should obtain written representations from management

a. acknowledging management's responsibility for ~~establishing~~ ***designing, implementing,*** and maintaining effective ICFR;

b. stating that management has performed an assessment of the effectiveness of the entity's ICFR and specifying the criteria;

c. stating that management did not use the auditor's procedures performed during the integrated audit as part of the basis for management's assessment about ICFR;

d. stating management's assessment about the effectiveness of the entity's ICFR based on the criteria as of a specified date;

e. stating that management has disclosed to the auditor all deficiencies in the design or operation of ICFR, including separately disclosing to the auditor all such deficiencies that it believes to be significant deficiencies or material weaknesses;

f. describing any fraud resulting in a material misstatement to the entity's financial statements and any other fraud that does not result in a material misstatement to the entity's financial statements, but involves senior management or management or other employees who have a significant role in the entity's ICFR;

g. stating whether the significant deficiencies and material weaknesses identified and communicated to management and those charged with governance during previous engagements pursuant to paragraph .59 have been resolved and specifically identifying any that have not; and

h. stating whether there were, subsequent to the date being reported on, any changes in ICFR or other conditions that might significantly affect ICFR, including any corrective actions taken by management with regard to significant deficiencies and material weaknesses (Ref: par. .A103)

[No amendment to paragraphs .58–.A6.]

.A6 For purposes of a financial statement audit, the proposed SAS **Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** ***defines the term*** **system of internal control** ***and recognizes that internal control***

frameworks may use different terms that are similar to the concept of the system of internal control. This section defines the term **internal control over financial reporting*****, which is a system of internal control, to more clearly define ICFR for purposes of expressing an opinion on the effectiveness of ICFR, based on suitable and available criteria.***

[Former paragraphs .A6–.A158 are renumbered as paragraphs .A7–.A159.]

[No amendment to paragraphs .07–.A20.]

.A21 Evaluating whether the following matters are important to the entity's financial statements and ICFR and, if so, how they may affect the auditor's procedures may assist the auditor in planning the audit of ICFR:

- Knowledge of the entity's ICFR obtained during other engagements performed by the auditor or, if applicable, during a review of a predecessor auditor's working papers
- Matters affecting the industry in which the entity operates, such as financial reporting practices, economic conditions, laws and regulations, and technological changes
- Matters relating to the entity's business, including its organization, operating characteristics, and capital structure
- The extent of recent changes, if any, in the entity, its operations, or its ICFR
- The auditor's preliminary judgments about financial statement materiality, risk, and other factors relating to the determination of material weaknesses
- Deficiencies previously communicated to those charged with governance or management
- Legal or regulatory matters of which the entity is aware
- The type and extent of available evidence related to the effectiveness of the entity's ICFR
- Preliminary judgments about the effectiveness of ICFR
- Public information about the entity relevant to the evaluation of the likelihood of material financial statement misstatements and the effectiveness of the entity's ICFR
- Knowledge about risks related to the entity evaluated as part of the auditor's ***procedures regarding acceptance or continuance of the*** client ***relationship or the integrated audit engagement*** ~~acceptance and retention evaluation.~~

- The relative complexity of the entity's operations

[No amendment to paragraphs .A22–.A24.]

.A25 Section 240 addresses the auditor's identification and assessment of the risks of material misstatement due to fraud. [fn14] Controls that might address these risks include

- controls over significant unusual transactions, particularly those that result in late or unusual journal entries;
- controls over journal entries and adjustments made in the period-end financial reporting process;
- controls over related party transactions;
- controls related to significant ~~management~~ ***accounting*** estimates; and
- controls that mitigate incentives for, and pressures on, management to falsify or inappropriately manage financial results.

[fn 14] [Footnote omitted for purposes of this proposed SAS.]

.A26 The extent of the procedures necessary to obtain the understanding required by paragraph .18 will vary, depending on the nature of those activities. In performing risk assessment procedures, the auditor is required to inquire of appropriate individuals within the internal audit function (if such function exists). [fn 15] Section 315 provides guidance with respect to such inquiries and certain additional procedures based on the responses to such inquiries. [fn 16]

[fn 15] Paragraph ~~.06*a*~~ ***.14*** of section 315. [Footnote renumbered by the issuance of SAS No. 140, April 2020.]

[fn 16] Paragraph ~~.A9–.A13~~.***A25 and appendix D*** of the proposed SAS. [Footnote renumbered by the issuance of SAS No. 140, April 2020.]

[No amendment to paragraphs .A26–.A32.]

.A33 A top-down approach involves

- beginning at the financial statement level;
- using the auditor's understanding of the overall risks to ICFR;
- focusing on entity-level controls;
- working down to significant classes of transactions, account balances, and disclosures, and their relevant assertions***, which directs attention to classes of***

transactions, accounts, disclosures, and assertions that present a reasonable possibility of material misstatement of the financial statements;

- ~~directing attention to classes of transactions, accounts, disclosures, and assertions that present a reasonable possibility of material misstatement of the financial statements;~~

- verifying the auditor's understanding of the risks in the entity's processes; and

- selecting controls for testing that sufficiently address the assessed risk of material misstatement to each relevant assertion.

[No amendment to paragraphs .A34–.A49.]

.A50 ***Inherent*** risk factors ***are*** relevant to the identification of significant classes of transactions, account balances, and disclosures, and their relevant assertions ~~include~~**.** ***Inherent risk factors may be qualitative or quantitative and affect the susceptibility of assertions to misstatement. Inherent risk factors are described in section 315***.

- ~~size and composition of the account;~~

- ~~susceptibility to misstatement due to errors or fraud;~~

- ~~volume of activity, complexity, and homogeneity of the individual transactions processed through the account or reflected in the disclosure;~~

- ~~nature of the account, class of transactions, or disclosure;~~

- ~~accounting and reporting complexities associated with the account, class of transactions, or disclosure;~~

- ~~exposure to losses in the account;~~

- ~~possibility of significant contingent liabilities arising from the activities reflected in the account or disclosure;~~

- ~~existence of related party transactions in the account; and~~

- ~~changes from the prior period in the account, class of transactions, or disclosure characteristics.~~

.A51 The ***inherent*** ~~R~~***r***isk factors ~~in paragraph .26~~ that the auditor is required to evaluate in the identification of significant classes of transactions, account balances, and disclosures, and their relevant assertions, are the same in the audit of ICFR as in the audit of the financial statements; accordingly, significant classes of transactions,

account balances, and disclosures, and their relevant assertions, are the same in an integrated audit.

Amendment to SAS No. 134, *Auditor Reporting and Amendments, Including Amendments Addressing Disclosures in the Audit of Financial Statements*, as Amended, and Section 701, *Communicating Key Audit Matters in the Independent Auditor's Report* (AICPA, Professional Standards, AU-C sec. 701)

5. The amendment to AU-C section 701 is effective for audits of financial statements for periods ending on or after December 15, 2023.

AU-C section 701, *Communicating Key Audit Matters in the Independent Auditor's Report*

[No amendment to paragraphs .01 –.A17]

.A18 Section 315 defines a *significant risk* as an identified ~~and assessed~~ risk of material misstatement ***for which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk due to the degree to which the inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur*** ~~that, in the auditor's judgment, requires special audit consideration.~~[fn 13] Areas of significant management judgment and significant unusual transactions may often be identified as significant risks. Significant risks are therefore often areas that require significant auditor attention.

[fn 13] ***See paragraph .13 of AU-C section 315,* Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.**

[Subsequent footnotes renumbered.]

[No further amendment to section 701.]

Amendment to SAS No. 137, *The Auditor's Responsibilities Relating to Other Information Included in Annual Reports*, as Amended (AICPA, *Professional Standards*, AU-C sec. 720)

6. The amendment to AU-C section 720 is effective for audits of financial statements for periods ending on or after December 15, 2023.

AU-C section 720, *Other Information in Documents Containing Audited Financial Statements*

[No amendment to paragraphs .01–.A33.]

.A34 The auditor's knowledge obtained in the audit includes the auditor's understanding of the entity and its environment, ***the applicable financial reporting framework, and*** ~~including~~ the entity's ***system of*** internal control, obtained in accordance with section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.*[fn 9] Section 315 sets out the auditor's required understanding, which includes such matters as obtaining an understanding of the following:

a. ***The entity's organizational structure, ownership and governance, and its business model, including the extent to which the business model integrates the use of IT***

~~*a.*~~***b.*** The relevant industry, regulatory, and other external factors

~~*b. The nature of the entity*~~

~~*c. The entity's selection and application of accounting policies*~~

~~*d. The entity's objectives and strategies*~~

~~*e.*~~***c.*** The ***relevant measures used, internally and externally, to assess*** ~~measurement and review of~~ the entity's financial performance

~~*f.*~~***d.*** The entity's internal control

[fn 9] [Footnote omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .A35–.A54.]

.A55 In reading the other information, the auditor may become aware of new information that has implications for the following:

- The auditor's understanding of the entity and its environment, ***the financial reporting framework, and the entity's system of internal control,*** which may indicate the need to revise the auditor's risk assessment [fn 12]

- The auditor's responsibility to evaluate the effect of identified misstatements on the audit and of uncorrected misstatements, if any, on the financial statements [fn 13]

- The auditor's responsibilities relating to subsequent events

[fn 12 and fn 13] [Footnotes omitted for purposes of this proposed SAS.]

[No further amendment to section 720.]

Amendment to SAS No. 143, *Auditing Accounting Estimates and Related Disclosures* (AICPA, *Professional Standards*, AU-C sec. 540)

7. The amendment to AU-C section 540 is effective for audits of financial statements for periods ending on or after December 15, 2023.

AU-C section 540, *Auditing Accounting Estimates and Related Disclosures*

[No amendment to paragraphs .01–.03.]

Key Concepts of This Section

.04 AU-C section 315 requires ***inherent risk and control risk to be assessed separately for identified risks of material misstatement*** ~~the auditor to assess the risk of material misstatement~~ at the relevant assertion level. ~~For this purpose, this SAS requires inherent risk and control risk to be assessed separately for accounting estimates.~~ ***In the context of this section and depending*** on the nature of a particular accounting estimate, the susceptibility of an assertion to a misstatement that could be material may be subject to or affected by estimation uncertainty, complexity, subjectivity, or other inherent risk factors, and the interrelationship among them. As explained in AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards*,[fn 2] inherent risk is ***influenced by inherent risk factors.*** ~~higher for some assertions and related classes of transactions, account balances, and disclosures than for others.~~ Accordingly, the assessment of inherent risk depends on the degree to which the inherent risk factors affect the ***susceptibility to misstatement of an assertion, and the level of inherent risk*** ~~likelihood or magnitude of misstatement and~~ varies on a scale that is referred to ~~in this SAS~~ as the *spectrum of inherent risk*. In assessing control risk, the auditor takes into account whether the auditor's further audit procedures contemplate planned reliance on the operating effectiveness of controls. If the auditor does not ***intend to test and rely on the operating effectiveness of controls,*** ~~perform tests of controls,~~ the auditor's assessment of ***control risk is such that the assessment of the risk of material misstatement is the same as the assessment of inherent risk.*** ~~the risk of material misstatement at the relevant assertion level cannot be reduced for the effective operation of controls with respect to the particular assertion~~. (Ref: par. .A8–.A10, .A65–.A66, and app. A)

[fn 2] [Footnote omitted for purposes of this proposed SAS.]

.05 This section refers to relevant requirements in AU-C sections 315 and 330 and provides related guidance to emphasize the importance of the auditor's decisions about controls relating to accounting estimates, including decisions about whether

- there are controls ***identified in accordance with paragraph .27 of AU-C section 315***~~relevant to the audit~~, for which the auditor is required to evaluate their design and determine whether they have been implemented.

- to test the operating effectiveness of ~~relevant~~ controls.

[No amendment to paragraph .06.]

.07 The exercise of professional skepticism in relation to accounting estimates is affected by the auditor's consideration of inherent risk factors, and its importance increases when accounting estimates are subject to a greater degree of estimation uncertainty or are affected to a greater degree by complexity, subjectivity, or other inherent risk factors. Similarly, the exercise of professional skepticism is important when there is greater susceptibility to misstatement due to management bias or ***other*** fraud ***risk factors insofar as they affect inherent risk***. (Ref: par. .A11)

.08 This section requires the auditor to evaluate, based on the audit procedures performed and the audit evidence obtained, whether the accounting estimates and related disclosures are reasonable [fn 3] in the context of the applicable financial reporting framework or are misstated. For purposes of this section, *reasonable*, in the context of the applicable financial reporting framework, means that the relevant requirements of the applicable financial reporting framework have been applied appropriately, including those that address the following: (Ref: par. .A12–.A13 and .A139–.A144)

- The development of the accounting estimate, including the selection of the method, assumptions, and data in view of the nature of the accounting estimate and the facts and circumstances of the entity

- The selection of management's point estimate

- The disclosures about the accounting estimate, including disclosures about how the accounting estimate was developed and that explain the nature, extent, and sources of estimation uncertainty

[fn 3] [Footnote omitted for purposes of this proposed SAS.]

[No proposed amendment to paragraphs .09–.11.]

Requirements

Risk Assessment Procedures and Related Activities

.12 When obtaining an understanding of the entity and its environment, ***the applicable financial reporting framework, and*** ~~including~~ the entity's ***system of*** internal control, as required by AU-C section 315, the auditor should obtain an understanding of the

following matters related to the entity's accounting estimates. The auditor's procedures to obtain the understanding should be performed to the extent necessary to ***obtain audit evidence that*** provide***s*** an appropriate basis for the identification and assessment of risks of material misstatement at the financial statement and relevant assertion levels [fn 4] (Ref: par. .A19–.A23)

[fn 4] [Footnote omitted for purposes of this proposed SAS.]

Obtaining an Understanding of the ~~The~~ Entity and Its Environment ***and the Applicable Financial Reporting Framework***

a. The entity's transactions and other events ***or*** ~~and~~ conditions that may give rise to the need for or changes in accounting estimates to be recognized or disclosed in the financial statements (Ref: par. .A24)

b. The requirements of the applicable financial reporting framework related to accounting estimates (including the recognition criteria, measurement bases, and the related presentation and disclosure requirements) and how they apply in the context of the nature and circumstances of the entity and its environment, including how ~~transactions and other events or conditions are subject to or affected by~~ ***the*** inherent risk factors ***affect susceptibility to misstatement of assertions***. (Ref: par. .A25–.A26)

c. Regulatory factors relevant to the entity's accounting estimates, including, when applicable, regulatory frameworks (Ref: par. .A27)

d. The nature of the accounting estimates and related disclosures that the auditor expects to be included in the entity's financial statements, based on the auditor's understanding of the matters in paragraph .12*a–c* of this section (Ref: par. .A28)

Obtaining an Understanding of the ~~The~~ Entity's ***System of*** Internal Control

e. The nature and extent of oversight and governance that the entity has in place over management's financial reporting process relevant to accounting estimates (Ref: par. .A29–.A31)

f. How management identifies the need for and applies specialized skills or knowledge related to accounting estimates, including with respect to the use of a management's specialist (Ref: par. .A32)

g. How the entity's risk assessment process identifies and addresses risks relating to accounting estimates (Ref: par. .A33–.A34)

h. The entity's information system as it relates to accounting estimates, including the following:

i. ***How information relating to accounting estimates and related disclosures for significant classes of transactions, account balances, or disclosures flows through the entity's information system*** ~~The classes of transactions, events, and conditions that are significant to the financial statements and that give rise to the need for or changes in accounting estimates and related disclosures~~ (Ref: par. .A20 and .A35)

ii. For such accounting estimates and related disclosures, how management

(1) identifies the relevant methods, assumptions, or sources of data, and the need for changes in them, that are appropriate in the context of the applicable financial reporting framework, including how management (Ref: par. .A36– .A37)

(a) selects or designs, and applies, the methods used, including the use of models (Ref: par. .A38–.A39)

(b) selects the assumptions to be used, including consideration of alternatives, and identifies significant assumptions (Ref: par. .A40–.A43)

(c) selects the data to be used (Ref: par. .A44)

(2) understands the degree of estimation uncertainty, including by considering the range of possible measurement outcomes (Ref: par. .A45)

(3) addresses the estimation uncertainty, including selecting a point estimate and related disclosures for inclusion in the financial statements (Ref: par. .A46–.A49)

i. ***Identified controls in the control activities component*** [fn 5] ~~Control activities relevant to the audit~~ over management's process for making accounting estimates as described in paragraph .12*h*(ii) of this section (Ref: par. .A50–.A54)

j. How management reviews the outcomes of previous accounting estimates and responds to the results of that review

[fn 5] Paragraph 26a(i)–(iv) of proposed SAS Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.

[No proposed amendment to paragraphs .13–.14. Subsequent footnotes renumbered.]

Identifying and Assessing the Risks of Material Misstatement

.15 In identifying and assessing the risks of material misstatement relating to an accounting estimate and related disclosures at the relevant assertion level, ***including separately assessing inherent risk and control risk at the relevant assertion level,*** as required by AU-C section 315, [fn 6] the auditor should ~~separately assess inherent risk and control risk. The auditor should~~ take the following into account in identifying the risks of material misstatement and assessing inherent risk: (Ref: par. .A64–.A71)

a. The degree to which the accounting estimate is subject to estimation uncertainty (Ref: par. .A72–.A75)

b. The degree to which one or both of the following are affected by complexity, subjectivity, or other inherent risk factors: (Ref: par. .A76–.A79)

i. The selection and application of the method, assumptions, and data in making the accounting estimate

ii. The selection of management's point estimate and related disclosures for inclusion in the financial statements

fn 6 Paragraphs .31–.34 of proposed SAS **Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and its Environment**.

.16 The auditor should determine whether any of the risks of material misstatement identified and assessed in accordance with paragraph .15 are, in the auditor's judgment, a significant risk. [fn 6] If the auditor has determined that a significant risk exists, the auditor should ***identify controls that address*** ~~obtain an understanding of the entity's controls, including control activities, relevant to~~ that risk [***fn 7***] and ~~, based on that understanding,~~ evaluate whether such controls have been suitably designed and implemented to mitigate such risks. [fn 8] (Ref: par. .A80)

[fn 6] Paragraph .***32***~~28~~ of AU-C section 315.

[***fn 7***] ***Paragraph .26a(i) of AU-C section 315***.

[fn 8] Paragraph ***.26a***~~.30~~ of AU-C section 315.

[Subsequent footnotes renumbered]

Responses to the Assessed Risks of Material Misstatement

[No proposed amendment to paragraphs .17]

.18 As required by AU-C section 330, [fn 11] the auditor should design and perform tests to obtain sufficient appropriate audit evidence about the operating effectiveness of ~~relevant~~ controls, if

a. the auditor's assessment of risks of material misstatement at the relevant assertion level includes an expectation that the controls are operating effectively, or

b. substantive procedures alone cannot provide sufficient appropriate audit evidence at the relevant assertion level.

In relation to accounting estimates, the auditor's tests of such controls should be responsive to the reasons for the assessment given to the risks of material misstatement. In designing and performing tests of controls, the auditor should obtain more persuasive

audit evidence the greater the reliance the auditor places on the effectiveness of a control. [fn 12] (Ref: par. .A85–.A89)

[fn 11 and 12] [Footnotes omitted for purposes of this proposed SAS.]

[No amendment to paragraphs .19–.A7.]

Application and Other Explanatory Material

…

Key Concepts of This Section

***Inherent Risk Factors* (Ref: par. .00)**

.A8 *Inherent risk factors* are characteristics of ~~conditions and~~ events ***or conditions*** that ~~may~~ affect ~~the~~ susceptibility ~~of an assertion~~ to misstatement***, whether due to fraud or error, of an assertion about a class of transactions, account balance, or disclosure,*** before consideration of controls. ***[fn 25]*** Appendix A, "Inherent Risk Factors," further explains the nature of these inherent risk factors, and their interrelationships, in the context of making accounting estimates and their presentation in the financial statements.

[fn 25] Paragraph .12 of AU-C section 315. [Subsequent footnotes renumbered.]

.A9 ~~In addition to the inherent risk factors of estimation uncertainty, complexity, or subjectivity, other inherent risk factors that the auditor may consider in identifying and~~ ***When*** assessing the risks of material misstatement ***at the assertion level [fn26] in addition to estimation uncertainty, complexity, and subjectivity, the auditor also takes into account the degree*** ~~may include the extent~~ to which ***other inherent risk factors included in AU-C section 315 affect susceptibility of assertions to misstatement about*** the accounting estimate. ***Such additional inherent risk factors include the following:*** ~~is subject to or affected by~~

- ***A*** change in the nature or circumstances of the relevant financial statement items, or requirements of the applicable financial reporting framework, which may give rise to the need for changes in the method, assumptions, or data used to make the accounting estimate~~.~~

- ***S***usceptibility to misstatement due to management bias or ***other*** fraud ***risk factors insofar as they affect inherent risk,*** in making the accounting estimate~~.~~

- ***Uncertainty, other than estimation uncertainty***

[fn 26] Paragraph .31 of AU-C section 315.

Control Risk

.A10 ~~An important consideration for the auditor in~~ ***In*** assessing control risk at the relevant

assertion level ***in accordance with AU-C section 315, the auditor takes into account*** ~~is the effectiveness of the design of the controls that~~ ***whether*** the auditor ~~intends~~ ***plans*** to ~~rely on~~ ***test the operating effectiveness of controls.*** ~~and the extent to which the controls address the assessed inherent risks at the relevant assertion level.~~ ***When the auditor is considering whether to test the operating effectiveness of controls, the*** ~~The~~ auditor's evaluation that controls are effectively designed and have been implemented supports an expectation***, by the auditor,*** about the operating effectiveness of the controls in ~~determining whether~~ ***establishing the plan*** to test them.

[No amendment to paragraphs .A11–.A18. Paragraph .A20, .A22–.A23, .A26–.A27, and .A30–.A33 have been included for contextual purposes.]

Risk Assessment Procedures and Related Activities

Obtaining an Understanding of the Entity and Its Environment, **the Applicable Financial Reporting Framework, and the Entity's System of Internal Control (Ref: par. .12)**

.A19 AU-C section 315 [24] requires the auditor to obtain an understanding of certain matters about the entity and its environment, ***the applicable financial reporting framework, and*** ~~including~~ the entity's ***system of*** internal control. The requirements in paragraph .12 of this section relate more specifically to accounting estimates and build on the broader requirements in AU-C section 315.

[24] [Footnote omitted for purposes of this proposed SAS.]

.A20 The classes of transactions, events, and conditions within the scope of paragraph .12*h* of this section are the same as the classes of transactions, events, and conditions relating to accounting estimates and related disclosures that are subject to AU-C section 315. [25] In obtaining the understanding of the entity's information system as it relates to accounting estimates, the auditor may consider

- whether the accounting estimates arise from the recording of routine and recurring transactions or whether they arise from nonrecurring or unusual transactions.
- how the information system addresses the completeness of accounting estimates and related disclosures, in particular, for accounting estimates related to liabilities.

[25] [Footnote omitted for purposes of this proposed SAS.]

Scalability

.A21 The nature, timing, and extent of the auditor's procedures to obtain the understanding of the entity and its environment, ~~including~~ ***the applicable financial reporting framework, and*** the entity's ***system of*** internal control, related to the entity's accounting estimates, may depend, to a greater or lesser degree, on the extent to which the individual matters apply in the circumstances. For example, the entity may have few transactions or other events ***or*** ~~and~~ conditions that give rise to the need for accounting

estimates; the applicable financial reporting requirements may be simple to apply; and there may be no relevant regulatory factors. Further, the accounting estimates may not require significant judgments, and the process for making the accounting estimates may be less complex. In these circumstances, the accounting estimates may be subject to or affected by estimation uncertainty, complexity, subjectivity, or other inherent risk factors to a lesser degree, and there may be fewer ***identified*** controls ***in the control activities component.*** ~~relevant to the audit.~~ If so, the auditor's risk assessment procedures are likely to be less extensive and may be performed primarily through inquiries of management with appropriate responsibilities for the financial statements***, such as*** ~~and~~ observation of management's process for making the accounting estimate ***(including when evaluating whether identified controls in that process are designed effectively and when determining whether the control has been implemented)***.

[No proposed amendment to paragraphs .A22–.A23.]

The Entity and Its Environment

The Entity's Transactions and Other Events ***or*** ~~and~~ Conditions (Ref: par. .12*a*)

.A24 Changes in circumstances that may give rise to the need for or changes in accounting estimates may include, for example, whether

- the entity has engaged in new types of transactions,
- terms of transactions have changed, or
- new events or conditions have occurred.

The Requirements of the Applicable Financial Reporting Framework (Ref: par. .12*b*)

.A25 Obtaining an understanding of the requirements of the applicable financial reporting framework provides the auditor with a basis for discussion with management and, where applicable, those charged with governance about how management has applied ***the*** ~~those~~ requirements ***of the applicable financial reporting framework*** relevant to the accounting estimates, and about the auditor's determination of whether they have been applied appropriately. This understanding also may assist the auditor in communicating with those charged with governance when the auditor considers a significant accounting practice that is acceptable under the applicable financial reporting framework to not be the most appropriate in the circumstances of the entity. [fn 26]

[fn 26] [Footnote omitted for purposes of this proposed SAS.]

[No proposed amendment to paragraphs .A26–.A28.]

The Entity's ***System of*** *Internal Control* ~~*Relevant to the Audit*~~

The Nature and Extent of Oversight and Governance (Ref: par. .12*e*)

.A29 In applying AU-C section 315[fn 27] the auditor's understanding of the nature and extent of oversight and governance that the entity has in place over management's process for making accounting estimates may be important to the auditor's required evaluation ***about*** ~~as it relates to~~ whether

- management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior, and
- the ~~strengths in the~~ control environment ~~elements collectively provide~~ ***provides*** an appropriate foundation for the other components of ***the system of*** internal control ***considering the nature and size of the entity,*** and
- ~~whether those other components are undermined by~~ ***control*** deficiencies ***identified*** in the control environment ***undermine the other components of the system of internal control***.

[27] Paragraph .***21a***~~15~~ of AU-C section 315.

[No proposed amendment to paragraphs .A30–.A34.]

The Entity's Information System Relating to Accounting Estimates (Ref: par. .12*h*(i))

.A35 During the audit, the auditor may identify classes of transactions, events, ***or***~~and~~ conditions that give rise to the need for accounting estimates and related disclosures that management failed to identify. AU-C section 315 addresses circumstances in which the auditor identifies risks of material misstatement that management failed to identify, including ***considering the implications for the auditor's evaluation of*** ~~determining whether there is a significant deficiency or material weakness in internal control with regard to~~ the entity's risk assessment process. [fn 30]

[fn 30] [Footnote omitted for purposes of this proposed SAS.]

[No proposed amendment to paragraphs .A36–.A38.]

Models

.A39 Management may design and implement specific controls around models used for making accounting estimates, whether it's management's own model or an external model. When the model itself has an increased level of complexity or subjectivity, such as an expected credit loss model or a fair value model using level 3 inputs, controls that address such complexity or subjectivity may be more likely to be identified as relevant to the audit. When complexity in relation to models is present, controls over data integrity are also more likely to be ***identified controls in accordance with paragraph .27 of AU-C section 315***~~relevant to the audit~~. Factors that may be appropriate for the auditor

to consider in obtaining an understanding of the model and ***related identified controls*** ~~control activities relevant to the audit~~ include the following:

- How management determines the relevance and accuracy of the model.
  - — The validation or back-testing of the model, including whether the model is validated prior to use and revalidated at regular intervals to determine whether it remains suitable for its intended use. The entity's validation of the model may include evaluation of
    - o the model's theoretical soundness,
    - o the model's mathematical integrity, and
    - o the accuracy and completeness of the data and the appropriateness of data and assumptions used in the model.
- How the model is appropriately changed or adjusted on a timely basis for changes in market or other conditions and whether there are appropriate change control policies over the model.
- Whether adjustments, also referred to as *overlays* in certain industries, are made to the output of the model and whether such adjustments are appropriate in the circumstances in accordance with the requirements of the applicable financial reporting framework. When the adjustments are not appropriate, such adjustments may be indicators of possible management bias.
- Whether the model is adequately documented, including its intended applications, limitations, key parameters, required data and assumptions, and the results of any validation performed on it and the nature of and basis for any adjustments made to its output.

Examples of valuation models may include the present value of expected future cash flows, option-pricing models, matrix pricing, option-adjusted spread models, and fundamental analysis.

[No amendment to paragraphs .A40–.A43.]

Data (Ref: par. .12*h*(ii)(1)(c))

.A44 Matters that the auditor may consider in obtaining an understanding of how management selects the data on which the accounting estimates are based include the following:

- The nature and source of the data, including information obtained from an external information source
- How management evaluates whether the data is appropriate

- The accuracy and completeness of the data
- The consistency of the data used with data used in previous periods
- The complexity of the IT ***applications or other aspects of the entity's IT environment*** ~~systems~~ used to obtain and process the data, including when this involves handling large volumes of data
- How the data is obtained, transmitted, and processed and how its integrity is maintained

[No amendments to paragraphs .A45–.A49.]

Identified Controls ~~Control Activities Relevant to the Audit~~ Over Management's Process for Making Accounting Estimates (Ref: par. .12*i*)

.A50 The auditor's judgment in identifying controls ~~relevant to the audit~~ ***in the control activities component*** and, therefore, the need to evaluate the design of those controls and determine whether they have been implemented, relates to management's process described in paragraph .12*h*(ii). The auditor may not identify ***controls*** ~~relevant control activities~~ in relation to all ~~the elements~~ ***aspects*** of paragraph .12*h*(ii)**.** ~~, depending on the complexity associated with the accounting estimate.~~

.A51 As part of ~~obtaining an understanding of~~ ***identifying*** the ***controls*** ~~control activities relevant to the audit~~, the auditor may consider the following:

- How management determines the appropriateness of the data used to develop the accounting estimates, including when management uses an external information source or data from outside the general and subsidiary ledgers.
- The review and approval of accounting estimates, including the assumptions or data used in their development, by appropriate levels of management and, where appropriate, those charged with governance.
- The segregation of duties between those responsible for making the accounting estimates and those committing the entity to the related transactions, including whether the assignment of responsibilities appropriately takes account of the nature of the entity and its products or services. For example, in the case of a large financial institution, relevant segregation of duties may consist of an independent function responsible for estimation and validation of fair value pricing of the entity's financial products staffed by individuals whose remuneration is not tied to such products.
- The effectiveness of the design of the ***controls*** ~~control activities~~. Generally, it may be more difficult for management to design controls that address subjectivity and estimation uncertainty in a manner that effectively prevents, or detects and corrects, material misstatements than it is to design controls that address

complexity. Controls that address subjectivity and estimation uncertainty may need to include more manual elements, which may be less reliable than automated controls as they can be more easily bypassed, ignored, or overridden by management. The design effectiveness of controls addressing complexity may vary depending on the reason for and the nature of the complexity. For example, it may be easier to design more effective controls related to a method that is routinely used or over the integrity of data.

.A52 When management makes extensive use of IT in making an accounting estimate, ***identified*** controls ~~relevant to the audit~~ ***in the control activities component*** are likely to include general IT controls and ~~application~~ ***information-processing*** controls. Such controls may address risks related to the following:

- Whether the IT ***application or other aspects of the IT environment*** ~~system~~ have the capability and is appropriately configured to process large volumes of data.

- Complex calculations in applying a method. When diverse ***IT applications*** ~~systems~~ are required to process complex transactions, regular reconciliations between the ***IT applications*** ~~systems~~ are made, in particular, when the ***IT applications*** ~~systems~~ do not have automated interfaces or may be subject to manual intervention.

- Whether the design and calibration of models is periodically evaluated.

- The complete and accurate extraction of data regarding accounting estimates from the entity's records or from external information sources.

- Data, including the complete and accurate flow of data through the entity's information system, the appropriateness of any modification to the data used in making accounting estimates, and the maintenance of the integrity and security of the data***; w***hen using external information sources, risks related to processing or recording the data.

- Whether management has controls around access, change, and maintenance of individual models to maintain a strong audit trail of the accredited versions of models and to prevent unauthorized access or amendments to those models.

- Whether there are appropriate controls over the transfer of information relating to accounting estimates into the general ledger, including appropriate controls over journal entries.

.A53 In some entities, the term *governance* may be used to describe activities within the control environment, ***the entity's process to monitor the system of internal control,*** ~~monitoring of controls,~~ and other components of ***the system of*** internal control, as described in AU-C section 315. [fn 33]

[fn 33] [Footnote omitted for purposes of this proposed SAS.]

.A54 For entities with an internal audit function, its work may be particularly helpful to the auditor in obtaining an understanding of the following:

- The nature and extent of management's use of accounting estimates
- The design and implementation of ***controls*** ~~control activities~~ that address the risks related to the data, assumptions, and models used to make the accounting estimates
- The aspects of the entity's information system that generate the data on which the accounting estimates are based
- How new risks relating to accounting estimates are identified, assessed, and managed

Reviewing the Outcome or Re-Estimation of Previous Accounting Estimates (Ref: par. .13)

.A55 A review of the outcome or re-estimation of previous accounting estimates (retrospective review) assists in identifying and assessing the risks of material misstatement when previous accounting estimates have an outcome through transfer or realization of the asset or liability in the current period or are re-estimated for the purpose of the current period. Through performing a retrospective review, the auditor may obtain the following:

- Information regarding the effectiveness of management's previous estimation process, from which the auditor can obtain audit evidence about the likely effectiveness of management's current process.
- Audit evidence of matters, such as the reasons for changes that may be required to be disclosed in the financial statements.
- Information regarding the complexity, subjectivity, or estimation uncertainty pertaining to the accounting estimates.
- Information regarding the susceptibility of accounting estimates to, or that may be an indicator of, possible management bias. The auditor's professional skepticism assists in identifying such circumstances or conditions and in determining the nature, timing, and extent of further audit procedures.

.A56 A retrospective review may provide audit evidence that supports the identification and assessment of the risks of material misstatement in the current period. Such a retrospective review may be performed for accounting estimates made for the prior period's financial statements or may be performed over several periods or a shorter period (such as half-yearly or quarterly). In some cases, a retrospective review over several periods may be appropriate when the outcome of an accounting estimate is resolved over a longer period, *or when a history of outcomes provides meaningful information or evidence of a trend*.

.A57 A retrospective review of management judgments and assumptions related to significant accounting estimates is required by AU-C section 240, *Consideration of Fraud in a Financial Statement Audit*. [fn 34] As a practical matter, the auditor's review of previous accounting estimates as a risk assessment procedure in accordance with this section may be carried out in conjunction with the review required by AU-C section 240.

[fn 34] [Footnote omitted for purposes of this proposed SAS.]

.A58 Based on the auditor's previous assessment of the risks of material misstatement, for example, if inherent risk is assessed as higher for one or more risks of material misstatement, the auditor may judge that a more detailed retrospective review is required. As part of the detailed retrospective review, the auditor may pay particular attention, when practicable, to the effect of data and significant assumptions used in making the previous accounting estimates. On the other hand, for example, for accounting estimates that arise from the recording of routine and recurring transactions, the auditor may judge that the application of analytical procedures as risk assessment procedures is sufficient for purposes of the review.

.A59 The measurement objective for fair value accounting estimates and other accounting estimates, based on current conditions at the measurement date, deals with perceptions about value at a point in time, which may change significantly and rapidly as the environment in which the entity operates changes. The auditor may, therefore, focus the review on obtaining information that may be relevant to identifying and assessing risks of material misstatement. For example, in some cases, obtaining an understanding of changes in market participant assumptions that affected the outcome of a previous period's fair value accounting estimates may be unlikely to provide relevant audit evidence. In this case, audit evidence may be obtained by understanding the outcomes of assumptions (such as a cash flow projection) and understanding the effectiveness of management's prior estimation process that supports the identification and assessment of the risk of material misstatement in the current period.

.A60 A difference between the outcome of an accounting estimate and the amount recognized in the previous period's financial statements does not necessarily represent a misstatement of the previous period's financial statements. For example, an entity assumed a forecasted unemployment rate in the development of a loan loss estimate, and the actual losses and unemployment rate differed from that assumed. A difference may represent a misstatement if, for example, the difference arises from information that was available to management when the previous period's financial statements were finalized or that could reasonably be expected to have been obtained and taken into account in the context of the applicable financial reporting framework.[35] Such a difference may call into question management's process for taking information into account in making the accounting estimate. As a result, the auditor may need to reconsider their risk assessment or may determine that more persuasive audit evidence needs to be obtained about the matter. Many financial reporting frameworks contain guidance on distinguishing between changes in accounting estimates that constitute misstatements and changes that do not, and the accounting treatment required to be followed in each

case.

fn 35 [Footnote omitted for purposes of this proposed SAS.]

[No proposed amendment to paragraphs .A61–.A63. Paragraph .A67, .A69, and .A71 included for contextual purposes only.]

Identifying and Assessing the Risks of Material Misstatement (Ref: par. .04 and .15)

.A64 Identifying and assessing risks of material misstatement at the relevant assertion level relating to accounting estimates includes not only accounting estimates that are recognized in the financial statements but also those that are included in the notes to the financial statements.

.A65 ~~AU-C section 200[38] states that GAAS does not ordinarily refer to inherent risk and control risk separately. However, this SAS~~ ***AU-C section 315*** requires a separate assessment of inherent risk and control risk to provide a basis for designing and performing further audit procedures to respond to the risks of material misstatement ***at the assertion level***, ***fn 39*** including significant risks, ~~at the relevant assertion level for accounting estimates~~ in accordance with AU-C section 330. ~~fn~~ See paragraphs .A148–.A149 of this ***section***~~SAS~~ for discussion about documentation of inherent risk factors.

fn 38 [Footnote omitted for purposes of this proposed SAS.]

fn 39 ~~fn. 39~~ ~~Paragraph .07*b* of AU-C section 330.~~ ***Paragraphs .31 and .34 of AU-C section 315. [Subsequent footnotes renumbered]***

.A66. As discussed in paragraph .04 of this ***section*** ~~SAS~~, AU-C section 200 fn 40 explains that inherent risk is ***influenced by inherent risk factors.*** ~~higher for some assertions and related classes of transactions, account balances, and disclosures than for others.~~ In identifying the risks of material misstatement and in assessing inherent risk ***for accounting estimates in accordance with AU-C section 315***, the auditor is required to take into account ***the inherent risk factors that affect susceptibility to misstatement of assertions and how they do so.*** ~~the degree to which the accounting estimate is subject to or affected by estimation uncertainty, complexity, subjectivity, or other inherent risk factors.~~ The auditor's consideration of the inherent risk factors may also provide information to be used in ~~determining~~ the following:

- ***Assessing the likelihood and magnitude of misstatement (such as, where*** ~~Where~~ inherent risk is assessed on the spectrum of inherent risk***)***

- ***Determining the*** ~~The~~ reasons for the assessment given to the risks of material misstatement at the relevant assertion level, and that the auditor's further audit procedures in accordance with paragraph .18 of this section are responsive to those reasons

The interrelationships between the inherent risk factors are further explained in appendix A.

[fn 40] [Footnote omitted for purposes of this proposed SAS.]

.A67 The reasons for the auditor's assessment of inherent risk at the relevant assertion level may result from one or more of the inherent risk factors of estimation uncertainty, complexity, subjectivity, or other inherent risk factors. Examples follow:

- Accounting estimates of expected credit losses are likely to be complex because the expected credit losses cannot be directly observed and may require the use of a complex model. The model may use a complex set of historical data and assumptions about future developments in a variety of entity-specific scenarios that may be difficult to predict. Accounting estimates for expected credit losses are also likely to be subject to high estimation uncertainty and significant subjectivity in making judgments about future events or conditions. Similar considerations apply to insurance contract liabilities.

- An accounting estimate for an obsolescence provision for an entity with a wide range of different inventory types may require complex systems and processes but may involve little subjectivity, and the degree of estimation uncertainty may be low, depending on the nature of the inventory.

- Other accounting estimates may not be complex to make but may have high estimation uncertainty and require significant judgment, for example, an accounting estimate that requires a single critical judgment about a liability, the amount of which is contingent on the outcome of the litigation.

.A68 The relevance and significance of inherent risk factors may vary from one estimate to another. Accordingly, the inherent risk factors may, either individually or in combination, affect simple accounting estimates to a lesser degree, and the auditor may identify fewer risks or assess inherent risk ***close to*** ~~at~~ the lower end of the spectrum of inherent risk.

.A69 Conversely, the inherent risk factors may, either individually or in combination, affect complex accounting estimates to a greater degree and may lead the auditor to assess inherent risk at the higher end of the spectrum of inherent risk. For these accounting estimates, the auditor's consideration of the effects of the inherent risk factors is likely to directly affect the number and nature of identified risks of material misstatement, the assessment of such risks, and ultimately, the persuasiveness of the audit evidence needed in responding to the assessed risks. Also, for these accounting estimates, the auditor's application of professional skepticism may be particularly important.

.A70 Events occurring after the date of the financial statements may provide additional information relevant to the auditor's assessment of the risks of material misstatement at the relevant assertion level. For example, the outcome of an accounting estimate may become known during the audit. In such cases, the auditor may assess or revise the assessment of the risks of material misstatement at the relevant assertion level, [fn 41] regardless of ***how*** the ***inherent risk factors affect susceptibility of assertions to misstatement relating to*** ~~degree to which~~ the accounting estimate**.** ~~was subject to or~~

~~affected by estimation uncertainty, complexity, subjectivity, or other inherent risk factors.~~ Events occurring after the date of the financial statements also may influence the auditor's selection of the approach to testing the accounting estimate in accordance with paragraph .18. For example, for a simple bonus accrual that is based on a straightforward percentage of compensation for selected employees, the auditor may conclude that there is relatively little complexity or subjectivity in making the accounting estimate and, therefore, may assess inherent risk at the relevant assertion level ***close to*** ~~at~~ the lower end of the spectrum of inherent risk. The payment of the bonuses subsequent to period-end may provide sufficient appropriate audit evidence regarding the assessed risks of material misstatement at the relevant assertion level.

[fn 41] Paragraph ***.37***~~.32~~ of AU-C section 315.

.A71 The auditor's assessment of control risk may be done in different ways depending on preferred audit techniques or methodologies. The control risk assessment may be expressed using qualitative categories (for example, control risk assessed as maximum, moderate, or minimum) or in terms of the auditor's expectation of how effective the controls are in addressing the identified risk, that is, the planned reliance on the effective operation of controls. For example, if control risk is assessed as maximum, the auditor contemplates no reliance on the effective operation of controls. If control risk is assessed at less than maximum, the auditor contemplates reliance on the effective operation of controls.

[No amendment to paragraphs .A72–.A78.]

Other Inherent Risk Factors **(Ref: par. .15*b*)**

.A79 The degree of subjectivity associated with an accounting estimate influences the susceptibility of the accounting estimate to misstatement due to management bias or ~~fraud~~ ***other fraud risk factors insofar as they affect inherent risk***. For example, when an accounting estimate is subject to a high degree of subjectivity, the accounting estimate is likely to be more susceptible to misstatement due to management bias or fraud, and this may result in a wide range of possible measurement outcomes. Management may select a point estimate from that range that is inappropriate in the circumstances, or that is inappropriately influenced by unintentional or intentional management bias, and that is, therefore, misstated. For continuing audits, indicators of possible management bias identified during the audit of preceding periods may influence the planning and risk assessment procedures in the current period.

[No amendment to paragraphs .A80–.A84.]

When the Auditor Intends to Rely on the Operating Effectiveness of ~~Relevant~~ Controls **(Ref: par. .18)**

.A85 Testing the operating effectiveness of ~~relevant~~ controls may be appropriate when inherent risk is assessed as higher on the spectrum of inherent risk, including for significant risks. This may be the case when the accounting estimate is subject to or affected by a high degree of complexity. When the accounting estimate is affected by a

high degree of subjectivity and, therefore, requires significant judgment by management, inherent limitations in the effectiveness of the design of controls may lead the auditor to focus more on substantive procedures than on testing the operating effectiveness of controls.

[No further amendment to AU-C section 540.]