Agenda Item 5

ISA 315 (Revised), *Identifying and Assessing the Risks of Material Misstatements*

Objective of Agenda Item

To discuss preliminary issues identified by the Task Force while monitoring the International Auditing and Assurance Standards Board (IAASB) ISA 315 project.

Task Force

The Task Force members are as follows:

- Tracy Harding–BerryDunn, Chair
- Dora Burzenski (supported by Sally Ann Bailey)–Deloitte
- Diane Hardesty–EY
- Kathy Healy–PwC
- Susan Jones–KPMG
- April King–RSM
- Maria Manasses–GT
- Dan Wernke–Clark Schaefer Hackett

Background

In July 2018, the IAASB issued an Exposure Draft that included a proposal to revise ISA 315, *Identifying and Assessing the Risks of Material Misstatements*, (ISA 315). The comment period ended November 2, 2018. At its March 2019 meeting, the IAASB discussed overall issues arising from the comment letters. More specifically, the following were the key themes discussed by the IAASB:

a. the ISA 315 Task Force's initial proposals to address specific responses to the proposed ISA 315, in particular, the broad concerns in relation to the length and complexity of the standard, and

b. proposed changes to address specific issues within the section on understanding the entity's system of internal control.

At its June 2019 meeting, the IAASB discussed issues with respect to the ISA 315 Task Force proposed changes to respond to the comments received in connection with the Exposure Draft. In particular, the ISA 315 Task Force sought IAASB's views about:

a. The new approach in presenting the requirements and application material to broadly address complexity, and scalability and proportionality issues raised, and
b. Specific proposed changes to address comments relative to the definitions, requirements, and application material.

At its meeting in September 2019, the IAASB approved the proposed ISA 315 as a final standard, including conforming amendments to other ISAs. The standard will be effective for audits of financial statements for periods beginning on or after December 15, 2021.

In the following sections are preliminary issues identified by the ASB Risk Assessment Task Force (the "Task Force") based on the version of the proposed ISA 315 approved by the IAASB as a final standard. The issues are categorized as follows:

I. General Comments

II. Components of Internal Control

III. Gaining an Understanding of Internal Control

IV. Identifying and Assessing the Risks of Material Misstatement

V. Paragraph 18 of AU-C 330

I. General

Areas of Support

Overall, the Task Force is supportive of the final ISA 315. In particular, the Task Force is supportive of the following specific areas:

- New requirement to make separate assessments of inherent and control risk,
- The introduction of the spectrum of inherent risk,
- Revised definition of significant risk. The revised definition states the following:

  Definition

  Significant risk – An identified risk of material misstatement: (Ref: Para. A10)

  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

  That is to be treated as a significant risk in accordance with the requirements of other ISAs

  Application Material

A10. 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. In the context. 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.

- The new requirement for the auditor to stand-back and reevaluate material significant classes of transaction, account balances, and disclosures that have been deemed to not contain relevant assertions

Questions for the ASB

1. What are the ASB's views on the revised definition of significant risk?
2. Can significant risks arise at the overall financial statements level? Does it matter?
3. Should the definition or application material indicate that both likelihood and magnitude need to be close to the upper end of the spectrum of inherent risk? The IAASB decided that may not necessarily be the case.

Consideration of PCAOB standards

A Task Force member believes that the ASB also should consider the extent to which the revised AU-C 315 would align with the PCAOB standards. A concern is creating significant differences in risk assessment (for example, whether the proposed standard would come to different conclusions as to what is a significant account or disclosure or what is a significant risk). It is thus important to determine whether the revised AU-C 315 will be able to bridge the wording differences such that different conclusions would not be reached on such matters. The Task Force intends to prepare analyses that will comparing the proposed SAS to the relevant PCAOB standard.

II. Internal Control

ISA 315 contains a series of requirements in which the auditor is required to perform risk assessment procedures to understand the components of internal control (paragraphs 28, 30, 31A, 36, and 39). Underpinning these requirements is application material that describes the components of internal control. The Task Force understands that in describing the components of internal control, the IAASB intended the standard to be framework neutral, that is, the content describing the component is not solely based on a particular framework. Although generally consistent with the Committee of Sponsoring Organizations of the Treadway Commission Internal Control Framework (COSO), the guidance in ISA 315 contains differences with COSO. The following table compares the definitions and the descriptions of the internal control components among ISA 315, AU-C 315, and COSO.

ISA 315	*AU-C 315*	*COSO*
Definitions		
Controls – Policies or procedures that an entity establishes to achieve the control objectives of management or those charged with governance. In this context: (Ref: Para. A2a–A4a) (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 communications, or implied through actions and decisions. (ii) Procedures are actions to implement policies.		Control—(1) As a noun (i.e., existence of a control), a policy or procedure that is part of internal control. Controls exist within each of the five components. (2) As a verb (i.e., to control), to establish or implement a policy or procedure that effects a principle.
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,	**Internal control**. A process effected by those charged with governance, management, and other personnel that is designed to provide reasonable assurance about the achievement of the entity's objectives with regard to the reliability of financial reporting, effectiveness and	Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

effectiveness and efficiency of operations, and compliance with applicable laws and regulations. For the purposes of the ISAs, 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, and (v) Control activities	efficiency of operations, and compliance with applicable laws and regulations. Internal control over safeguarding of assets against unauthorized acquisition, use, or disposition may include controls relating to financial reporting and operations objectives.	
Components		
Control Environment		
Appendix 3, par. 3--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.	**.A78** 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 internal control and its importance in the entity. The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.	The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process

		for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control. **Principles Relating to Control Environment** • The entity demonstrates a commitment to integrity and ethical values. • Those charged with governance demonstrate independence from management and exercises oversight of the development and performance of internal control. • Management establishes, with those charged with governance oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. • The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

		• The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Entity's Risk Assessment Process		
Appendix 3, 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.	**A89** An entity's risk assessment process for financial reporting purposes is its identification, analysis, and management of risks relevant to the preparation and fair presentation of financial statements. If that process is appropriate to the circumstances, including the nature, size, and complexity of the entity, it assists the auditor in identifying risks of material misstatement. For example, risk assessment may address how the entity considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements. Risks relevant to reliable financial reporting also relate to specific events or transactions. Whether the entity's risk assessment process is appropriate to the circumstances is a matter of professional judgment.	Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

		The Principles Relating to The Risk Assessment Component • The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to external reporting objectives. • The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. • The entity considers the potential for fraud in assessing risks to the achievement of objectives. • The entity identifies and assesses changes that could significantly impact the system of internal control.
Monitoring of Controls		
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	**.A110** Monitoring of controls is a process to assess the effectiveness of internal control performance over time. It involves assessing the effectiveness of controls on a timely basis and taking necessary remedial actions. Management accomplishes monitoring of controls through ongoing activities, separate evaluations, or a combination of the two. Ongoing monitoring activities often are	Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted

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.	built into the normal recurring activities of an entity and include regular management and supervisory activities.	periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, standard-setting bodies, or management and the board of directors, and deficiencies are communicated to management and the board of directors as appropriate. **Principles Relating to The Monitoring Activities Component** • The principles relating to the monitoring of controls component are as follows: • The entity selects, develops, and performs ongoing or separate evaluations to ascertain whether the components of internal control are present and functioning. • The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and those charged with governance, as appropriate.
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: • Initiate, record and process entity transactions (as well as to capture, process and disclose information about events and conditions other than transactions) 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 (e.g., transferring of accumulated transactions from a subsidiary ledger); • Capture and process information relevant to the preparation of the financial statements for events and conditions other than transactions, such as the depreciation and	**.A92** *The information system, including related business processes relevant to financial reporting (Ref: par. .19).* The information system relevant to financial reporting objectives, which includes the accounting system, consists of the procedures and records designed and established to • initiate, authorize, record, process, and report entity transactions (as well as events and conditions) and 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; • transfer information from transaction processing systems to the general ledger; • capture information relevant to financial reporting for events and conditions other than transactions, such as the depreciation and	Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations. **The Principles Relating to The Information And Communication** • The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. • The entity internally communicates information, including objectives and

amortization of assets and changes in the recoverability of assets; and • Ensure information required to be disclosed by the applicable financial reporting framework is accumulated, recorded, processed, summarized and appropriately reported in the financial statements.	amortization of assets and changes in the recoverability of accounts receivables; and • ensure information required to be disclosed by the applicable financial reporting framework is accumulated, recorded, processed, summarized, and appropriately reported in the financial statements.	responsibilities for internal control, necessary to support the functioning of internal control. • The entity communicates with external parties regarding matters affecting the functioning of internal control.
Control Activities		
20. Controls in the control activities component are identified in accordance with paragraph 39. 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 to the following. • *Authorization and approvals*. An authorization affirms that a transaction is valid (i.e. it represents an actual economic event or is within an entity's	Control activities are the policies and procedures that help ensure that management directives are carried out. Control activities, whether within IT or manual systems, have various objectives and are applied at various organizational and functional levels. Examples of specific control activities include those relating to the following: • Authorization • Performance reviews • Information processing • Physical controls • Segregation of duties	Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

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		**The Principles Relating to The Control Activities** • The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. • The entity selects and develops general control activities over technology to support the achievement of objectives. • The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

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: o The physical security of assets, including adequate safeguards such as secured facilities over access to assets and records. o The authorization for access to computer programs and data files (i.e., logical access). o 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 example above, 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.		

Task Force Views

The Task Force has discussed whether the ASB ought to explore whether our proposed SAS should be more aligned to the COSO framework than the descriptions contained in ISA 315 since COSO is more widely used in our jurisdiction.

Questions for the ASB

4. What are the ASB's views about the alignment of the definitions and descriptions of the internal control components?

III. Gaining an Understanding of Internal Control

The following table summarizes the requirements and application material of ISA 315 that deal with the auditor's requirements to gain an understanding and evaluate each of the components of internal control.

Requirement	*Application Material*
28. The auditor shall obtain an understanding of the control environment relevant to the preparation of the financial statements, through performing risk assessment procedures, by: (Ref: Para. A106 – A107) (a) Understanding the set of controls, processes and structures that address: (Ref: Para. A108–A108a) (i) How management's oversight responsibilities are carried out, such as the entity's culture and management's and (b) Evaluating whether: (Ref: Para. A110a–A114b) (i) Management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior;	Scalability A106. 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 where there are no other owners. Accordingly, some considerations about the entity's control environment may be less relevant or may not be applicable. A107. 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**: • 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 behaviour through oral communication and by management example. Consequently, the attitudes, awareness and actions of

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,	(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	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: Para. 28(a)) A108. Audit evidence for the auditor's understanding of the control environment may be obtained through a combination of inquiries and other risk assessment procedures (i.e., corroborating inquiries through observation or inspection of documents). A108a. 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: Para. 28(b)) Why the auditor evaluates the control environment A108b. 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. 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 A102). The auditor's evaluation of the control environment A110a. The auditor's evaluation of the control environment is based on the understanding obtained in accordance with paragraph 28(a). A113. 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

and retains competent individuals; and (v) How the entity holds individuals accountable for their responsibilities in the pursuit of the objectives of the system of internal control;	internal control.

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.

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.

A114.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.

A114a.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.

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 (e.g., to overstate earnings).

A114b. The auditor's evaluation of the control environment as it relates to the entity's use of IT may include such matters as:

- 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)).

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

(a) Understanding the entity's process for: (Ref: Para. A117–A117a)
   (i) Identifying business risks relevant to financial reporting objectives; (Ref: Para. A59)
   (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: Para. A119a–A120)

Obtaining an Understanding of the Entity's Risk Assessment Process (Ref: Para. 30–31)

Understanding the entity's risk assessment process (Ref: Para. 30(a))

A117. As explained in paragraph A59, not all business risks give rise to risks of material misstatement. 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:

- 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; and
- Considered the potential for fraud when considering the risks to achieving the entity's objectives.[1]

A117a.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: Para. 30(b))

Why the auditor evaluates whether the entity's risk assessment process is appropriate

A117b. 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 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 A102).

Evaluating whether the entity's risk assessment process is appropriate (Ref: Para. 30(b))

[1] See ISA 240, paragraph 9

	A119a. The auditor's evaluation of the appropriateness of the entity's risk assessment process is based on the understanding obtained in accordance with paragraph 30(a). Scalability A120. 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. **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 (e.g., 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 the discussions the auditor has with management that management are in fact performing risk assessment procedures.
31. If the auditor identifies risks of material misstatement that management failed to identify, the auditor shall: (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 30(b).

31A .The auditor shall obtain an understanding of the entity's process for monitoring the system of internal control relevant to the preparation of the financial statements, through performing risk assessment procedures, by: (Ref: Para. A123–A124)

(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 and

(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.

Obtaining an Understanding of the Entity's Process to Monitor the Entity's System of Internal Control (Ref: Para. 31A)

Scalability

A123. 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's is directly involved in operations, as there may not be any other monitoring activities.

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.

A124. For entities where 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: Para. 31A(a))

A126a. Matters that may be relevant for the auditor to consider when understanding how the entity monitors its system of internal control include:

- 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; and

identified; (Ref: Para. A126a–A127) and (ii) The entity's internal audit function, if any, including its nature, responsibilities and activities; (Ref: Para. 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: Para. A135a–A135b)	(Ref: Para. A135c)	• How identified deficiencies have been addressed through appropriate remedial actions, including timely communication of such deficiencies to those responsible for taking remedial action. A127. 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: o Evaluate the continuing design effectiveness of information processing controls and modify them, as appropriate, for changes in conditions; or o 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: Para. 31A(a)(ii)) **Appendix 4** 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, ISA 610 (Revised 2013)[2] applies.

[2] ISA 610 (Revised 2013), *Using the Work of Internal Auditors*

	Other sources of information used in the entity's process to monitor the system of internal control Understanding the sources of information (Ref: Para. 31A(b)) A135.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 A135a. 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: Para 31A(c)) A135b. 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 A102). Evaluating whether the entity's process to monitor the system of internal control is appropriate (Ref: Para. 31A(c)) A135c.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.

36. The auditor shall obtain an understanding of the entity's information system and communication relevant to the preparation of the financial statements, through performing risk assessment procedures, by: (Ref: Para. A135n)

(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: Para. A136a–A146) (i) How information flows through the entity's information system, including how:	and (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: Para. A159(a))

Obtaining an Understanding of the Information System and Communication (Ref: Para. 36)

Appendix 3, Paragraphs 15–19, sets out further considerations relating to the information system and communication.

Scalability

A135n. 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 ISA 330 and may further assist the auditor in identifying or assessing risks of material misstatement (see paragraph A102).

Obtaining an understanding of the information system (Ref: Para. 36(a))

A136a. 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. [*From paragraph A94a*] Further, some entities may have information systems that are highly integrated such that controls may be designed in a manner to simultaneously achieve financial reporting, compliance and operational objectives, and combinations thereof.

A136b. 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:

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		• The competence of the individuals undertaking the work; • Whether there are adequate resources; and • Whether there is appropriate segregation of duties. A137a. 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 the information processing process. A137b. 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. A141c. The auditor's understanding of the information system may be obtained in various ways and may include: • 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; or • Selecting transactions and tracing them through the applicable process in the information system (i.e., performing a walk-through). Automated tools and techniques A141e. 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

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 (a)(i) to (a)(iii) above; (b) Understanding how the entity communicates significant matters that support the preparation of the financial statements and related		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 A142. 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 include: • 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 experts 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: o Assumptions developed internally that may affect an asset's useful life; or o 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

reporting responsibilities in the information system and other components of the system of internal control: (Ref: Para. A158a–A159) (i) Between people within the entity, including how financial reporting roles and responsibilities are communicated; (ii) Between management and those charged with governance; and (iii) With external parties, such as those with regulatory authorities;		conditions that have been identified that may cast significant doubt on the entity's ability to continue as a going concern.[3] A143. 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 information technology in the information system Why does the auditor understand the IT environment relevant to the information system A144. 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. A144a. 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 A144b. 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. A146. 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 flows into, through and out the entity's information system. Obtaining an Understanding of the Entity's Communication (Ref: Para. 36(b)) Scalability

[3] See ISA 570 (Revised), paragraphs 19–20

	A158a. 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. A159. In less complex entities, communication may be less structured (e.g., 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: Para. 36(c)) A159a. 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 paragraphs 36(a)–(b).

39. The auditor shall obtain an understanding of the control activities component, through performing risk assessment procedures, by: (Ref: Para. A160–A161a)

(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: Para. A170–A172)
   (ii) Controls over journal entries, including

and

(d) For each control identified in (a) or (c)(ii): (Ref: Para. A194–A200)
   (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; and

A160. 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.

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.

A160a. 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 risks to the integrity of information (i.e., 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.

A160b.There may also be direct controls that 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 39. However, 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.

Example:

A sales manager's review of a summary of sales activity for specific stores by region ordinarily is only indirectly related 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.

A160c. Paragraph 39 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

non-standard journal entries used to record non-recurring, unusual transactions or adjustments; (Ref: Para. A175–A175a) (iii) Controls for which the auditor plans to test operating effectiveness in determining the nature, timing and extent of substantive testing, which shall include controls	(ii) Determining whether the control has been implemented by performing procedures in addition to inquiry of the entity's personnel.	general IT control alone is typically not sufficient to address a risk of material misstatement at the assertion level. A160d. The controls that the auditor is required to identify and evaluate the design and determine the implementation of, in accordance with paragraph 39 are those: • Controls which 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 ISA 330. These controls also include controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. • Controls include 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 understanding of the risks of material misstatement, including the identification of additional risks of material misstatement (see paragraph A102). This understanding also provides the basis for the auditor's design of the nature, timing and extent of substantive audit procedures that are responsive to the related assessed risks of material misstatement. • Other controls that the auditor considers are appropriate to enable the auditor to meet the objectives of paragraph 17 with respect to risks at the assertion level. A160e. Controls in the control activities component are required to be identified when such controls meet one or more of the criteria included in paragraph 39(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: Para. 39) A160f. 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. A160g. 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.

that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence; and (Ref: Para. A175d–A177) (iv) Other controls that the auditor considers are appropriate to enable the auditor to meet the objectives of paragraph 17 with		A160h. 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: Para. 39) A161. 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. **Example**: Management's sole authority for granting credit to customers and approving significant purchases can provide strong control over important account balances and transactions. A161a.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 ISA 240, domination of management by a single individual can be a potential control deficiency since there is an opportunity for management override of controls. [4] Controls that Address Risks of Material Misstatement at the Assertion Level (Ref: Para. 39(a)) Controls that address risks that are determined to be a significant risk (Ref: Para. 39(a)(i)) A170. 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 ISA 330.[5] Although risks relating to significant non-routine or judgmental matters are often less likely to be subject to routine controls, management may have other responses intended to deal with such risks. Accordingly, the auditor's understanding of whether the entity

[4] ISA 240, paragraph A28

[5] ISA 330, paragraph 21

respect to risks at the assertion level, based on the auditor's professional judgment; (Ref: Para.A177a)		has designed and implemented controls for significant risks arising from non-routine or judgmental matters may include whether and how management responds to the risks. Such responses may include: • Controls such as a review of assumptions by senior management or experts. • Documented processes for accounting estimations. • Approval by those charged with governance. **Example**: Where there are one-off events such as the receipt of a notice of a significant lawsuit, consideration of the entity's response may include such matters as whether it has been referred to appropriate experts (such as internal or external legal counsel), whether an assessment has been made of the potential effect, and how it is proposed that the circumstances are to be disclosed in the financial statements. A172. ISA 240[6] 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: Para. 39(a)(ii)) A175. 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 entity incorporates information from transaction processing into the general ledger ordinarily involves the use of journal entries, whether standard or non-standard, or automated or manual. The extent to which other controls are identified may vary based on the nature of the entity and the auditor's planned approach to further audit procedures. **Example**: In an audit of a less complex entity, the entity's information system may not be complex and the auditor may not plan to rely on the operating effectiveness of controls. Further, the auditor may not have identified any significant risks or any other risks of material misstatement for which it is necessary for the auditor
(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: Para. A179a–A188)		
(c) For such IT applications and other aspects of the		

[6] ISA 240, paragraphs 28 and A33

IT environment identified in (b), identifying: (Ref: Para. A188a–A189) (i) The related risks arising from the use of IT; and (ii) The entity's general IT controls that address such risks;	

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

A175a. In manual general ledger systems, non-standard 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 may therefore be more easily identified through the use of automated techniques.

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: Para. 39(a)(iii))

A175d. 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 ISA 330,[7] 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.

A176. 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

[7] ISA 330, paragraph 8(b)

	procedures in accordance with ISA 330, such controls are also required to be identified because ISA 330[8] requires the auditor to design and perform tests of those controls. **Examples**: The auditor may plan to test the operating effectiveness of controls: • 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 (e.g., 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. A177. The auditor's plans 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: Para. 39(a)(iv)) A177a. Other controls that the auditor may consider are appropriate to identify, and evaluate the design and determine the implementation, may include: • 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; or • Complementary user entity controls, if using a service organization.[9] Identifying IT Applications and Other Aspects of the IT Environment, Risks Arising from the Use of IT and General IT Controls (Ref: Para. 39(b)–(c)) **Appendix 5** includes example characteristics of IT applications and other aspects of the IT environment, and guidance related to those characteristics, that may be

[8] ISA 330, paragraph 8(a)

[9] ISA 402, *Audit Considerations Relating to an Entity Using a Service Organization*

	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: Para. 39(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 A179a. Understanding the risks arising from the use of IT and the general IT controls implemented by the entity to address those risks may affect: • The auditor's decision about whether to test the operating effectiveness of controls to address risks of material misstatement at the assertion level; **Example**: When general IT controls are not designed effectively or appropriately implemented to address risks arising from the use of IT (e.g., 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; **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 (i.e. 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 (e.g., 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; **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 direct data changes to the reports.

- The auditor's assessment of inherent risk at the assertion level; or

  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 an indicator 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.

  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

A180. 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.

	A180a. 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. A180b. 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 not plan to rely on controls over the system-generated reports and plan to directly test the inputs and outputs of such reports, in which case the auditor may not identify the related IT applications as being subject to risks arising from IT. Scalability A180c. 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 the circumstances of the entity and its IT environment, as well as 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**: • 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 (e.g., the chart of accounts, reporting parameters or thresholds). In addition, the entity may have a process or procedures to manage access to the application (e.g., 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 and the IT environment may involve multiple IT applications and the IT processes to manage the IT environment may be complex (e.g., 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. A180d. 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 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 A188. 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 (e.g., 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: Para. 39(c)) **Appendix 6** sets out considerations for understanding general IT controls. A188a. 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 that address risks related to inappropriate data changes (e.g., the risk of inappropriate changes to the data through direct database access or the ability to directly manipulate information). A189. 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 (e.g., 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). Applicable risks arising from the use of IT may also be identified related to cybersecurity. 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. Evaluating the Design, and Determining Implementation, of Identified Controls in the Control Activities Component (Ref: Para 39(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 (i.e., the control objective). A194a. 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.

	A198. 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 application of specific controls. • Inspecting documents and reports. Inquiry alone, however, is not sufficient for such purposes. A198a. 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 39(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 39(b)-(d) on the newly designed or implemented controls. A198b.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(s) of material misstatement is an input to the auditor's control risk assessment at the assertion level. A199. 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, the auditor may plan to test the operating effectiveness of automated controls by identifying and testing general IT controls that provide for the consistent operation of an automated control instead of performing tests of operating effectiveness on the automated controls directly. 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 ISA 330.[10] A200. When the auditor does not plan to test the operating effectiveness of identified controls, the auditor's understanding may still assist in the design of the nature, timing and extent of substantive audit procedures that are responsive to the related risks of material misstatement. **Example**: The results of these risk assessment procedures may provide a basis for the auditor's consideration of possible deviations in a population when designing audit samples.

[10] ISA 330, paragraphs 8–11

Task Force Views

General Comments Relating to The Components of Internal Control—

- The Task Force has expressed continued concern about the need to "evaluate" each component of internal control; in particular, the requirement in paragraph 36(c) to evaluate whether the relevant aspects of the information system and communication appropriately support the preparation of financial statements seems to go beyond the objective of risk assessment procedures, and approach that of an internal control exam. In paragraph 36(c) and corresponding paragraphs for the other components, a suggestion is to change *evaluating* to *considering* or *assessing*.

Paragraph 30—

- The Task Force noted that fraud risks are not mentioned in the risk assessment process requirements, and only briefly mentioned in the application material. A Task Force member believes that ISA 240 does address the entity's risk assessment process in regard to fraud. However, other Task Force members believe the importance of fraud risks to the evaluation warrants more prominent mention in 315.

Paragraph 36—The Task Force raised the issue that it is not clear whether the understanding required by subparagraph (a)(iii) is limited to significant classes of transactions, account balances, and disclosures.

Paragraph 39—

- The Task Force noted that the term "controls relevant to the audit" is no longer being used in ISA 315. Therefore, the issue was raised whether the term should be retained in the proposed SAS.

- Under subparagraph (a)(iv) the auditor would identify control activities relevant to the audit using his/her professional judgment. However, it may be unclear how the auditor would make this identification. We continue to believe that the ASB's Q&As would be helpful in this regard, either as application material or other guidance issued concurrently with a proposed SAS (see Appendix for excerpts of the TQAs).

- Also, the Task Force noted that the following sentence from paragraph 21 of extant AU-C 315 is not captured in this requirement:

  > 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. However, the auditor should obtain an understanding of the process of reconciling detailed records to the general ledger for material account balances.

  We recommend this requirement be retained, with "material" replaced by "significant."

- Design and implementation is limited to the control activities component. We discussed (but did not come to a conclusion regarding) whether controls may exist in other components that may be relevant to the audit and thus subject to design and implementation, and recommend this question be considered before finalizing this wording.

Questions for the ASB

5. What are the ASB's views about the descriptions of the components of internal control and the work effort set forth in ISA 315?

IV. *Identifying and Assessing the Risks of Material Misstatement*

The following are paragraphs from ISA 315 that deal with the auditor's identifying and assessing the risks of material misstatement.

Requirement	***Application Material***
Identifying Risks of Material Misstatement	
45. The auditor shall identify the risks of material misstatement and determine whether they exist at: (Ref: Para. A201–A206)	*Why the Auditor Identifies and Assesses the Risks of Material Misstatement* A201. 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. A201a. 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 ISA 330. *Identifying Risks of Material Misstatement* A202. The identification of risks of material misstatement is performed before consideration of any related controls (i.e., the

Requirement	*Application Material*
	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.[11] A202a. 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 A202b. 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 A203. In identifying and assessing the risks of material misstatement, the auditor may use the categories of assertions as described in paragraph A204(a)–(b) below or may express them differently provided all aspects described below 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. A204. Assertions used by the auditor in considering the different types of potential misstatements that may occur may fall into the following categories:

[11] ISA 200, paragraph A15a

Requirement	*Application Material*
	Assertions about classes of transactions and events, and related disclosures, for the period under audit: Occurrence—transactions and events that have been recorded or disclosed have occurred, and such transactions and events pertain to the entity. 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. Accuracy—amounts and other data relating to recorded transactions and events have been recorded appropriately, and related disclosures have been appropriately measured and described. Cutoff—transactions and events have been recorded in the correct accounting period. Classification—transactions and events have been recorded in the proper accounts. 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. Assertions about account balances, and related disclosures, at the period end: Existence—assets, liabilities, and equity interests exist. Rights and obligations—the entity holds or controls the rights to assets, and liabilities are the obligations of the entity.

Requirement	*Application Material*
	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. 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. Classification—assets, liabilities and equity interests have been recorded in the proper accounts. 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. A205. The assertions described in paragraph A204(a)–(b) above, 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. **Example**: An example of such a disclosure includes where the entity may be required by the applicable financial reporting framework to describe its 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.

Requirement	*Application Material*
	Considerations Specific to Public Sector Entities A206. When making assertions about the financial statements of public sector entities, in addition to those assertions set out in paragraph A204(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: Para. 45(a) and 47)
(a) The financial statement level; (Ref: Para. A206a–A207e) or	Why the Auditor Identifies and Assesses Risks of Material Misstatement at the Financial Statement Level A206a. 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 would therefore require an overall response in accordance with ISA 330. A206aa. 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 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 A207. 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

Requirement	*Application Material*
	(e.g., 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 may therefore affect the auditor's risk identification and assessment of risks of material misstatement at the assertion level. 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 auditor may determine that the going concern basis of accounting gives rise to a risk of material misstatement at the financial statement level. In this situation, the accounting framework may need to be applied using a liquidation basis, which would likely affect all assertions pervasively. A207a. 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, and: • The outcome of the related evaluations required by paragraphs 28(b), 30(b), 31A(c) and 36(c); and • Any control deficiencies identified in accordance with paragraph 43.

Requirement	*Application Material*
	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. A207b. 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. **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 may therefore determine that there is a greater susceptibility to misstatement due to fraud risk factors that affect inherent risk (i.e., 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 under-statement of liabilities and expenses to ensure that financing will be obtained). A207c. 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 where withdrawal is possible under applicable law or regulation.

Examples:

- 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 as to 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.

A207d. ISA 705 (Revised)[12] 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 where withdrawal is possible under applicable law or regulation.

Considerations Specific to Public Sector Entities

A207e. For public sector entities, the identification of risks at the financial statement level may include consideration of

Requirement	*Application Material*
	matters related to the political climate, public interest and program sensitivity.
(b) The assertion level for classes of transactions, account balances, and disclosures. (Ref: Para. A208)	A208. Risks of material misstatements that do not relate pervasively to the financial statements are risks of material misstatement at the assertion level.
46. The auditor shall determine the relevant assertions and the related significant classes of transactions, account balances and disclosures. (Ref: Para. A211–A214)	A211. 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 36. This understanding may further assist the auditor in identifying and assessing risks of material misstatement (see A102). Automated Tools and Techniques A213. The auditor may use automated techniques to assist in the identification of significant classes of transactions, account balances and disclosures. Examples: • 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 was comprised of numerous offsetting transactions and journal entries occurring during the period, indicating that the account balance or class of transactions may be significant (e.g., a payroll clearing account). This same payroll

[12] ISA 705 (Revised), *Modifications to the Opinion in the Independent Auditor's Report*

Requirement	*Application Material*
	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 A214. 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 may therefore be considered significant by the auditor include disclosures about: • 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.

Requirement	***Application Material***
	• 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 Financial Statement Level	
47. For each risk identified in accordance with paragraph 45(a), the auditor shall assess the risk and: (Ref: Para. A206a–A207e)	Why the Auditor Identifies and Assesses Risks of Material Misstatement at the Financial Statement Level A206a. 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 would therefore require an overall response in accordance with ISA 330. A206aa. 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 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 A207. 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 (e.g., risk of management override of controls). Rather, they

Requirement	*Application Material*
	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 may therefore affect the auditor's risk identification and assessment of risks of material misstatement at the assertion level. 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 auditor may determine that the going concern basis of accounting gives rise to a risk of material misstatement at the financial statement level. In this situation, the accounting framework may need to be applied using a liquidation basis, which would likely affect all assertions pervasively. A207a. 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, and: • The outcome of the related evaluations required by paragraphs 28(b), 30(b), 31A(c) and 36(c); and • Any control deficiencies identified in accordance with paragraph 43.

Requirement	*Application Material*
	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. A207b. 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. 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 may therefore determine that there is a greater susceptibility to misstatement due to fraud risk factors that affect inherent risk (i.e., 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 under-statement of liabilities and expenses to ensure that financing will be obtained). A207c. 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 where withdrawal is possible under applicable law or regulation. Examples: • 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 as to cause the auditor to conclude that the risk of intentional misrepresentation by

Requirement	*Application Material*
	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. A207d. ISA 705 (Revised) 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 where withdrawal is possible under applicable law or regulation. Considerations Specific to Public Sector Entities A207e. For public sector 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.
(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.	

Requirement	***Application Material***
Assessing Risks of Material Misstatement at the Assertion Level	
Assessing Inherent Risk	
48. For each risk identified in accordance with paragraph 45(b), the auditor shall assess inherent risk by assessing the likelihood and magnitude of misstatement. In doing so, the auditor shall take into account how, and the degree to which: (Ref: Para. A220a–A228)	Why the auditor assesses likelihood and magnitude of misstatement A220a. 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. A220b. 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 ISA 330 and other ISAs. A221.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

Requirement	*Application Material*
	A221a. In assessing inherent risk, the auditor uses professional judgment in determining the significance of the combination of the likelihood and magnitude of a misstatement. A221b. 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. A221c. 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. A222. In considering the magnitude of a misstatement, the auditor considers the qualitative and quantitative aspects of the possible misstatement (i.e., misstatements in assertions about classes of transactions, account balances or disclosures may be judged to be material due to size, nature or circumstances). A222a. 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 (i.e., 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. A222b. 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

Requirement	*Application Material*
	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. A225. 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: Para 48(b)) A226. 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. A227. 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.

Requirement	***Application Material***
	Considerations Specific to Public Sector Entities A228. In exercising professional judgment as to the assessment of the risk of material misstatement, public sector auditors may consider the complexity of the regulations and directives, and the risks of non-compliance with authorities.
(a) Inherent risk factors affect the susceptibility of relevant assertions to misstatement.	
(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.	

49. The auditor shall determine whether any of the assessed risks of material misstatement are significant risks. (Ref: Para. A228a–A229b)	Why significant risks are determined and the implications for the audit A228a. 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: • Controls that address significant risks are required to be identified in accordance with paragraph 39(a)(i), with a requirement to evaluate whether the control has been designed effectively and implemented in accordance with paragraph 39(d). • ISA 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. • ISA 330 requires the auditor to obtain more persuasive audit evidence the higher the auditor's assessment of risk. • ISA 260 (Revised) requires communicating with those charged with governance about the significant risks identified by the auditor. • ISA 701 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. • 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.

	• ISA 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. Determining significant risks A229a. 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 for an entity period on period. It may depend on the nature and circumstances of the entity for which the risk is being assessed. A229aa. The determination of which of the assessed risks of material misstatement are close to the upper end of the spectrum of inherent risk, and are therefore 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 ISA. ISA 240 provides further requirements and guidance in relation to the identification and assessment of the risks of material misstatement due to fraud. Example: • 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.

Requirement	*Application Material*
	• 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. A229b. The auditor also takes into the 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 may therefore 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. • 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. • Changes in the entity's business that involve changes in accounting, for example, mergers and acquisitions.

50. The auditor shall determine whether substantive procedures alone cannot provide sufficient appropriate audit evidence for any of the risks of material misstatement at the assertion level. (Ref: Para. A231a–A231e)	Why risks for which substantive procedures alone do not provide sufficient appropriate audit evidence are required to be identified A231a. 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 ISA 330 to address risks of material misstatement at the assertion level. A231b. Paragraph 39(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 ISA 330, to design and perform tests of such controls. Determining risks for which substantive procedures alone do not provide sufficient appropriate audit evidence A231d. Where 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 where 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 applications. 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.

Requirement	***Application Material***
	• 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. 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, substantial controls testing is typically performed to determine that the origination and completion of calls, and data activity is correctly captured (e.g., minutes of a call or volume of a download) and recorded correctly in the entity's billing system. A231e. ISA 540 (Revised) provides further guidance related to accounting estimates about risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. In relation to accounting estimates this may not be limited to automated processing, but may also be applicable to complex models.
Assessing Control Risk	

51. If the auditor plans to test the operating effectiveness of controls, the auditor shall assess control risk. If the auditor does not plan to test the operating effectiveness of controls, the auditor's assessment of control risk shall be such that the assessment of the risk of material misstatement is the same as the assessment of inherent risk. (Ref: Para. A232–A235a)	Assessing Control Risk (Ref: Para. 51) A232. 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 ISA 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 53. A233. 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. A234. 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, takes 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. A235a. 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

Requirement	***Application Material***
	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 ISA 330.

Requirement	***Application Material***
Evaluating the Audit Evidence Obtained from the Risk Assessment Procedures	
51A. The auditor shall 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 shall perform additional risk assessment procedures until audit evidence has bene obtained to provide such a basis. In identifying and assessing the risks of material misstatement, the auditor shall take into account all audit evidence obtained from the risk assessment procedures, whether corroborative or contradictory to assertions made by management. (Ref: Para. A239a–A239c)	Why the Auditor Evaluates Audit Evidence from Risk Assessment Procedures A239a. 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 ISA 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 A239b. Audit evidence from risk assessment procedures comprises both information that supports and corroborates management's assertions, and any information that contradicts such assertions. Professional skepticism A239c. 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.

Requirement	***Application Material***
Classes of Transactions, Account Balances and Disclosures that are Not Significant, but Which Are Material	
52. 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 shall evaluate whether the auditor's determination remains appropriate. (Ref: Para. A240–A242)	Classes of Transactions, Account Balances and Disclosures that Are Not Significant, but Which Are Material (Ref: Para. 52) A240. As explained in ISA 320, 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. For the purpose of this ISA and paragraph 18 of ISA 330, classes of transactions, account balances or disclosures are material if omitting, misstating or obscuring information about them could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements as a whole. A241. 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 (i.e., there are no relevant assertions identified). 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 A240. A242. Audit procedures to address classes of transactions, account balances or disclosures that are material but are not

Requirement	***Application Material***
	determined to be significant are addressed in ISA 330. When a class of transactions, account balance or disclosure is determined to be significant as required by paragraph 46, the class of transactions, account balance or disclosure is also a material class of transactions, account balance or disclosure for the purposes of paragraph 18 of ISA 330.
Revision of Risk Assessment	
53. If the auditor obtains new information which is inconsistent with the audit evidence on which the auditor originally based the identification or assessments of the risks of material misstatement, the auditor shall revise the identification or assessment. (Ref: Para. A243)	Revision of Risk Assessment (Ref: Para. 53) A243. 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. 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. Paragraphs 16 and 17 of ISA 330 provide further guidance about evaluating the operating effectiveness of controls.

Task Force Views

- Par. 45—The Task Force noted that the work effort to identify the risks of material misstatement in ISA 315 is different than AU-C 315. Paragraph 45(b) of ISA 315 requires the auditor, among other things, to identify the risks of material misstatement and determine whether they exist at the *assertion* level. Also, paragraph 48 requires, in part, that for each risk identified in accordance with paragraph 45(b) the auditor shall assess inherent risk by assessing the likelihood and magnitude of misstatement. In doing so, the auditor shall take into account how, and the degree to which, 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.

  Paragraph 26(b) of AU-C 315 requires the auditor to identify and assess the risks of material misstatements at the *relevant assertion* level.

  AU-C section 315 defines relevant assertion level as follows:

  > A financial statement assertion that has a reasonable possibility of containing a misstatement or misstatements that would cause the financial statements to be materially misstated. The determination of whether an assertion is a relevant assertion is made without regard to the effect of internal controls.

  ISA 315 defines a relevant assertion as follows:

  > 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 (i.e., the inherent risk).

  In connection with the approval of ISA 315, the IAASB approved the following conforming amendment to ISA 200:

  > *Risk of Material Misstatement* (Ref: Para. 13(n))
  >
  > A15a. For the purposes of the ISAs, a risk of material misstatement exists when:
  >
  > (a) There is a reasonable possibility of a misstatement occurring (i.e., its likelihood); and
  >
  > (b) If it were to occur, there is a reasonable possibility of the misstatement being material (i.e., its magnitude).

- For sections of the standard that involve iterative aspects, is the iterative nature of the auditor's risk assessment process clearly explained? For example., using significant classes of transactions, account balances, and disclosures identification to scope the information and communications component of ICFR, then finalizing the identification of relevant assertions and significant classes of transaction, account balances, and disclosures when reaching conclusions on the risks of material misstatements and assessing them.

- Par 51—A Task Force member raised a question as to whether this requirement contradicts the AICPA Audit Sampling Guide, which allows some "credit" for design effectiveness. Will this change, if adopted by the ASB, result in a need to eliminate this from the Audit Sampling Guide? Paragraph 3.26 of the Audit Sampling Guide reads as follows:

  > When the auditor has performed only an assessment of design and implementation and assessed the design as effective and has obtained evidence that the controls have been implemented, the auditor might use a slightly lower confidence level for detailed substantive procedures (for example, 92 percent or 93 percent rather than a 95 percent confidence level if that was the level that the auditor would have otherwise planned for tests of details had the design or implementation of controls been assessed as ineffective).
  >
  > It may be that this is intended merely as a modification to the extent of further audit procedures (specifically, substantive procedures) rather than a reduction in control risk, but it will be important to be clear as to how this approach complies with the revised 315.

- Alignment with AU-C 940—The Task Force needs to consider the impact between ISA 315 and AU-C 940.

Questions for the ASB

6. What are the ASB's views with respect to a) the requirement to assess the risks of material misstatement at the [relevant] assertion level, b) differences between ISA 315 and AU-C 315 with respect to the definition of relevant assertions, c) the implications for the Audit Sampling Audit Guide of assessing control risk in the manner prescribed in paragraph 51 (i.e., such that ROMM = inherent risk) unless the auditor plans to test the operating effectiveness of controls, and d) alignment with AU-C 940?

V. Paragraph 18 of AU-C 330

In the ASB comment letter in response to the exposure draft of the proposed ISA 315, the ASB included the following comment:

> Paragraph 18 of ISA 330 states: "Irrespective of the assessed risks of material misstatement, the auditor shall design and perform substantive procedures for each material class of transactions, account balance, and disclosure." We believe that this requirement is counterintuitive to, and may undermine the effectiveness of, the risk assessment process in ISA 315, particularly in view of the enhancements being proposed by ED-315. That is, the auditor is required to identify and assess the risks of material misstatement in order to design tailored audit responses. In addition, the stand-back requirement in ED-315 paragraph 52 provides an opportunity to again consider the assessed risks, with a specific focus on material classes of transactions, account balances, and disclosures that the auditor has not identified as significant. If an auditor would be required to perform substantive audit procedures regardless of the assessment of risks of material misstatement under ISA 315, then the objective of performing the work effort under ISA 315 could be questioned. Accordingly, we recommend that paragraph 18 of ISA 330 be eliminated.

In addition, if paragraph 18 of ISA 330 is retained, we recommend application material be added to provide guidance as to how the auditor should determine which assertions should be addressed in designing and performing further audit procedures, given that this requirement only applies to classes of transactions, account balances and disclosures that the auditor has determined, through the ISA 315 process, do not contain relevant assertions.

The Task Force thus continues to believe that, given the risk assessment required under AU-C 315, this paragraph is not necessary, notwithstanding the significance of the divergence from ISA 330.

Also, under AU-C 315 and AU-C 330, the auditor is required to assess the risks of material misstatement at the *relevant* assertion level and design and perform further audit procedures for all *relevant* assertions related to each material class of transactions, account balance, and disclosure. AU-C 315 and 330 state the following:

AU-C 315

.26 To provide a basis for designing and performing further audit procedures, the auditor should identify and assess the risks of material misstatement at

a. the financial statement level and (Ref: par. .A122–.A125)

b. the relevant assertion level for classes of transactions, account balances, and disclosures. (Ref: par. .A126–.A133)

AU-C 330

.18 Irrespective of the assessed risks of material misstatement, the auditor should design and perform substantive procedures for all relevant assertions related to each material class of transactions, account balance, and disclosure. (Ref: par. .A45–.A50)

This is a difference that exist between the extant ISAs and extant AU-Cs. As a result, if the ASB decides to retain paragraph 18 of AU-C 330, the Task Force would recommend maintaining the construct in extant AU-C 315 and AU-C 330.

Questions for the ASB

7. What are the ASB's views with respect to the Task Force's views to eliminate paragraph 18 of AU-C 318?

Appendix

Q&A Section 8200

[TQAs No. 17-19 intentionally omitted]

20. Control Activities That Are Always Relevant to the Audit

Inquiry—The auditor is required to obtain an understanding of control activities relevant to the audit, including the process of reconciling detailed records to the general ledger for material account balances.[13] What control activities are always considered to be relevant in every audit?

Reply—As discussed in AU-C section 315, control activities relevant to the audit are "…those control activities the auditor judges it necessary to understand in order to make a preliminary assessment of control risk which together with the assessment of inherent risk comprise the risks of material misstatement at the assertion level and design further audit procedures responsive to assessed risks."[14] However, there are situations in which the auditor would be required to consider control activities relevant to the audit and, accordingly, obtain an understanding of those control activities. The following are controls activities that, if present, are always relevant to the audit:

- Control activities that address significant risks[15]
- Control activities, relevant to fraud risks,[16]
- Control activities that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence[17](note that in such circumstance, the operating effectiveness of the control is required to be tested)[18]
- Control activities that address risks for which the auditor intends to rely on the operating effectiveness of controls in determining the nature, timing, and extent of substantive procedures[19]
- Control activities over journal entries, including nonstandard journal entries used to record nonrecurring, unusual transactions, or adjustments[20]

For control activities determined to be relevant to the audit whether required by the standards or based on auditor judgment, the auditor should understand how the entity has responded to risks

[13] Paragraph 21 of AU-C section 315
[14] Paragraph 21 of AU-C section 315
[15] Paragraph 30 of AU-C section 315
[16] Paragraph 27 of AU-C section 240, *Consideration of Fraud in a Financial Statement Audit*
[17] Paragraph 31 of AU-C section 315
[`18] Paragraph 8 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*
[19] Paragraph .A101 of AU-C section 315 and paragraph 8a of AU-C section 330
[20] Paragraph 19f of AU-C section 315

arising from IT which may impact the design or implementation of the entity's control activities.[21] In addition, if applicable to the audit, control activities meeting any of the criteria stated above over the entity's use of a service organization are relevant to the audit.[22]

[Issue Date: April 2017]

21. Control Activities That May Be Relevant to the Audit

Inquiry— What are the control activities that may vary from audit engagement to audit engagement and may be relevant to the audit (based on the auditor's judgment)?

Reply— In addition to the controls activities that are always relevant to the audit, other control activities may exist that might be considered relevant to the audit by the auditor based on his or her professional judgment.[23] An audit does not require an understanding of all control activities related to each significant class of transactions, account, balance, and disclosure in the financial statements, or to every assertion relevant to them.[24] The control activities relevant to the audit will vary according to the nature, size, and complexity of the entity and its operations and the circumstances of the engagement. For example, the concepts underlying control activities in smaller entities are likely to be similar to those in larger entities, but the formality with which they operate may vary. The following factors may assist the auditor in identifying whether other control activities are relevant to the audit:

- Materiality and inherent risk (for example, the auditor's emphasis may be on identifying and obtaining an understanding of control activities that address the areas in which the auditor considers that risks of material misstatement are likely to be higher[25])
- The understanding of other internal control components (for example, the presence or absence of control activities obtained from the understanding of other components of internal control assists the auditor in determining whether it is necessary to devote additional attention to obtaining an understanding of control activities[26])
- The implementation of any new systems and the effectiveness of general IT controls (for example, deficiencies in general IT controls may have an effect on the effective design and operation of application controls[27])
- Lack of segregation of duties (for example, in a smaller entity, fewer employees may limit the extent to which segregation of duties is possible; relevant control activities may be more limited to, for example, understanding controls performed by management)

[21] Paragraph 22 of AU-C section 315
[22] Paragraph 10 of AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization*
[23] Paragraph .A100 of AU-C section 315.
[24] Paragraph 21 of AU-C section 315.
[25] Paragraphs A101 and 102 of AU-C section 315
[26] Paragraph A103 of AU-C section 315
[27] Paragraph A108 of AU-C section 315

- Legal and regulatory requirements (for example, governmental entities often have additional responsibilities with respect to internal control[28])

The following are controls activities that may be considered relevant to the audit (based on the factors listed above):

- Control activities over the completeness and accuracy of information produced by the entity if the auditor intends to make use of the information in designing and performing further audit procedures[29]
- Control activities relating to operations or compliance objectives if such controls relate to data the auditor evaluates or uses in applying audit procedures[30]
- Control activities over safeguarding of assets to the extent such controls are relevant to the reliability of financial reporting[31]
- Control activities that are dependent on other controls (that is, indirect controls)[32]

[Issue Date: April 2017]

[28] Paragraph A74 of AU-C section 315
[29] Paragraph A70 of AU-C section 315
[30] Paragraph A71 of AU-C section 315
[31] Paragraph A72 of AU-C section 315
[32] Paragraph 10b of AU-C section 330