INTERNATIONAL STANDARD ON AUDITING 315 (REVISED 2019)

IDENTIFYING AND ASSESSING THE RISKS OF MATERIAL MISSTATEMENT

(Effective for audits of financial statements for periods beginning on or after December 15, 2021)

CONTENTS

	Paragraph
Introduction	
Scope of this ISA	1
Key Concepts	2
Scalability	9
Effective Date	10
Objective	11
Definitions	12
Requirements	
Risk Assessment Pocedures and Related Activities	13–18
Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework and the Entity's System of Internal Control	19–27
Identifying and Assessing the Risks of Material Misstatement	28–37
Documentation	38
Application and Other Explanatory Material	
Definitions	A1–A10
Risk Assessment Procedures and Related Activities	A11–A47
Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework and the Entity's System of Internal Control	A48–A183
Identifying and Assessing the Risks of Material Misstatement	A184–A236
Documentation	A237–A241

Appendix 1: Considerations for Understanding the Entity and its Business Model

Appendix 2: Understanding Inherent Risk Factors

Appendix 3: Understanding the Entity's System of Internal Control

Appendix 4: Considerations for Understanding an Entity's Internal Audit Function

Appendix 5: Considerations for Understanding Information Technology (IT)

Appendix 6: Considerations for Understanding General IT Controls

---

International Standard on Auditing (ISA) 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement*, should be read in conjunction with ISA 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*.

Introduction

Scope of this ISA

1. This International Standard on Auditing (ISA) deals with the auditor's responsibility to identify and assess the risks of material misstatement in the financial statements.

Key Concepts in this ISA

2. ISA 200 deals with the overall objectives of the auditor in conducting an audit of the financial statements,[1] including to obtain sufficient appropriate audit evidence to reduce audit risk to an acceptably low level.[2] Audit risk is a function of the risks of material misstatement and detection risk.[3] ISA 200 explains that the risks of material misstatement may exist at two levels:[4] the overall financial statement level; and the assertion level for classes of transactions, account balances and disclosures.

3. ISA 200 requires the auditor to exercise professional judgment in planning and performing an audit, and to plan and perform an audit with professional skepticism recognizing that circumstances may exist that cause the financial statements to be materially misstated.[5]

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

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

5. ISA 200 explains that risks of material misstatement are assessed at the assertion level in order to determine the nature, timing and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence.[6] For

ISA

[1] ISA 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*
[2] ISA 200, paragraph 17
[3] ISA 200, paragraph 13(c)
[4] ISA 200, paragraph A36
[5] ISA 200, paragraphs 15–16
[6] ISA 200, paragraph A43a and ISA 330, *The Auditor's Responses to Assessed Risks*, paragraph 6

the identified risks of material misstatement at the assertion level, a separate assessment of inherent risk and control risk is required by this ISA. The degree to which inherent risk varies is referred to in this ISA as the 'spectrum of inherent risk.'

6. Risks of material misstatement identified and assessed by the auditor include both those due to error and those due to fraud. Although both are addressed by this ISA, the significance of fraud is such that further requirements and guidance are included in ISA 240[7] in relation to risk assessment procedures and related activities to obtain information that is used to identify, assess and respond to the risks of material misstatement due to fraud.

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

8. ISA 330 requires the auditor to design and implement overall responses to address the assessed risks of material misstatement at the financial statement level.[8] ISA 330 further explains that the auditor's assessment of the risks of material misstatement at the financial statement level, and the auditor's overall responses, is affected by the auditor's understanding of the control environment. ISA 330 also requires the auditor to design and perform further audit procedures whose nature, timing and extent are based on and are responsive to the assessed risks of material misstatement at the assertion level.[9]

Scalability

9. ISA 200 states that some ISAs include scalability considerations which illustrate the application of the requirements to all entities regardless of whether their nature and circumstances are less complex or more complex.[10] This ISA is intended for audits of all entities, regardless of size or complexity and the application material therefore incorporates specific considerations specific to both less and more complex entities, where appropriate. While the size of an entity may be an indicator of its complexity, some smaller entities may be complex and some larger entities may be less complex.

---

7 ISA 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*

8 ISA 330, paragraph 5

9 ISA 330, paragraph 6

10 ISA 200, paragraph A65a

Effective Date

10. This ISA is effective for audits of financial statements for periods beginning on or after December 15, 2021.

Objective

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

Definitions

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

    (a) *Assertions* – Representations, explicit or otherwise, with respect to the recognition, measurement, presentation and disclosure of information in the financial statements which are inherent in management representing that the financial statements are prepared in accordance with the applicable financial reporting framework. Assertions are used by the auditor to consider the different types of potential misstatements that may occur when identifying, assessing and responding to the risks of material misstatement. (Ref: Para. A1)

    (b) *Business risk* – A risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.

    (c) *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. A2–A5)

        (i) Policies are statements of what should, or should not, be done within the entity to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

        (ii) Procedures are actions to implement policies.

    (d) *General information technology (IT) controls* – Controls over the entity's IT processes that support the continued proper operation of the IT environment, including the continued effective functioning of information processing controls and the integrity of information (i.e., the completeness, accuracy and validity of information) in the entity's information system. Also see the definition of *IT environment*.

(e) *Information processing controls* – Controls relating to the processing of information in IT applications or manual information processes 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). (Ref: Para. A6)

(f) *Inherent risk factors* – Characteristics of events or conditions that affect susceptibility to misstatement, whether due to fraud or error, of an assertion about a class of transactions, account balance or disclosure, before consideration of controls. Such factors may be qualitative or quantitative, and include complexity, subjectivity, change, uncertainty or susceptibility to misstatement due to management bias or other fraud risk factors[11] insofar as they affect inherent risk. (Ref: Para. A7–A8)

(g) *IT environment* – The IT applications and supporting IT infrastructure, as well as the IT processes and personnel involved in those processes, that an entity uses to support business operations and achieve business strategies. For the purposes of this ISA:

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

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

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

(h) *Relevant assertions* – An assertion about a class of transactions, account balance or disclosure is relevant when it has an identified risk of material misstatement. The determination of whether an assertion is a relevant assertion is made before consideration of any related controls (i.e., the inherent risk). (Ref: Para. A9)

(i) *Risks arising from the use of IT* – Susceptibility of information processing controls to ineffective design or operation, or risks to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information) in the entity's information system, due to ineffective design or operation of controls in the entity's IT processes (see IT environment).

[11] ISA 240, paragraphs A24–A27

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

(k) *Significant class of transactions, account balance or disclosure* – A class of transactions, account balance or disclosure for which there is one or more relevant assertions.

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

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

(ii) That is to be treated as a significant risk in accordance with the requirements of other ISAs.[12]

(m) *System of internal control* – The system designed, implemented and maintained by those charged with governance, management and other personnel, to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. For the purposes of the ISAs, the system of internal control consists of five inter-related 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.

Requirements

Risk Assessment Procedures and Related Activities

13. The auditor shall design and perform risk assessment procedures to obtain audit evidence that provides an appropriate basis for: (Ref: Para. A11–A18)

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

(b) The design of further audit procedures in accordance with ISA 330.

[12] ISA 240, paragraph 27 and ISA 550, *Related Parties*, paragraph 18

The auditor shall design and perform risk assessment procedures in a manner that is not biased towards obtaining audit evidence that may be corroborative or towards excluding audit evidence that may be contradictory. (Ref: Para. A14)

14. The risk assessment procedures shall include the following: (Ref: Para. A19–A21)

    (a) Inquiries of management and of other appropriate individuals within the entity, including individuals within the internal audit function (if the function exists). (Ref: Para. A22–A26)

    (b) Analytical procedures. (Ref: Para. A27–A31)

    (c) Observation and inspection. (Ref: Para. A32–A36)

Information from Other Sources

15. In obtaining audit evidence in accordance with paragraph 13, the auditor shall consider information from: (Ref: Para. A37–A38)

    (a) The auditor's procedures regarding acceptance or continuance of the client relationship or the audit engagement; and

    (b) When applicable, other engagements performed by the engagement partner for the entity.

16. When the auditor intends to use information obtained from the auditor's previous experience with the entity and from audit procedures performed in previous audits, the auditor shall evaluate whether such information remains relevant and reliable as audit evidence for the current audit. (Ref: Para. A39–A41)

Engagement Team Discussion

17. The engagement partner and other key engagement team members shall discuss the application of the applicable financial reporting framework and the susceptibility of the entity's financial statements to material misstatement. (Ref: Para. A42–A47)

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

Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework and the Entity's System of Internal Control (Ref: Para. A48–A49)

Understanding the Entity and Its Environment, and the Applicable Financial Reporting Framework (Ref: Para. A50–A55)

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

(a) The following aspects of the entity and its environment:

(i) The entity's organizational structure, ownership and governance, and its business model, including the extent to which the business model integrates the use of IT; (Ref: Para. A56–A67)

(ii) Industry, regulatory and other external factors; (Ref: Para. A68–A73) and

(iii) The measures used, internally and externally, to assess the entity's financial performance; (Ref: Para. A74–A81)

(b) The applicable financial reporting framework, and the entity's accounting policies and the reasons for any changes thereto; (Ref: Para. A82–A84) and

(c) How inherent risk factors affect susceptibility of assertions to misstatement and the degree to which they do so, in the preparation of the financial statements in accordance with the applicable financial reporting framework, based on the understanding obtained in (a) and (b). (Ref: Para. A85–A89)

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

Understanding the Components of the Entity's System of Internal Control (Ref: Para. A90 – A95)

Control Environment, the Entity's Risk Assessment Process and the Entity's Process to Monitor the System of Internal Control (Ref: Para. A96–A98)

Control environment

<table>
<tr><td colspan="2">21. 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. A99–A100)</td></tr>
<tr><td>(a) Understanding the set of controls, processes and structures that address: (Ref: Para. A101–A102)

(i) How management's oversight responsibilities are carried out, such as the entity's culture and management's commitment to integrity and ethical values;</td><td>and

(b) Evaluating whether: (Ref: Para. A103–A108)

(i) Management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior;</td></tr>
</table>

(ii) When those charged with governance are separate from management, the independence of, and oversight over the entity's system of internal control by, those charged with governance; (iii) The entity's assignment of authority and responsibility; (iv) How the entity attracts, develops, and retains competent individuals; and (v) How the entity holds individuals accountable for their responsibilities in the pursuit of the objectives of the system of internal control;	(ii) The control environment provides an appropriate foundation for the other components of the entity's system of internal control considering the nature and complexity of the entity; and (iii) Control deficiencies identified in the control environment undermine the other components of the entity's system of internal control.

The entity's risk assessment process

22. The auditor 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. A109–A110) (i) Identifying business risks relevant to financial reporting objectives; (Ref: Para. A62) (ii) Assessing the significance of those risks, including the likelihood of their occurrence; and (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. A111–A113)

23. 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 22(b).

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

<table>
<tr><td colspan="2">24. 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. A114–A115)</td></tr>
<tr><td>(a) Understanding those aspects of the entity's process that address:
(i) Ongoing and separate evaluations for monitoring the effectiveness of controls, and the identification and remediation of control deficiencies identified; (Ref: Para. A116–A117) and
(ii) The entity's internal audit function, if any, including its nature, responsibilities and activities; (Ref: Para. A118)
(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. A119–A120)</td><td>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. (Ref: Para. A121–A122)</td></tr>
</table>

Information System and Communication, and Control Activities (Ref: Para. A123–A130)

The information system and communication

25. 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. A131)

(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. A132–A143)

(i) How information flows through the entity's information system, including how:

a. Transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger and reported in the financial statements; and

b. Information about events and conditions, other than transactions, is captured, processed and disclosed in the financial statements;

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. A146)

(ii) The accounting records, specific accounts in the financial statements and other supporting records relating to the flows of information in the information system; (iii) The financial reporting process used to prepare the entity's financial statements, including disclosures; and (iv) The entity's resources, including the IT environment, relevant to (a)(i) to (a)(iii) above; (b) Understanding how the entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control: (Ref: Para. A144–A145) (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;	

Control activities

26. The auditor shall obtain an understanding of the control activities component, through performing risk assessment procedures, by: (Ref: Para. A147–A157)

(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. A158–A159)

(ii) Controls over journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments; (Ref: Para. A160–A161)

(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 that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence; and (Ref: Para. A162–A164)

and

(d) For each control identified in (a) or (c)(ii): (Ref: Para. A175–A181)

(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

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

(iii) Other controls that the auditor considers are appropriate to enable the auditor to meet the objectives of paragraph 13 with respect to risks at the assertion level, based on the auditor's professional judgment; (Ref: Para. A165) (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. A166–A172) (c) For such IT applications and other aspects of the IT environment identified in (b), identifying: (Ref: Para. A173–A174) (i) The related risks arising from the use of IT; and (ii) The entity's general IT controls that address such risks;	

Control Deficiencies Within the Entity's System of Internal Control

27. Based on the auditor's evaluation of each of the components of the entity's system of internal control, the auditor shall determine whether one or more control deficiencies have been identified. (Ref: Para. A182–A183)

Identifying and Assessing the Risks of Material Misstatement (Ref: Para. A184–A185)

Identifying Risks of Material Misstatement

28. The auditor shall identify the risks of material misstatement and determine whether they exist at: (Ref: Para. A186–A192)

(a) The financial statement level; (Ref: Para. A193–A200) or

(b) The assertion level for classes of transactions, account balances and disclosures. (Ref: Para. A201)

29. The auditor shall determine the relevant assertions and the related significant classes of transactions, account balances and disclosures. (Ref: Para. A202–A204)

Assessing Risks of Material Misstatement at the Financial Statement Level

30. For identified risks of material misstatement at the financial statement level, the auditor shall assess the risks and: (Ref: Para. A193–A200)

(a) Determine whether such risks affect the assessment of risks at the assertion level; and

(b) Evaluate the nature and extent of their pervasive effect on the financial statements.

Assessing Risks of Material Misstatement at the Assertion Level

Assessing Inherent Risk (Ref: Para. A205–A217)

31. For identified risks of material misstatement at the assertion level, 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:

(a) Inherent risk factors affect the susceptibility of relevant assertions to misstatement; and

(b) The risks of material misstatement at the financial statement level affect the assessment of inherent risk for risks of material misstatement at the assertion level. (Ref: Para. A215–A216)

32. The auditor shall determine whether any of the assessed risks of material misstatement are significant risks. (Ref: Para. A218–A221)

33. 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. A222–A225)

Assessing Control Risk

34. 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. A226–A229)

Evaluating the Audit Evidence Obtained from the Risk Assessment Procedures

35. 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 been 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. A230–A232)

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

36. For material classes of transactions, account balances or disclosures that have not been determined to be significant classes of transactions, account balances or disclosures, the auditor shall evaluate whether the auditor's determination remains appropriate. (Ref: Para. A233–A235)

Revision of Risk Assessment

37. 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. A236)

Documentation

38. The auditor shall include in the audit documentation:[13] (Ref: Para. A237–A241)

    (a) The discussion among the engagement team and the significant decisions reached;

    (b) Key elements of the auditor's understanding in accordance with paragraphs 19, 21, 22, 24 and 25; the sources of information from which the auditor's understanding was obtained; and the risk assessment procedures performed;

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

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

[13] ISA 230, *Audit Documentation*, paragraphs 8–11, and A6–A7

Application and Other Explanatory Material

Definitions (Ref: Para. 12)

Assertions (Ref: Para. 12(a))

A1. Categories of assertions are used by auditors to consider the different types of potential misstatements that may occur when identifying, assessing and responding to the risks of material misstatement. Examples of these categories of assertions are described in paragraph A190. The assertions differ from the written representations required by ISA 580,[14] to confirm certain matters or support other audit evidence.

Controls (Ref: Para. 12(c))

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

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

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

A5. Controls may be direct or indirect. Direct controls are controls that are precise enough to address risks of material misstatement at the assertion level. Indirect controls are controls that support direct controls.

Information Processing Controls (Ref: Para. 12(e))

A6. Risks to the integrity of information arise from susceptibility to ineffective implementation of the entity's information policies, which are policies that define the information flows, records and reporting processes in the entity's information system. Information processing controls are procedures that support effective implementation of the entity's information policies. Information processing controls may be automated (i.e., embedded in IT applications) or manual (e.g., input or output controls) and may rely on other controls, including other information processing controls or general IT controls.

Inherent Risk Factors (Ref: Para. 12(f))

Appendix 2 sets out further considerations relating to understanding inherent risk factors.

[14] ISA 580, *Written Representations*

A7. Inherent risk factors may be qualitative or quantitative and affect the susceptibility of assertions to misstatement. Qualitative inherent risk factors relating to the preparation of information required by the applicable financial reporting framework include:

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

A8. Other inherent risk factors, that affect susceptibility to misstatement of an assertion about a class of transactions, account balance or disclosure may include:

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

Relevant Assertions (Ref: Para. 12(h))

A9. A risk of material misstatement may relate to more than one assertion, in which case all the assertions to which such a risk relates are relevant assertions. If an assertion does not have an identified risk of material misstatement, then it is not a relevant assertion.

Significant Risk (Ref: Para. 12(l))

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. 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.

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

A11. The risks of material misstatement to be identified and assessed include both those due to fraud and those due to error, and both are covered by this ISA. However, the significance of fraud is such that further requirements and guidance are included in ISA 240 in relation to risk assessment procedures and related activities to obtain information that is used to identify and assess the

risks of material misstatement due to fraud.[15] In addition, the following ISAs provide further requirements and guidance on identifying and assessing risks of material misstatement regarding specific matters or circumstances:

- ISA 540 (Revised)[16] in regard to accounting estimates;
- ISA 550 in regard to related party relationships and transactions;
- ISA 570 (Revised)[17] in regard to going concern; and
- ISA 600[18] in regard to group financial statements.

A12. Professional skepticism is necessary for the critical assessment of audit evidence gathered when performing the risk assessment procedures, and assists the auditor in remaining alert to audit evidence that is not biased towards corroborating the existence of risks or that may be contradictory to the existence of risks. Professional skepticism is an attitude that is applied by the auditor when making professional judgments that then provides the basis for the auditor's actions. The auditor applies professional judgment in determining when the auditor has audit evidence that provides an appropriate basis for risk assessment.

A13. The application of professional skepticism by the auditor may include:

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

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

A14. Designing and performing risk assessment procedures to obtain audit evidence to support the identification and assessment of the risks of material misstatement in an unbiased manner may assist the auditor in identifying potentially contradictory information, which may assist the auditor in exercising professional skepticism in identifying and assessing the risks of material misstatement.

---

15 ISA 240, paragraphs 12–27

16 ISA 540 (Revised), *Auditing Accounting Estimates and Related Disclosures*

17 ISA 570 (Revised), *Going Concern*

18 ISA 600, *Special Considerations—Audits of Group Financial Statements (Including the Work of Component Auditors)*

Sources of Audit Evidence (Ref: Para. 13)

A15. Designing and performing risk assessment procedures to obtain audit evidence in an unbiased manner may involve obtaining evidence from multiple sources within and outside the entity. However, the auditor is not required to perform an exhaustive search to identify all possible sources of audit evidence. In addition to information from other sources[19], sources of information for risk assessment procedures may include:

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

Regardless of the source of information, the auditor considers the relevance and reliability of the information to be used as audit evidence in accordance with ISA 500.[20]

Scalability (Ref: Para. 13)

A16. The nature and extent of risk assessment procedures will vary based on the nature and circumstances of the entity (e.g., the formality of the entity's policies and procedures, and processes and systems). The auditor uses professional judgment to determine the nature and extent of the risk assessment procedures to be performed to meet the requirements of this ISA.

A17. Although the extent to which an entity's policies and procedures, and processes and systems are formalized may vary, the auditor is still required to obtain the understanding in accordance with paragraphs 19, 21, 22, 24, 25 and 26.

Examples:

Some entities, including less complex entities, and particularly owner-managed entities, may not have established structured processes and systems (e.g., a risk assessment process or a process to monitor the system of internal control) or may have established processes or systems with limited documentation or a lack of consistency in how they are undertaken. When such systems and processes lack formality, the auditor may still be able to perform risk assessment procedures through observation and inquiry.

Other entities, typically more complex entities, are expected to have more formalized and documented policies and procedures. The auditor may use such documentation in performing risk assessment procedures.

ISA

[19] See paragraphs A37 and A38.

[20] ISA 500, *Audit Evidence*, paragraph 7

A18. The nature and extent of risk assessment procedures to be performed the first time an engagement is undertaken may be more extensive than procedures for a recurring engagement. In subsequent periods, the auditor may focus on changes that have occurred since the preceding period.

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

A19. ISA 500[21] explains the types of audit procedures that may be performed in obtaining audit evidence from risk assessment procedures and further audit procedures. The nature, timing and extent of the audit procedures may be affected by the fact that some of the accounting data and other evidence may only be available in electronic form or only at certain points in time.[22] The auditor may perform substantive procedures or tests of controls, in accordance with ISA 330, concurrently with risk assessment procedures, when it is efficient to do so. Audit evidence obtained that supports the identification and assessment of risks of material misstatement may also support the detection of misstatements at the assertion level or the evaluation of the operating effectiveness of controls.

A20. Although the auditor is required to perform all the risk assessment procedures described in paragraph 14 in the course of obtaining the required understanding of the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control (see paragraphs 19–26), the auditor is not required to perform all of them for each aspect of that understanding. Other procedures may be performed when the information to be obtained may be helpful in identifying risks of material misstatement. Examples of such procedures may include making inquiries of the entity's external legal counsel or external supervisors, or of valuation experts that the entity has used.

Automated Tools and Techniques (Ref: Para. 14)

A21. Using automated tools and techniques, the auditor may perform risk assessment procedures on large volumes of data (from the general ledger, sub-ledgers or other operational data) including for analysis, recalculations, reperformance or reconciliations.

Inquiries of Management and Others within the Entity (Ref: Para. 14(a))

Why Inquiries Are Made of Management and Others Within the Entity

A22. Information obtained by the auditor to support an appropriate basis for the identification and assessment of risks, and the design of further audit procedures, may be obtained through inquiries of management and those responsible for financial reporting.

A23. Inquiries of management and those responsible for financial reporting and of other appropriate individuals within the entity and other employees with

[21] ISA 500, paragraphs A14–A17 and A21–A25

[22] ISA 500, paragraph A12

different levels of authority may offer the auditor varying perspectives when identifying and assessing risks of material misstatement.

Examples:

- Inquiries directed towards those charged with governance may help the auditor understand the extent of oversight by those charged with governance over the preparation of the financial statements by management. ISA 260 (Revised)[23] identifies the importance of effective two-way communication in assisting the auditor to obtain information from those charged with governance in this regard.
- Inquiries of employees responsible for initiating, processing or recording complex or unusual transactions may help the auditor to evaluate the appropriateness of the selection and application of certain accounting policies.
- Inquiries directed towards in-house legal counsel may provide information about such matters as litigation, compliance with laws and regulations, knowledge of fraud or suspected fraud affecting the entity, warranties, post-sales obligations, arrangements (such as joint ventures) with business partners, and the meaning of contractual terms.
- Inquiries directed towards marketing or sales personnel may provide information about changes in the entity's marketing strategies, sales trends, or contractual arrangements with its customers.
- Inquiries directed towards the risk management function (or inquiries of those performing such roles) may provide information about operational and regulatory risks that may affect financial reporting.
- Inquiries directed towards IT personnel may provide information about system changes, system or control failures, or other IT-related risks.

Considerations Specific to Public Sector Entities

A24. When making inquiries of those who may have information that is likely to assist in identifying risks of material misstatement, auditors of public sector entities may obtain information from additional sources such as from the auditors that are involved in performance or other audits related to the entity.

Inquiries of the Internal Audit Function

Appendix 4 sets out considerations for understanding an entity's internal audit function.

[23] ISA 260 (Revised), *Communication with Those Charged with Governance,* paragraph 4(b)

Why inquiries are made of the internal audit function (if the function exists)

A25. If an entity has an internal audit function, inquiries of the appropriate individuals within the function may assist the auditor in understanding the entity and its environment, and the entity's system of internal control, in the identification and assessment of risks.

Considerations specific to public sector entities

A26. Auditors of public sector entities often have additional responsibilities with regard to internal control and compliance with applicable laws and regulations. Inquiries of appropriate individuals in the internal audit function may assist the auditors in identifying the risk of material non-compliance with applicable laws and regulations, and the risk of control deficiencies related to financial reporting.

Analytical Procedures (Ref: Para. 14(b))

Why Analytical Procedures Are Performed as a Risk Assessment Procedure

A27. Analytical procedures help identify inconsistencies, unusual transactions or events, and amounts, ratios, and trends that indicate matters that may have audit implications. Unusual or unexpected relationships that are identified may assist the auditor in identifying risks of material misstatement, especially risks of material misstatement due to fraud.

A28. Analytical procedures performed as risk assessment procedures may therefore assist in identifying and assessing the risks of material misstatement by identifying aspects of the entity of which the auditor was unaware or understanding how inherent risk factors, such as change, affect susceptibility of assertions to misstatement.

Types of Analytical Procedures

A29. Analytical procedures performed as risk assessment procedures may:

- Include both financial and non-financial information, for example, the relationship between sales and square footage of selling space or volume of goods sold (non-financial).
- Use data aggregated at a high level. Accordingly, the results of those analytical procedures may provide a broad initial indication about the likelihood of a material misstatement.

> **Example**:
>
> In the audit of many entities, including those with less complex business models and processes, and a less complex information system, the auditor may perform a simple comparison of information, such as the change in interim or monthly account balances from balances in prior periods, to obtain an indication of potentially higher risk areas.

A30. This ISA deals with the auditor's use of analytical procedures as risk assessment procedures. ISA 520[24] deals with the auditor's use of analytical procedures as substantive procedures ("substantive analytical procedures") and the auditor's responsibility to perform analytical procedures near the end of the audit. Accordingly, analytical procedures performed as risk assessment procedures are not required to be performed in accordance with the requirements of ISA 520. However, the requirements and application material in ISA 520 may provide useful guidance to the auditor when performing analytical procedures as part of the risk assessment procedures.

Automated tools and techniques

A31. Analytical procedures can be performed using a number of tools or techniques, which may be automated. Applying automated analytical procedures to the data may be referred to as data analytics.

> **Example**:
>
> The auditor may use a spreadsheet to perform a comparison of actual recorded amounts to budgeted amounts, or may perform a more advanced procedure by extracting data from the entity's information system, and further analyzing this data using visualization techniques to identify classes of transactions, account balances or disclosures for which further specific risk assessment procedures may be warranted.

Observation and Inspection (Ref: Para. 14(c))

Why Observation and Inspection Are Performed as Risk Assessment Procedures

A32. Observation and inspection may support, corroborate or contradict inquiries of management and others, and may also provide information about the entity and its environment.

Scalability

A33. Where policies or procedures are not documented, or the entity has less formalized controls, the auditor may still be able to obtain some audit evidence to support the identification and assessment of the risks of material misstatement through observation or inspection of the performance of the control.

> **Examples**:
>
> - The auditor may obtain an understanding of controls over an inventory count, even if they have not been documented by the entity, through direct observation.
> - The auditor may be able to observe segregation of duties.
> - The auditor may be able to observe passwords being entered.

[24] ISA 520, *Analytical Procedures*

Observation and Inspection as Risk Assessment Procedures

A34. Risk assessment procedures may include observation or inspection of the following:

- The entity's operations.
- Internal documents (such as business plans and strategies), records, and internal control manuals.
- Reports prepared by management (such as quarterly management reports and interim financial statements) and those charged with governance (such as minutes of board of directors' meetings).
- The entity's premises and plant facilities.
- Information obtained from external sources such as trade and economic journals; reports by analysts, banks, or rating agencies; regulatory or financial publications; or other external documents about the entity's financial performance (such as those referred to in paragraph A79).
- The behaviors and actions of management or those charged with governance (such as the observation of an audit committee meeting).

Automated tools and techniques

A35. Automated tools or techniques may also be used to observe or inspect, in particular assets, for example through the use of remote observation tools (e.g., a drone).

Considerations Specific to Public Sector Entities

A36. Risk assessment procedures performed by auditors of public sector entities may also include observation and inspection of documents prepared by management for the legislature, for example documents related to mandatory performance reporting.

Information from Other Sources (Ref: Para. 15)

Why the Auditor Considers Information from Other Sources

A37. Information obtained from other sources may be relevant to the identification and assessment of the risks of material misstatement by providing information and insights about:

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

Other Relevant Sources

A38. Other relevant sources of information include:

- The auditor's procedures regarding acceptance or continuance of the client relationship or the audit engagement in accordance with ISA 220, including the conclusions reached thereon.[25]
- Other engagements performed for the entity by the engagement partner. The engagement partner may have obtained knowledge relevant to the audit, including about the entity and its environment, when performing other engagements for the entity. Such engagements may include agreed-upon procedures engagements or other audit or assurance engagements, including engagements to address incremental reporting requirements in the jurisdiction.

Information from the Auditor's Previous Experience with the Entity and Previous Audits (Ref: Para. 16)

Why information from previous audits is important to the current audit

A39. The auditor's previous experience with the entity and from audit procedures performed in previous audits may provide the auditor with information that is relevant to the auditor's determination of the nature and extent of risk assessment procedures, and the identification and assessment of risks of material misstatement.

Nature of the Information from Previous Audits

A40. The auditor's previous experience with the entity and audit procedures performed in previous audits may provide the auditor with information about such matters as:

- Past misstatements and whether they were corrected on a timely basis.
- The nature of the entity and its environment, and the entity's system of internal control (including control deficiencies).
- Significant changes that the entity or its operations may have undergone since the prior financial period.
- Those particular types of transactions and other events or account balances (and related disclosures) where the auditor experienced difficulty in performing the necessary audit procedures, for example, due to their complexity.

A41. The auditor is required to determine whether information obtained from the auditor's previous experience with the entity and from audit procedures performed in previous audits remains relevant and reliable, if the auditor intends

[25] ISA 220, *Quality Control for an Audit of Financial Statements,* paragraph 12

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

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

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

A42. The discussion among the engagement team about the application of the applicable financial reporting framework and the susceptibility of the entity's financial statements to material misstatement:

- Provides an opportunity for more experienced engagement team members, including the engagement partner, to share their insights based on their knowledge of the entity. Sharing information contributes to an enhanced understanding by all engagement team members.
- Allows the engagement team members to exchange information about the business risks to which the entity is subject, how inherent risk factors may affect the susceptibility to misstatement of classes of transactions, account balances and disclosures, and about how and where the financial statements might be susceptible to material misstatement due to fraud or error.
- Assists the engagement team members to gain a better understanding of the potential for material misstatement of the financial statements in the specific areas assigned to them, and to understand how the results of the audit procedures that they perform may affect other aspects of the audit, including the decisions about the nature, timing and extent of further audit procedures. In particular, the discussion assists engagement team members in further considering contradictory information based on each member's own understanding of the nature and circumstances of the entity.
- Provides a basis upon which engagement team members communicate and share new information obtained throughout the audit that may affect the assessment of risks of material misstatement or the audit procedures performed to address these risks.

ISA 240 requires the engagement team discussion to place particular emphasis on how and where the entity's financial statements may be susceptible to material misstatement due to fraud, including how fraud may occur.[26]

[26] ISA 240, paragraph 16

A43. Professional skepticism is necessary for the critical assessment of audit evidence, and a robust and open engagement team discussion, including for recurring audits, may lead to improved identification and assessment of the risks of material misstatement. Another outcome from the discussion may be that the auditor identifies specific areas of the audit for which exercising professional skepticism may be particularly important, and may lead to the involvement of more experienced members of the engagement team who are appropriately skilled to be involved in the performance of audit procedures related to those areas.

Scalability

A44. When the engagement is carried out by a single individual, such as a sole practitioner (i.e., where an engagement team discussion would not be possible), consideration of the matters referred to in paragraphs A42 and A46 nonetheless may assist the auditor in identifying where there may be risks of material misstatement.

A45. When an engagement is carried out by a large engagement team, such as for an audit of group financial statements, it is not always necessary or practical for the discussion to include all members in a single discussion (for example, in a multi-location audit), nor is it necessary for all the members of the engagement team to be informed of all the decisions reached in the discussion. The engagement partner may discuss matters with key members of the engagement team including, if considered appropriate, those with specific skills or knowledge, and those responsible for the audits of components, while delegating discussion with others, taking into account the extent of communication considered necessary throughout the engagement team. A communications plan, agreed by the engagement partner, may be useful.

Discussion of Disclosures in the Applicable Financial Reporting Framework

A46. As part of the discussion among the engagement team, consideration of the disclosure requirements of the applicable financial reporting framework assists in identifying early in the audit where there may be risks of material misstatement in relation to disclosures, even in circumstances where the applicable financial reporting framework only requires simplified disclosures. Matters the engagement team may discuss include:

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

Considerations Specific to Public Sector Entities

A47. As part of the discussion among the engagement team by auditors of public sector entities, consideration may also be given to any additional broader objectives, and related risks, arising from the audit mandate or obligations for public sector entities.

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

Appendices 1 through 6 set out further considerations relating to obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control.

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

A48. Obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control is a dynamic and iterative process of gathering, updating and analyzing information and continues throughout the audit. Therefore, the auditor's expectations may change as new information is obtained.

A49. The auditor's understanding of the entity and its environment and the applicable financial reporting framework may also assist the auditor in developing initial expectations about the classes of transactions, account balances and disclosures that may be significant classes of transactions, account balances and disclosures. These expected significant classes of transactions, account balances and disclosures form the basis for the scope of the auditor's understanding of the entity's information system.

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

A50. The auditor's understanding of the entity and its environment, and the applicable financial reporting framework, assists the auditor in understanding the events and conditions that are relevant to the entity, and in identifying how inherent risk factors affect the susceptibility of assertions to misstatement in the preparation of the financial statements, in accordance with the applicable financial reporting framework, and the degree to which they do so. Such information establishes a frame of reference within which the auditor identifies and assesses risks of material misstatement. This frame of reference also assists the auditor in planning the audit and exercising professional judgment and professional skepticism throughout the audit, for example, when:

- Identifying and assessing risks of material misstatement of the financial statements in accordance with ISA 315 (Revised 2019) or other relevant standards (e.g., relating to risks of fraud in accordance with ISA 240 or

when identifying or assessing risks related to accounting estimates in accordance with ISA 540 (Revised));

- Performing procedures to help identify instances of non-compliance with laws and regulations that may have a material effect on the financial statements in accordance with ISA 250;[27]
- Evaluating whether the financial statements provide adequate disclosures in accordance with ISA 700 (Revised);[28]
- Determining materiality or performance materiality in accordance with ISA 320;[29] or
- Considering the appropriateness of the selection and application of accounting policies, and the adequacy of financial statement disclosures.

A51. The auditor's understanding of the entity and its environment, and the applicable financial reporting framework, also informs how the auditor plans and performs further audit procedures, for example, when:

- Developing expectations for use when performing analytical procedures in accordance with ISA 520;[30]
- Designing and performing further audit procedures to obtain sufficient appropriate audit evidence in accordance with ISA 330; and
- Evaluating the sufficiency and appropriateness of audit evidence obtained (e.g., relating to assumptions or management's oral and written representations).

Scalability

A52. The nature and extent of the required understanding is a matter of the auditor's professional judgment and varies from entity to entity based on the nature and circumstances of the entity, including:

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

A53. The auditor's risk assessment procedures to obtain the required understanding may be less extensive in audits of less complex entities and more extensive for

[27] ISA 250 (Revised), *Consideration of Laws and Regulations in an Audit of Financial Statements,* paragraph 14

[28] ISA 700 (Revised), *Forming an Opinion and Reporting on Financial Statements,* paragraph 13(e)

[29] ISA 320, *Materiality in Planning and Performing an Audit*, paragraphs 10–11

[30] ISA 520, paragraph 5

entities that are more complex. The depth of the understanding that is required by the auditor is expected to be less than that possessed by management in managing the entity.

A54. Some financial reporting frameworks allow smaller entities to provide simpler and less detailed disclosures in the financial statements. However, this does not relieve the auditor of the responsibility to obtain an understanding of the entity and its environment and the applicable financial reporting framework as it applies to the entity.

A55. The entity's use of IT and the nature and extent of changes in the IT environment may also affect the specialized skills that are needed to assist with obtaining the required understanding.

The Entity and Its Environment (Ref: Para. 19(a))

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

The entity's organizational structure and ownership

A56. An understanding of the entity's organizational structure and ownership may enable the auditor to understand such matters as:

- The complexity of the entity's structure.

> **Example**:
>
> The entity may be a single entity or the entity's structure may include subsidiaries, divisions or other components in multiple locations. Further, the legal structure may be different from the operating structure. Complex structures often introduce factors that may give rise to increased susceptibility to risks of material misstatement. Such issues may include whether goodwill, joint ventures, investments, or special-purpose entities are accounted for appropriately and whether adequate disclosure of such issues in the financial statements has been made.

- The ownership, and relationships between owners and other people or entities, including related parties. This understanding may assist in determining whether related party transactions have been appropriately identified, accounted for, and adequately disclosed in the financial statements.[31]
- The distinction between the owners, those charged with governance and management.

[31] ISA 550 establishes requirements and provide guidance on the auditor's considerations relevant to related parties.

Example:

In less complex entities, owners of the entity may be involved in managing the entity, therefore there is little or no distinction. In contrast, such as in some listed entities, there may be a clear distinction between management, the owners of the entity, and those charged with governance.[32]

- The structure and complexity of the entity's IT environment.

Examples:

An entity may:

- Have multiple legacy IT systems in diverse businesses that are not well integrated resulting in a complex IT environment.
- Be using external or internal service providers for aspects of its IT environment (e.g., outsourcing the hosting of its IT environment to a third party or using a shared service centre for central management of IT processes in a group).

Automated tools and techniques

A57. The auditor may use automated tools and techniques to understand flows of transactions and processing as part of the auditor's procedures to understand the information system. An outcome of these procedures may be that the auditor obtains information about the entity's organizational structure or those with whom the entity conducts business (e.g., vendors, customers, related parties).

Considerations specific to public sector entities

A58. Ownership of a public sector entity may not have the same relevance as in the private sector because decisions related to the entity may be made outside of the entity as a result of political processes. Therefore, management may not have control over certain decisions that are made. Matters that may be relevant include understanding the ability of the entity to make unilateral decisions, and the ability of other public sector entities to control or influence the entity's mandate and strategic direction.

Example:

A public sector entity may be subject to laws or other directives from authorities that require it to obtain approval from parties external to the entity of its strategy and objectives prior to it implementing them. Therefore, matters related to understanding the legal structure of the entity may include applicable laws and regulations, and the classification of the entity (i.e., whether the entity is a ministry, department, agency or other type of entity).

ISA

[32] ISA 260 (Revised), paragraphs A1 and A2, provide guidance on the identification of those charged with governance and explains that in some cases, some or all of those charged with governance may be involved in managing the entity.

Governance

Why the auditor obtains an understanding of governance

A59. Understanding the entity's governance may assist the auditor with understanding the entity's ability to provide appropriate oversight of its system of internal control. However, this understanding may also provide evidence of deficiencies, which may indicate an increase in the susceptibility of the entity's financial statements to risks of material misstatement.

Understanding the entity's governance

A60. Matters that may be relevant for the auditor to consider in obtaining an understanding of the governance of the entity include:

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

The Entity's Business Model

Appendix 1 sets out additional considerations for obtaining an understanding of the entity and its business model, as well as additional considerations for auditing special purpose entities.

Why the auditor obtains an understanding of the entity's business model

A61. Understanding the entity's objectives, strategy and business model helps the auditor to understand the entity at a strategic level, and to understand the business risks the entity takes and faces. An understanding of the business risks that have an effect on the financial statements assists the auditor in identifying risks of material misstatement, since most business risks will eventually have financial consequences and, therefore, an effect on the financial statements.

Examples:

An entity's business model may rely on the use of IT in different ways:

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

For both of these entities the business risks arising from a significantly different business model would be substantially different, notwithstanding both entities sell shoes.

Understanding the entity's business model

A62. Not all aspects of the business model are relevant to the auditor's understanding. Business risks are broader than the risks of material misstatement of the financial statements, although business risks include the latter. The auditor does not have a responsibility to understand or identify all business risks because not all business risks give rise to risks of material misstatement.

A63. Business risks increasing the susceptibility to risks of material misstatement may arise from:

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

A64. Examples of matters that the auditor may consider when obtaining an understanding of the entity's business model, objectives, strategies and related business risks that may result in a risk of material misstatement of the financial statements include:

- Industry developments, such as the lack of personnel or expertise to deal with the changes in the industry;

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

A65. Ordinarily, management identifies business risks and develops approaches to address them. Such a risk assessment process is part of the entity's system of internal control and is discussed in paragraph 22, and paragraphs A109–A113.

Considerations specific to public sector entities

A66. Entities operating in the public sector may create and deliver value in different ways to those creating wealth for owners but will still have a 'business model' with a specific objective. Matters public sector auditors may obtain an understanding of that are relevant to the business model of the entity, include:

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

A67. For the audits of public sector entities, "management objectives" may be influenced by requirements to demonstrate public accountability and may include objectives which have their source in law, regulation or other authority.

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

Industry factors

A68. Relevant industry factors include industry conditions such as the competitive environment, supplier and customer relationships, and technological developments. Matters the auditor may consider include:

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

A69. The industry in which the entity operates may give rise to specific risks of material misstatement arising from the nature of the business or the degree of regulation.

> **Example**:
>
> In the construction industry, long-term contracts may involve significant estimates of revenues and expenses that give rise to risks of material misstatement. In such cases, it is important that the engagement team include members with sufficient relevant knowledge and experience.[33]

Regulatory factors

A70. Relevant regulatory factors include the regulatory environment. The regulatory environment encompasses, among other matters, the applicable financial reporting framework and the legal and political environment and any changes thereto. Matters the auditor may consider include:

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

A71. ISA 250 (Revised) includes some specific requirements related to the legal and regulatory framework applicable to the entity and the industry or sector in which the entity operates.[34]

Considerations specific to public sector entities

A72. For the audits of public sector entities, there may be particular laws or regulations that affect the entity's operations. Such elements may be an essential consideration when obtaining an understanding of the entity and its environment.

Other external factors

A73. Other external factors affecting the entity that the auditor may consider include the general economic conditions, interest rates and availability of financing, and inflation or currency revaluation.

---

33 ISA 220, paragraph 14

34 ISA 250 (Revised), paragraph 13

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

Why the auditor understands measures used by management

A74. An understanding of the entity's measures assists the auditor in considering whether such measures, whether used externally or internally, create pressures on the entity to achieve performance targets. These pressures may motivate management to take actions that increase the susceptibility to misstatement due to management bias or fraud (e.g., to improve the business performance or to intentionally misstate the financial statements) (see ISA 240 for requirements and guidance in relation to the risks of fraud).

A75. Measures may also indicate to the auditor the likelihood of risks of material misstatement of related financial statement information. For example, performance measures may indicate that the entity has unusually rapid growth or profitability when compared to that of other entities in the same industry.

Measures used by management

A76. Management and others ordinarily measure and review those matters they regard as important. Inquiries of management may reveal that it relies on certain key indicators, whether publicly available or not, for evaluating financial performance and taking action. In such cases, the auditor may identify relevant performance measures, whether internal or external, by considering the information that the entity uses to manage its business. If such inquiry indicates an absence of performance measurement or review, there may be an increased risk of misstatements not being detected and corrected.

A77. Key indicators used for evaluating financial performance may include:

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

Scalability (Ref: Para. 19(a)(iii))

A78. The procedures undertaken to understand the entity's measures may vary depending on the size or complexity of the entity, as well as the involvement of owners or those charged with governance in the management of the entity.

Examples:

- For some less complex entities, the terms of the entity's bank borrowings (i.e., bank covenants) may be linked to specific performance measures related to the entity's performance or financial position (e.g., a maximum working capital amount). The auditor's understanding of the performance measures used by the bank may help identify areas where there is increased susceptibility to the risk of material misstatement.
- For some entities whose nature and circumstances are more complex, such as those operating in the insurance or banking industries, performance or financial position may be measured against regulatory requirements (e.g., regulatory ratio requirements such as capital adequacy and liquidity ratios performance hurdles). The auditor's understanding of these performance measures may help identify areas where there is increased susceptibility to the risk of material misstatement.

Other considerations

A79. External parties may also review and analyze the entity's financial performance, in particular for entities where financial information is publicly available. The auditor may also consider publicly available information to help the auditor further understand the business or identify contradictory information such as information from:

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

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

A80. The measurement and review of financial performance is not the same as the monitoring of the system of internal control (discussed as a component of the system of internal control in paragraphs A114–A122), though their purposes may overlap:

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

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

Considerations specific to public sector entities

A81. In addition to considering relevant measures used by a public sector entity to assess the entity's financial performance, auditors of public sector entities may also consider non-financial information such as achievement of public benefit outcomes (for example, the number of people assisted by a specific program).

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

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

A82. Matters that the auditor may consider when obtaining an understanding of the entity's applicable financial reporting framework, and how it applies in the context of the nature and circumstances of the entity and its environment include:

- The entity's financial reporting practices in terms of the applicable financial reporting framework, such as:
  - Accounting principles and industry-specific practices, including for industry-specific significant classes of transactions, account balances and related disclosures in the financial statements (for example, loans and investments for banks, or research and development for pharmaceuticals).
  - Revenue recognition.
  - Accounting for financial instruments, including related credit losses.
  - Foreign currency assets, liabilities and transactions.
  - Accounting for unusual or complex transactions including those in controversial or emerging areas (for example, accounting for cryptocurrency).
- An understanding of the entity's selection and application of accounting policies, including any changes thereto as well as the reasons therefore, may encompass such matters as:
  - The methods the entity uses to recognize, measure, present and disclose significant and unusual transactions.
  - The effect of significant accounting policies in controversial or emerging areas for which there is a lack of authoritative guidance or consensus.

- Changes in the environment, such as changes in the applicable financial reporting framework or tax reforms that may necessitate a change in the entity's accounting policies.
- Financial reporting standards and laws and regulations that are new to the entity and when and how the entity will adopt, or comply with, such requirements.

A83. Obtaining an understanding of the entity and its environment may assist the auditor in considering where changes in the entity's financial reporting (e.g., from prior periods) may be expected.

> **Example**:
>
> If the entity has had a significant business combination during the period, the auditor would likely expect changes in classes of transactions, account balances and disclosures associated with that business combination. Alternatively, if there were no significant changes in the financial reporting framework during the period, the auditor's understanding may help confirm that the understanding obtained in the prior period remains applicable.

Considerations specific to public sector entities

A84. The applicable financial reporting framework in a public sector entity is determined by the legislative and regulatory frameworks relevant to each jurisdiction or within each geographical area. Matters that may be considered in the entity's application of the applicable financial reporting requirements, and how it applies in the context of the nature and circumstances of the entity and its environment, include whether the entity applies a full accrual basis of accounting or a cash basis of accounting in accordance with the International Public Sector Accounting Standards, or a hybrid.

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

> **Appendix 2** provides examples of events and conditions that may give rise to the existence of risks of material misstatement, categorized by inherent risk factor.

Why the auditor understands inherent risk factors when understanding the entity and its environment and the applicable financial reporting framework

A85. Understanding the entity and its environment, and the applicable financial reporting framework, assists the auditor in identifying events or conditions, the characteristics of which may affect the susceptibility of assertions about classes of transactions, account balances or disclosures to misstatement. These characteristics are inherent risk factors. Inherent risk factors may affect susceptibility of assertions to misstatement by influencing the likelihood of

occurrence of a misstatement or the magnitude of the misstatement if it were to occur. Understanding how inherent risk factors affect the susceptibility of assertions to misstatement may assist the auditor with a preliminary understanding of the likelihood or magnitude of misstatements, which assists the auditor in identifying risks of material misstatement at the assertion level in accordance with paragraph 28(b). Understanding the degree to which inherent risk factors affect susceptibility of assertions to misstatement also assists the auditor in assessing the likelihood and magnitude of a possible misstatement when assessing inherent risk in accordance with paragraph 31(a). Accordingly, understanding the inherent risk factors may also assist the auditor in designing and performing further audit procedures in accordance with ISA 330.

A86. The auditor's identification of risks of material misstatement at the assertion level and assessment of inherent risk may also be influenced by audit evidence obtained by the auditor in performing other risk assessment procedures, further audit procedures or in fulfilling other requirements in the ISAs (see paragraphs A95, A103, A111, A121, A124 and A151).

The effect of inherent risk factors on a class of transactions, account balance or disclosure

A87. The extent of susceptibility to misstatement of a class of transactions, account balance or disclosure arising from complexity or subjectivity is often closely related to the extent to which it is subject to change or uncertainty.

> **Example**:
>
> If the entity has an accounting estimate that is based on assumptions, the selection of which are subject to significant judgment, the measurement of the accounting estimate is likely to be affected by both subjectivity and uncertainty.

A88. The greater the extent to which a class of transactions, account balance or disclosure is susceptible to misstatement because of complexity or subjectivity, the greater the need for the auditor to apply professional skepticism. Further, when a class of transactions, account balance or disclosure is susceptible to misstatement because of complexity, subjectivity, change or uncertainty, these inherent risk factors may create opportunity for management bias, whether unintentional or intentional, and affect susceptibility to misstatement due to management bias. The auditor's identification of risks of material misstatement, and assessment of inherent risk at the assertion level, are also affected by the interrelationships among inherent risk factors.

A89. Events or conditions that may affect susceptibility to misstatement due to management bias may also affect susceptibility to misstatement due to other fraud risk factors. Accordingly, this may be relevant information for use in accordance with paragraph 24 of ISA 240, which requires the auditor to evaluate whether the information obtained from the other risk assessment procedures and related activities indicates that one or more fraud risk factors are present.

Understanding the Components of the Entity's System of Internal Control (Ref: Para. 21–27)

Appendix 3 further describes the nature of the entity's system of internal control and inherent limitations of internal control, respectively. Appendix 3 also provides further explanation of the components of a system of internal control for the purposes of the ISAs.

A90. The auditor's understanding of the entity's system of internal control is obtained through risk assessment procedures performed to understand and evaluate each of the components of the system of internal control as set out in paragraphs 21 to 27.

A91. The components of the entity's system of internal control for the purpose of this ISA may not necessarily reflect how an entity designs, implements and maintains its system of internal control, or how it may classify any particular component. Entities may use different terminology or frameworks to describe the various aspects of the system of internal control. For the purpose of an audit, auditors may also use different terminology or frameworks provided all the components described in this ISA are addressed.

Scalability

A92. The way in which the entity's system of internal control is designed, implemented and maintained varies with an entity's size and complexity. For example, less complex entities may use less structured or simpler controls (i.e., policies and procedures) to achieve their objectives.

Considerations Specific to Public Sector Entities

A93. Auditors of public sector entities often have additional responsibilities with respect to internal control, for example, to report on compliance with an established code of practice or reporting on spending against budget. Auditors of public sector entities may also have responsibilities to report on compliance with law, regulation or other authority. As a result, their considerations about the system of internal control may be broader and more detailed.

Information Technology in the Components of the Entity's System of Internal Control

Appendix 5 provides further guidance on understanding the entity's use of IT in the components of the system of internal control.

A94. The overall objective and scope of an audit does not differ whether an entity operates in a mainly manual environment, a completely automated environment, or an environment involving some combination of manual and automated elements (i.e., manual and automated controls and other resources used in the entity's system of internal control).

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

A95. In evaluating the effectiveness of the design of controls and whether they have been implemented (see paragraphs A175 to A181) the auditor's understanding of each of the components of the entity's system of internal control provides a preliminary understanding of how the entity identifies business risks and how it responds to them. It may also influence the auditor's identification and assessment of the risks of material misstatement in different ways (see paragraph A86). This assists the auditor in designing and performing further audit procedures, including any plans to test the operating effectiveness of controls. For example:

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

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

A96. The controls in the control environment, the entity's risk assessment process and the entity's process to monitor the system of internal control are primarily indirect controls (i.e., controls that are not sufficiently precise to prevent, detect or correct misstatements at the assertion level but which support other controls and may therefore have an indirect effect on the likelihood that a misstatement will be detected or prevented on a timely basis). However, some controls within these components may also be direct controls.

Why the auditor is required to understand the control environment, the entity's risk assessment process and the entity's process to monitor the system of internal control

A97. The control environment provides an overall foundation for the operation of the other components of the system of internal control. The control environment does not directly prevent, or detect and correct, misstatements. It may, however, influence the effectiveness of controls in the other components of the system of internal control. Similarly, the entity's risk assessment process and its process for monitoring the system of internal control are designed to operate in a manner that also supports the entire system of internal control.

A98. Because these components are foundational to the entity's system of internal control, any deficiencies in their operation could have pervasive effects on the preparation of the financial statements. Therefore, the auditor's understanding and

evaluations of these components affect the auditor's identification and assessment of risks of material misstatement at the financial statement level, and may also affect the identification and assessment of risks of material misstatement at the assertion level. Risks of material misstatement at the financial statement level affect the auditor's design of overall responses, including, as explained in ISA 330, an influence on the nature, timing and extent of the auditor's further procedures.[35]

Obtaining an understanding of the control environment (Ref: Para. 21)

Scalability

A99. 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.

A100. 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 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. 21(a))

A101. 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).

[35] ISA 330, paragraphs A1–A3

A102. 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. 21(b))

Why the auditor evaluates the control environment

A103. 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 A86).

The auditor's evaluation of the control environment

A104. The auditor's evaluation of the control environment is based on the understanding obtained in accordance with paragraph 21(a).

A105. Some entities may be dominated by a single individual who may exercise a great deal of discretion. The actions and attitudes of that individual may have a pervasive effect on the culture of the entity, which in turn may have a pervasive effect on the control environment. Such an effect may be positive or negative.

> **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.

A106. 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.

A107. 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).

A108. 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)).

Obtaining an understanding of the entity's risk assessment process (Ref: Para. 22–23)

Understanding the entity's risk assessment process (Ref: Para. 22(a))

A109. As explained in paragraph A62, 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.[36]

[36] ISA 240, paragraph 19

A110. 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. 22(b))

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

A111. 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 A86).

Evaluating whether the entity's risk assessment process is appropriate (Ref: Para. 22(b))

A112. The auditor's evaluation of the appropriateness of the entity's risk assessment process is based on the understanding obtained in accordance with paragraph 22(a).

Scalability

A113. 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.

Obtaining an understanding of the entity's process to monitor the entity's system of internal control (Ref: Para. 24)

Scalability

A114. In less complex entities, and in particular owner-manager entities, the auditor's understanding of the entity's process to monitor the system of internal control

is often focused on how management or the owner-manager is directly involved in operations, 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.

A115. 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. 24(a))

A116. 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
- How identified deficiencies have been addressed through appropriate remedial actions, including timely communication of such deficiencies to those responsible for taking remedial action.

A117. The auditor may also consider how the entity's process to monitor the system of internal control addresses monitoring information processing controls that involve the use of IT. This may include, for example:

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

Understanding the entity's internal audit function (Ref: Para. 24(a)(ii))

Appendix 4 sets out further considerations for understanding the entity's internal audit function.

A118. 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)[37] applies.

Other sources of information used in the entity's process to monitor the system of internal control

Understanding the sources of information (Ref: Para. 24(b))

A119. 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

A120. 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 (Ref: Para 24(c))

Why the auditor evaluates whether the entity's process to monitor the system of internal control is appropriate

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

A121. 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 A86).

Evaluating whether the entity's process to monitor the system of internal control is appropriate (Ref: Para. 24(c))

A122. The auditor's evaluation of the appropriateness of the entity's process to monitor the system of internal control is based on the auditor's understanding of the entity's process to monitor the system of internal control.

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

A123. The controls in the information system and communication, and control activities components are primarily direct controls (i.e., controls that are sufficiently precise to prevent, detect or correct misstatements at the assertion level).

Why the auditor is required to understand the information system and communication and controls in the control activities component

A124. The auditor is required to understand the entity's information system and communication because understanding the entity's policies that define the flows of transactions and other aspects of the entity's information processing activities relevant to the preparation of the financial statements, and evaluating whether the component appropriately supports the preparation of the entity's financial statements, supports the auditor's identification and assessment of risks of material misstatement at the assertion level. This understanding and evaluation may also result in the identification of risks of material misstatement at the financial statement level when the results of the auditor's procedures are inconsistent with expectations about the entity's system of internal control that may have been set based on information obtained during the engagement acceptance or continuance process (see paragraph A86).

A125. The auditor is required to identify specific controls in the control activities component, and evaluate the design and determine whether the controls have been implemented, as it assists the auditor's understanding about management's approach to addressing certain risks and therefore provides a basis for the design and performance of further audit procedures responsive to these risks as required by ISA 330. The higher on the spectrum of inherent risk a risk is assessed, the more persuasive the audit evidence needs to be. Even when the auditor does not plan to test the operating effectiveness of identified controls, the auditor's understanding may still affect the design of the nature, timing and extent of substantive audit procedures that are responsive to the related risks of material misstatement.

The iterative nature of the auditor's understanding and evaluation of the information system and communication, and control activities

A126. As explained in paragraph A49, the auditor's understanding of the entity and its environment, and the applicable financial reporting framework, may assist the auditor in developing initial expectations about the classes of transactions, account balances and disclosures that may be significant classes of transactions, account balances and disclosures. In obtaining an understanding of the information system and communication component in accordance with paragraph 25(a), the auditor may use these initial expectations for the purpose of determining the extent of understanding of the entity's information processing activities to be obtained.

A127. The auditor's understanding of the information system includes understanding the policies that define flows of information relating to the entity's significant classes of transactions, account balances, and disclosures, and other related aspects of the entity's information processing activities. This information, and the information obtained from the auditor's evaluation of the information system may confirm or further influence the auditor's expectations about the significant classes of transactions, account balances and disclosures initially identified (see paragraph A126).

A128. In obtaining an understanding of how information relating to significant classes of transactions, account balances and disclosures flows into, through, and out of the entity's information system, the auditor may also identify controls in the control activities component that are required to be identified in accordance with paragraph 26(a). The auditor's identification and evaluation of controls in the control activities component may first focus on controls over journal entries and controls that the auditor plans to test the operating effectiveness of in designing the nature, timing and extent of substantive procedures.

A129. The auditor's assessment of inherent risk may also influence the identification of controls in the control activities component. For example, the auditor's identification of controls relating to significant risks may only be identifiable when the auditor has assessed inherent risk at the assertion level in accordance with paragraph 31. Furthermore, controls addressing risks for which the auditor has determined that substantive procedures alone do not provide sufficient appropriate audit evidence (in accordance with paragraph 33) may also only be identifiable once the auditor's inherent risk assessments have been undertaken.

A130. The auditor's identification and assessment of risks of material misstatement at the assertion level is influenced by both the auditor's:

- Understanding of the entity's policies for its information processing activities in the information system and communication component, and
- Identification and evaluation of controls in the control activities component.

Obtaining an understanding of the information system and communication (Ref: Para. 25)

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

Scalability

A131. 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 A86).

Obtaining an understanding of the information system (Ref: Para. 25(a))

A132. Included within the entity's system of internal control are aspects that relate to the entity's reporting objectives, including its financial reporting objectives, but may also include aspects that relate to its operations or compliance objectives, when such aspects are relevant to financial reporting. Understanding how the entity initiates transactions and captures information as part of the auditor's understanding of the information system may include information about the entity's systems (its policies) designed to address compliance and operations objectives because such information is relevant to the preparation of the financial statements. Further, some entities may have information systems that are highly integrated such that controls may be designed in a manner to simultaneously achieve financial reporting, compliance and operational objectives, and combinations thereof.

A133. Understanding the entity's information system also includes an understanding of the resources to be used in the entity's information processing activities. Information about the human resources involved that may be relevant to understanding risks to the integrity of the information system include:

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

A134. 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.

A135. 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.

A136. 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

A137. The auditor may also use automated techniques to obtain direct access to, or a digital download from, the databases in the entity's information system that store accounting records of transactions. By applying automated tools or techniques to this information, the auditor may confirm the understanding obtained about how transactions flow through the information system by tracing journal entries, or other digital records related to a particular transaction, or an entire population of transactions, from initiation in the accounting records through to recording in the general ledger. Analysis of complete or large sets of transactions may also result in the identification of variations from the normal, or expected, processing procedures for these transactions, which may result in the identification of risks of material misstatement.

Information obtained from outside of the general and subsidiary ledgers

A138. 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:
  - Assumptions developed internally that may affect an asset's useful life; or
  - Data such as interest rates that are affected by factors outside the control of the entity.
- Information disclosed in the financial statements about sensitivity analyses derived from financial models that demonstrates that management has considered alternative assumptions.
- Information recognized or disclosed in the financial statements that has been obtained from an entity's tax returns and records.
- Information disclosed in the financial statements that has been obtained from analyses prepared to support management's assessment of the entity's ability to continue as a going concern, such as disclosures, if any, related to events or conditions that have been identified that may cast significant doubt on the entity's ability to continue as a going concern.[38]

A139. 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.

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

The entity's use of information technology in the information system

Why does the auditor understand the IT environment relevant to the information system

A140. 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.

A141. 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

A142. 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.

A143. 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. 25(b))

Scalability

A144. 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.

A145. 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. 25(c))

A146. 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 25(a)–(b).

Control Activities (Ref: Para. 26)

Controls in the control activities component

Appendix 3, Paragraphs 20 and 21 set out further considerations relating to control activities.

A147. 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.

A148. 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.

A149. 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 26. 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.

A150. Paragraph 26 also requires the auditor to identify and evaluate general IT controls for IT applications and other aspects of the IT environment that the auditor has determined to be subject to risks arising from the use of IT, because general IT controls support the continued effective functioning of information

processing controls. A general IT control alone is typically not sufficient to address a risk of material misstatement at the assertion level.

A151. The controls that the auditor is required to identify and evaluate the design, and determine the implementation of, in accordance with paragraph 26 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 A95). 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 13 with respect to risks at the assertion level, based on the auditor's professional judgment.

A152. Controls in the control activities component are required to be identified when such controls meet one or more of the criteria included in paragraph 26(a). However, when multiple controls each achieve the same objective, it is unnecessary to identify each of the controls related to such objective.

Types of controls in the control activities component (Ref: Para. 26)

A153. 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.

A154. 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.

A155. 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. 26)

A156. 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.

A157. 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.[39]

Controls that address risks of material misstatement at the assertion level (Ref: Para. 26(a))

Controls that address risks that are determined to be a significant risk (Ref: Para. 26(a)(i))

A158. 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.[40] 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 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.

[39] ISA 240, paragraph A28

[40] ISA 330, paragraph 21

> **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.

A159. ISA 240[41] 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. 26(a)(ii))

A160. 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 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

A161. 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.

---

[41] ISA 240, paragraphs 28 and A33

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. 26(a)(iii))

A162. 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,[42] to design and perform tests of controls that address such risks of material misstatement when substantive procedures alone do not provide sufficient appropriate audit evidence at the assertion level. As a result, when such controls exist that address these risks, they are required to be identified and evaluated.

A163. In other cases, when the auditor plans to take into account the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures in accordance with ISA 330, such controls are also required to be identified because ISA 330[43] 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.

A164. 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

[42] ISA 330, paragraph 8(b)

[43] ISA 330, paragraph 8(a)

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. 26(a)(iv))

A165. 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.[44]

Identifying IT applications and other aspects of the IT environment, risks arising from the use of IT and general IT controls (Ref: Para. 26(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 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. 26(b))

Why the auditor identifies risks arising from the use of IT and general IT controls related to identified IT applications and other aspects of the IT environment

A166. 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.

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

- 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

A167. 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.

A168. 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.

A169. 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

A170. 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.

A171. 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

A172. 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. 26(c))

Appendix 6 sets out considerations for understanding general IT controls.

A173. 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).

A174. 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 26(d))

A175. 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).

A176. 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.

A177. 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.

A178. The auditor may expect, based on experience from the previous audit or based on current period risk assessment procedures, that management does not have effectively designed or implemented controls to address a significant risk. In such instances, the procedures performed to address the requirement in paragraph 26(d) may consist of determining that such controls have not been effectively designed or implemented. If the results of the procedures indicate that controls have been newly designed or implemented, the auditor is required to perform the procedures in paragraph 26(b)–(d) on the newly designed or implemented controls.

A179. 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.

A180. 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.[45]

A181. 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.

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

A182. In performing the evaluations of each of the components of the entity's system of internal control,[46] the auditor may determine that certain of the entity's

[45] ISA 330, paragraphs 8–11

[46] Paragraphs 21(b), 22(b), 24(c), 25(c) and 26(d)

policies in a component are not appropriate to the nature and circumstances of the entity. Such a determination may be an indicator that assists the auditor in identifying control deficiencies. If the auditor has identified one or more control deficiencies, the auditor may consider the effect of those control deficiencies on the design of further audit procedures in accordance with ISA 330.

A183. If the auditor has identified one or more control deficiencies, ISA 265[47] requires the auditor to determine whether, individually or in combination, the deficiencies constitute a significant deficiency. The auditor uses professional judgment in determining whether a deficiency represents a significant control deficiency.[48]

Examples:

Circumstances that may indicate a significant control deficiency exists include matters such as:

- The identification of fraud of any magnitude that involves senior management;
- Identified internal processes that are inadequate relating to the reporting and communication of deficiencies noted by internal audit;
- Previously communicated deficiencies that are not corrected by management in a timely manner;
- Failure by management to respond to significant risks, for example, by not implementing controls over significant risks; and
- The restatement of previously issued financial statements.

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

Why the Auditor Identifies and Assesses the Risks of Material Misstatement

A184. 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.

A185. 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

47 ISA 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*, paragraph 8

48 ISA 265, paragraphs A6–A7 set out indicators of significant deficiencies, and matters to be considered in determining whether a deficiency, or a combination of deficiencies, in internal control constitute a significant deficiency.

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 (Ref: Para. 28)

A186. The identification of risks of material misstatement is performed before consideration of any related controls (i.e., the inherent risk), and is based on the auditor's preliminary consideration of misstatements that have a reasonable possibility of both occurring, and being material if they were to occur.[49]

A187. 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

A188. 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

A189. In identifying and assessing the risks of material misstatement, the auditor may use the categories of assertions as described in paragraph A190(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.

A190. Assertions used by the auditor in considering the different types of potential misstatements that may occur may fall into the following categories:

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

[49] ISA 200, paragraph A15a

(i) Occurrence—transactions and events that have been recorded or disclosed have occurred, and such transactions and events pertain to the entity.

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

(iii) Accuracy—amounts and other data relating to recorded transactions and events have been recorded appropriately, and related disclosures have been appropriately measured and described.

(iv) Cutoff—transactions and events have been recorded in the correct accounting period.

(v) Classification—transactions and events have been recorded in the proper accounts.

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

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

(i) Existence—assets, liabilities and equity interests exist.

(ii) Rights and obligations—the entity holds or controls the rights to assets, and liabilities are the obligations of the entity.

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

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

(v) Classification—assets, liabilities and equity interests have been recorded in the proper accounts.

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

A191. The assertions described in paragraph A190(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.

Considerations Specific to Public Sector Entities

A192. When making assertions about the financial statements of public sector entities, in addition to those assertions set out in paragraph A190(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. 28(a) and 30)

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

A193. 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.[50]

A194. 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

A195. 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 represent circumstances that may pervasively increase the risks of material misstatement at the assertion level. The auditor's evaluation of whether risks identified relate

[50] ISA 330, paragraph 5

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.

A196. 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 21(b), 22(b), 24(c) and 25(c); and
- Any control deficiencies identified in accordance with paragraph 27.

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

A197. 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 understatement of liabilities and expenses to ensure that financing will be obtained).

A198. 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.

A199. ISA 705 (Revised)[51] 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

A200. 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.

Risks of Material Misstatement at the Assertion Level v(Ref: Para. 28(b))

> **Appendix 2** sets out examples, in the context of inherent risk factors, of events or conditions that may indicate susceptibility to misstatement that may be material.

A201. Risks of material misstatements that do not relate pervasively to the financial statements are risks of material misstatement at the assertion level.

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

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

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

A202. Determining relevant assertions and the significant classes of transactions, account balances and disclosures provides the basis for the scope of the auditor's understanding of the entity's information system required to be obtained in accordance with paragraph 25(a). This understanding may further assist the auditor in identifying and assessing risks of material misstatement (see A86).

Automated Tools and Techniques

A203. 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 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

A204. 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.
- Sensitivity analysis, including the effects of changes in assumptions used in the entity's valuation techniques intended to enable users to understand the underlying measurement uncertainty of a recorded or disclosed amount.

Assessing Risks of Material Misstatement at the Assertion Level

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

Assessing the likelihood and magnitude of misstatement (Ref: Para: 31)

Why the auditor assesses likelihood and magnitude of misstatement

A205. 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.

A206. 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.

A207. 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

A208. In assessing inherent risk, the auditor uses professional judgment in determining the significance of the combination of the likelihood and magnitude of a misstatement.

A209. 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.

A210. 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.

A211. 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).

A212. 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.

A213. For a risk to be assessed as higher on the spectrum of inherent risk, it does not mean that both the magnitude and likelihood need to be assessed as high. Rather, it is the intersection of the magnitude and likelihood of the material misstatement on the spectrum of inherent risk that will determine whether the assessed inherent risk is higher or lower on the spectrum of inherent risk. A higher inherent risk assessment may also arise from different combinations of likelihood and magnitude, for example a higher inherent risk assessment could result from a lower likelihood but a very high magnitude.

A214. 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 31(b))

A215. 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.

A216. In circumstances in which risks of material misstatement are identified as financial statement level risks due to their pervasive effect on a number of

assertions, and are identifiable with specific assertions, the auditor is required to take into account those risks when assessing inherent risk for risks of material misstatement at the assertion level.

Considerations Specific to Public Sector Entities

A217. 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.

Significant Risks (Ref: Para. 32)

Why significant risks are determined and the implications for the audit

A218. 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 of inherent risk, through the performance of certain required responses, including:

- Controls that address significant risks are required to be identified in accordance with paragraph 26(a)(i), with a requirement to evaluate whether the control has been designed effectively and implemented in accordance with paragraph 26(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.[52]
- ISA 330 requires the auditor to obtain more persuasive audit evidence the higher the auditor's assessment of risk.[53]
- ISA 260 (Revised) requires communicating with those charged with governance about the significant risks identified by the auditor.[54]
- 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.[55]
- 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.[56]

52 ISA 330, paragraphs 15 and 21
53 ISA 330, paragraph 7(b)
54 ISA 260 (Revised), paragraph 15
55 ISA 701, *Communicating Key Audit Matters in the Independent Auditor's Report*, paragraph 9
56 ISA 220, paragraphs 17 and A19

- 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.[57]

Determining significant risks

A219. 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.

A220. 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.[58]

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.
- 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.

A221. 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:

[57] ISA 600, paragraphs 30 and 31
[58] ISA 240, paragraphs 26–28

- 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.

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

Why risks for which substantive procedures alone do not provide sufficient appropriate audit evidence are required to be identified

A222. 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.

A223. Paragraph 26(a)(iii) also requires the identification of controls that address risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence because the auditor is required, in accordance with ISA 330,[59] to design and perform tests of such controls.

Determining risks for which substantive procedures alone do not provide sufficient appropriate audit evidence

A224. 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.

[59] ISA 330, paragraph 8

- 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.

A225. ISA 540 (Revised) provides further guidance related to accounting estimates about risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.[60] In relation to accounting estimates this may not be limited to automated processing, but may also be applicable to complex models.

Assessing Control Risk (Ref: Para. 34)

A226. 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 37.

A227. 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.

A228. If the auditor plans to test the operating effectiveness of controls, it may be necessary to test a combination of controls to confirm the auditor's expectation that the controls are operating effectively. The auditor may plan to test both direct and indirect controls, including general IT controls, and, if so, take into account the combined expected effect of the controls when assessing control risk. To the extent that the control to be tested does not fully address the assessed inherent risk , the auditor determines the implications on the design of further audit procedures to reduce audit risk to an acceptably low level.

A229. 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

[60] ISA 540 (Revised), paragraphs A87–A89

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

Evaluating the Audit Evidence Obtained from the Risk Assessment Procedures (Ref: Para 35)

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

A230. 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

A231. Audit evidence from risk assessment procedures comprises both information that supports and corroborates management's assertions, and any information that contradicts such assertions.[62]

Professional Skepticism

A232. In evaluating the audit evidence from the risk assessment procedures, the auditor considers whether sufficient understanding about the entity and its environment, the applicable financial reporting framework and the entity's system of internal control has been obtained to be able to identify the risks of material misstatement, as well as whether there is any evidence that is contradictory that may indicate a risk of material misstatement.

Classes of Transactions, Account Balances and Disclosures that Are Not Significant, but Which Are Material (Ref: Para. 36)

A233. As explained in ISA 320,[63] 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

61 ISA 330, paragraphs A29–A30
62 ISA 500, paragraph A1
63 ISA 320, paragraph A1

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.[64] 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.

A234. 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 A233.

A235. Audit procedures to address classes of transactions, account balances or disclosures that are material but are not determined to be significant are addressed in ISA 330.[65] When a class of transactions, account balance or disclosure is determined to be significant as required by paragraph 29, 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 (Ref: Para. 37)

A236. 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.

[64] ISA 320, paragraph 4
[65] ISA 330, paragraph 18

Documentation (Ref: Para. 38)

A237. For recurring audits, certain documentation may be carried forward, updated as necessary to reflect changes in the entity's business or processes.

A238. ISA 230 notes that, among other considerations, although there may be no single way in which the auditor's exercise of professional skepticism is documented, the audit documentation may nevertheless provide evidence of the auditor's exercise of professional skepticism.[66] For example, when the audit evidence obtained from risk assessment procedures includes evidence that both corroborates and contradicts management's assertions, the documentation may include how the auditor evaluated that evidence, including the professional judgments made in evaluating whether the audit evidence provides an appropriate basis for the auditor's identification and assessment of the risks of material misstatement. Examples of other requirements in this ISA for which documentation may provide evidence of the exercise of professional skepticism by the auditor include:

- Paragraph 13, which requires the auditor to design and perform risk assessment procedures in a manner that is not biased towards obtaining audit evidence that may corroborate the existence of risks or towards excluding audit evidence that may contradict the existence of risks;
- Paragraph 17, which requires a discussion among key engagement team members of the application of the applicable financial reporting framework and the susceptibility of the entity's financial statements to material misstatement;
- Paragraphs 19(b) and 20, which require the auditor to obtain an understanding of the reasons for any changes to the entity's accounting policies and to evaluate whether the entity's accounting policies are appropriate and consistent with the applicable financial reporting framework;
- Paragraphs 21(b), 22(b), 23(b), 24(c), 25(c), 26(d) and 27, which require the auditor to evaluate, based on the required understanding obtained, whether the components of the entity's system of internal control are appropriate to the entity's circumstances considering the nature and complexity of the entity, and to determine whether one of more control deficiencies have been identified;
- Paragraph 35, which requires the auditor to take into account all audit evidence obtained from the risk assessment procedures, whether corroborative or contradictory to assertions made by management, and to evaluate whether the audit evidence obtained from the risk assessment procedures provides an appropriate basis for the identification and assessment of the risks of material misstatement; and

[66] ISA 230, paragraph A7

- Paragraph 36, which requires the auditor to evaluate, when applicable, whether the auditor's determination that there are no risks of material misstatement for a material class of transactions, account balance or disclosure remains appropriate.

Scalability

A239. The manner in which the requirements of paragraph 38 are documented is for the auditor to determine using professional judgment.

A240. More detailed documentation, that is sufficient to enable an experienced auditor, having no previous experience with the audit, to understand the nature, timing and extent of the audit procedures performed, may be required to support the rationale for difficult judgments made.

A241. For the audits of less complex entities, the form and extent of documentation may be simple and relatively brief. The form and extent of the auditor's documentation is influenced by the nature, size and complexity of the entity and its system of internal control, availability of information from the entity and the audit methodology and technology used in the course of the audit. It is not necessary to document the entirety of the auditor's understanding of the entity and matters related to it. Key elements[67] of understanding documented by the auditor may include those on which the auditor based the assessment of the risks of material misstatement. However, the auditor is not required to document every inherent risk factor that was taken into account in identifying and assessing the risks of material misstatement at the assertion level.

Example:

In audits of less complex entities audit documentation may be incorporated in the auditor's documentation of the overall strategy and audit plan.[68] Similarly, for example, the results of the risk assessment may be documented separately, or may be documented as part of the auditor's documentation of further audit procedures.[69]

[67] ISA 230, paragraph 8
[68] ISA 300, *Planning an Audit of Financial Statements*, paragraphs 7, 9 and A11
[69] ISA 330, paragraph 28

Appendix 1

(Ref: Para. A61–A67)

Considerations for Understanding the Entity and its Business Model

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

Objectives and Scope of an Entity's Business Model

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

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

3. A description of a business model typically includes:

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

- How the entity's business model integrates the use of IT in its interactions with customers, suppliers, lenders and other stakeholders through IT interfaces and other technologies.

4. A business risk may have an immediate consequence for the risk of material misstatement for classes of transactions, account balances, and disclosures at the assertion level or the financial statement level. For example, the business risk arising from a significant fall in real estate market values may increase the risk of material misstatement associated with the valuation assertion for a lender of medium-term real estate backed loans. However, the same risk, particularly in combination with a severe economic downturn that concurrently increases the underlying risk of lifetime credit losses on its loans, may also have a longer-term consequence. The resulting net exposure to credit losses may cast significant doubt on the entity's ability to continue as a going concern. If so, this could have implications for management's, and the auditor's, conclusion as to the appropriateness of the entity's use of the going concern basis of accounting, and determination as to whether a material uncertainty exists. Whether a business risk may result in a risk of material misstatement is, therefore, considered in light of the entity's circumstances. Examples of events and conditions that may give rise to the existence of risks of material misstatement are indicated in **Appendix 2**.

Activities of the Entity

5. Examples of matters that the auditor may consider when obtaining an understanding of the activities of the entity (included in the entity's business model) include:

   (a) Business operations such as:

      - Nature of revenue sources, products or services, and markets, including involvement in electronic commerce such as Internet sales and marketing activities.
      - Conduct of operations (for example, stages and methods of production, or activities exposed to environmental risks).
      - Alliances, joint ventures, and outsourcing activities.
      - Geographic dispersion and industry segmentation.
      - Location of production facilities, warehouses, and offices, and location and quantities of inventories.
      - Key customers and important suppliers of goods and services, employment arrangements (including the existence of union contracts, pension and other post- employment benefits, stock option or incentive bonus arrangements, and government regulation related to employment matters).

- Research and development activities and expenditures.
- Transactions with related parties.

(b) Investments and investment activities such as:

- Planned or recently executed acquisitions or divestitures.
- Investments and dispositions of securities and loans.
- Capital investment activities.
- Investments in non-consolidated entities, including non-controlled partnerships, joint ventures and non-controlled special-purpose entities.

(c) Financing and financing activities such as:

- Ownership structure of major subsidiaries and associated entities, including consolidated and non-consolidated structures.
- Debt structure and related terms, including off-balance-sheet financing arrangements and leasing arrangements.
- Beneficial owners (for example, local, foreign, business reputation and experience) and related parties.
- Use of derivative financial instruments.

Nature of Special-Purpose Entities

6. A special-purpose entity (sometimes referred to as a special-purpose vehicle) is an entity that is generally established for a narrow and well-defined purpose, such as to effect a lease or a securitization of financial assets, or to carry out research and development activities. It may take the form of a corporation, trust, partnership or unincorporated entity. The entity on behalf of which the special-purpose entity has been created may often transfer assets to the latter (for example, as part of a derecognition transaction involving financial assets), obtain the right to use the latter's assets, or perform services for the latter, while other parties may provide the funding to the latter. As ISA 550 indicates, in some circumstances, a special-purpose entity may be a related party of the entity.[70]

7. Financial reporting frameworks often specify detailed conditions that are deemed to amount to control, or circumstances under which the special-purpose entity should be considered for consolidation. The interpretation of the requirements of such frameworks often demands a detailed knowledge of the relevant agreements involving the special-purpose entity.

[70] ISA 550, paragraph A7

Appendix 2

(Ref: Para. 12(f), 19(c), A7–A8, A85–A89)

Understanding Inherent Risk Factors

This appendix provides further explanation about the inherent risk factors, as well as matters that the auditor may consider in understanding and applying the inherent risk factors in identifying and assessing the risks of material misstatement at the assertion level.

The Inherent Risk Factors

1. Inherent risk factors are characteristics of events or conditions that affect susceptibility of an assertion about a class of transactions, account balance or disclosure, to misstatement, whether due to fraud or error, and before consideration of controls. Such factors may be qualitative or quantitative, and include complexity, subjectivity, change, uncertainty or susceptibility to misstatement due to management bias or other fraud risk factors[71] insofar as they affect inherent risk. In obtaining the understanding of the entity and its environment, and the applicable financial reporting framework and the entity's accounting policies, in accordance with paragraphs 19(a)–(b), the auditor also understands how inherent risk factors affect susceptibility of assertions to misstatement in the preparation of the financial statements.

2. Inherent risk factors relating to the preparation of information required by the applicable financial reporting framework (referred to in this paragraph as "required information") include:

    - *Complexity*—arises either from the nature of the information or in the way that the required information is prepared, including when such preparation processes are more inherently difficult to apply. For example, complexity may arise:

        - In calculating supplier rebate provisions because it may be necessary to take into account different commercial terms with many different suppliers, or many interrelated commercial terms that are all relevant in calculating the rebates due; or

        - When there are many potential data sources, with different characteristics used in making an accounting estimate, the processing of that data involves many interrelated steps, and the data is therefore inherently more difficult to identify, capture, access, understand or process.

    - *Subjectivity*—arises from inherent limitations in the ability to prepare required information in an objective manner, due to limitations in the

[71] ISA 240, paragraphs A24–A27

availability of knowledge or information, such that management may need to make an election or subjective judgment about the appropriate approach to take and about the resulting information to include in the financial statements. Because of different approaches to preparing the required information, different outcomes could result from appropriately applying the requirements of the applicable financial reporting framework. As limitations in knowledge or data increase, the subjectivity in the judgments that could be made by reasonably knowledgeable and independent individuals, and the diversity in possible outcomes of those judgments, will also increase.

- *Change*—results from events or conditions that, over time, affect the entity's business or the economic, accounting, regulatory, industry or other aspects of the environment in which it operates, when the effects of those events or conditions are reflected in the required information. Such events or conditions may occur during, or between, financial reporting periods. For example, change may result from developments in the requirements of the applicable financial reporting framework, or in the entity and its business model, or in the environment in which the entity operates. Such change may affect management's assumptions and judgments, including as they relate to management's selection of accounting policies or how accounting estimates are made or related disclosures are determined.

- *Uncertainty*—arises when the required information cannot be prepared based only on sufficiently precise and comprehensive data that is verifiable through direct observation. In these circumstances, an approach may need to be taken that applies the available knowledge to prepare the information using sufficiently precise and comprehensive observable data, to the extent available, and reasonable assumptions supported by the most appropriate available data, when it is not. Constraints on the availability of knowledge or data, which are not within the control of management (subject to cost constraints where applicable) are sources of uncertainty and their effect on the preparation of the required information cannot be eliminated. For example, estimation uncertainty arises when the required monetary amount cannot be determined with precision and the outcome of the estimate is not known before the date the financial statements are finalized.

- *Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk*—susceptibility to management bias results from conditions that create susceptibility to intentional or unintentional failure by management to maintain neutrality in preparing the information. Management bias is often associated with certain conditions that have the potential to give rise to management not maintaining neutrality in exercising judgment (indicators of potential

management bias), which could lead to a material misstatement of the information that would be fraudulent if intentional. Such indicators include incentives or pressures insofar as they affect inherent risk (for example, as a result of motivation to achieve a desired result, such as a desired profit target or capital ratio), and opportunity, not to maintain neutrality. Factors relevant to the susceptibility to misstatement due to fraud in the form of fraudulent financial reporting or misappropriation of assets are described in paragraphs A1 to A5 of ISA 240.

3. When complexity is an inherent risk factor, there may be an inherent need for more complex processes in preparing the information, and such processes may be inherently more difficult to apply. As a result, applying them may require specialized skills or knowledge, and may require the use of a management's expert.

4. When management judgment is more subjective, the susceptibility to misstatement due to management bias, whether unintentional or intentional, may also increase. For example, significant management judgment may be involved in making accounting estimates that have been identified as having high estimation uncertainty, and conclusions regarding methods, data and assumptions may reflect unintentional or intentional management bias.

Examples of Events or Conditions that May Give Rise to the Existence of Risks of Material Misstatement

5. The following are examples of events (including transactions) and conditions that may indicate the existence of risks of material misstatement in the financial statements, at the financial statement level or the assertion level. The examples provided by inherent risk factor cover a broad range of events and conditions; however, not all events and conditions are relevant to every audit engagement and the list of examples is not necessarily complete. The events and conditions have been categorized by the inherent risk factor that may have the greatest effect in the circumstances. Importantly, due to the interrelationships among inherent risk factors, the example events and conditions also are likely to be subject to, or affected by, other inherent risk factors to varying degrees.

Relevant Inherent Risk Factor:	Examples of Events or Conditions That May Indicate the Existence of Risks of Material Misstatement at the Assertion Level:
Complexity	Regulatory: ● Operations that are subject to a high degree of complex regulation. Business model: ● The existence of complex alliances and joint ventures. Applicable financial reporting framework: ● Accounting measurements that involve complex processes. Transactions: ● Use of off-balance sheet finance, special-purpose entities, and other complex financing arrangements.
Subjectivity	Applicable financial reporting framework: ● A wide range of possible measurement criteria of an accounting estimate. For example, management's recognition of depreciation or construction income and expenses. ● Management's selection of a valuation technique or model for a non-current asset, such as investment properties.
Change	Economic conditions: ● Operations in regions that are economically unstable, for example, countries with significant currency devaluation or highly inflationary economies. Markets: ● Operations exposed to volatile markets, for example, futures trading. Customer loss: ● Going concern and liquidity issues including loss of significant customers. Industry model: ● Changes in the industry in which the entity operates. Business model: ● Changes in the supply chain. ● Developing or offering new products or services, or moving into new lines of business.

Relevant Inherent Risk Factor:	Examples of Events or Conditions That May Indicate the Existence of Risks of Material Misstatement at the Assertion Level:
	Geography: ● Expanding into new locations. Entity structure: ● Changes in the entity such as large acquisitions or reorganizations or other unusual events. ● Entities or business segments likely to be sold. Human resources competence: ● Changes in key personnel including departure of key executives. IT: ● Changes in the IT environment. ● Installation of significant new IT systems related to financial reporting. Applicable financial reporting framework: ● Application of new accounting pronouncements. Capital: ● New constraints on the availability of capital and credit. Regulatory: ● Inception of investigations into the entity's operations or financial results by regulatory or government bodies. • Impact of new legislation related to environmental protection.
Uncertainty	Reporting: ● Events or transactions that involve significant measurement uncertainty, including accounting estimates, and related disclosures. ● Pending litigation and contingent liabilities, for example, sales warranties, financial guarantees and environmental remediation.

Relevant Inherent Risk Factor:	Examples of Events or Conditions That May Indicate the Existence of Risks of Material Misstatement at the Assertion Level:
Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk	Reporting: ● Opportunities for management and employees to engage in fraudulent financial reporting, including omission, or obscuring, of significant information in disclosures. Transactions: ● Significant transactions with related parties. ● Significant amount of non-routine or non-systematic transactions including intercompany transactions and large revenue transactions at period end. ● Transactions that are recorded based on management's intent, for example, debt refinancing, assets to be sold and classification of marketable securities.

Other events or conditions that may indicate risks of material misstatement at the financial statement level:

- Lack of personnel with appropriate accounting and financial reporting skills.
- Control deficiencies – particularly in the control environment, risk assessment process and process for monitoring, and especially those not addressed by management.
- Past misstatements, history of errors or a significant amount of adjustments at period end.

Appendix 3

(Ref: Para. 12(m), 21–26, A90–A181)

Understanding the Entity's System of Internal Control

1. The entity's system of internal control may be reflected in policy and procedures manuals, systems and forms, and the information embedded therein, and is effected by people. The entity's system of internal control is implemented by management, those charged with governance, and other personnel based on the structure of the entity. The entity's system of internal control can be applied, based on the decisions of management, those charged with governance or other personnel and in the context of legal or regulatory requirements, to the operating model of the entity, the legal entity structure, or a combination of these.

2. This appendix further explains the components of, as well as the limitations of, the entity's system of internal control as set out in paragraphs 12(m), 21–26, and A90–A181, as they relate to a financial statement audit.

3. Included within the entity's system of internal control are aspects that relate to the entity's reporting objectives, including its financial reporting objectives, but it may also include aspects that relate to its operations or compliance objectives, when such aspects are relevant to financial reporting.

> **Example**:
>
> Controls over compliance with laws and regulations may be relevant to financial reporting when such controls are relevant to the entity's preparation of disclosures of contingencies in the financial statements.

Components of the Entity's System of Internal Control

Control Environment

4. The control environment includes the governance and management functions and the attitudes, awareness, and actions of those charged with governance and management concerning the entity's system of internal control, and its importance in the entity. The control environment sets the tone of an organization, influencing the control consciousness of its people, and provides the overall foundation for the operation of the other components of the entity's system of internal control.

5. An entity's control consciousness is influenced by those charged with governance, because one of their roles is to counterbalance pressures on management in relation to financial reporting that may arise from market demands or remuneration schemes. The effectiveness of the design of the control environment in relation to participation by those charged with governance is therefore influenced by such matters as:

- Their independence from management and their ability to evaluate the actions of management.
- Whether they understand the entity's business transactions.
- The extent to which they evaluate whether the financial statements are prepared in accordance with the applicable financial reporting framework, including whether the financial statements include adequate disclosures.

6. The control environment encompasses the following elements:

(a) *How management's responsibilities are carried out, such as creating and maintaining the entity's culture and demonstrating management's commitment to integrity and ethical values*. The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical behavior are the product of the entity's ethical and behavioral standards or codes of conduct, how they are communicated (e.g., through policy statements), and how they are reinforced in practice (e.g., through management actions to eliminate or mitigate incentives or temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts). The communication of entity policies on integrity and ethical values may include the communication of behavioral standards to personnel through policy statements and codes of conduct and by example.

(b) *When those charged with governance are separate from management, how those charged with governance demonstrate independence from management and exercise oversight of the entity's system of internal control*. An entity's control consciousness is influenced by those charged with governance. Considerations may include whether there are sufficient individuals who are independent from management and objective in their evaluations and decision-making; how those charged with governance identify and accept oversight responsibilities and whether those charged with governance retain oversight responsibility for management's design, implementation and conduct of the entity's system of internal control. The importance of the responsibilities of those charged with governance is recognized in codes of practice and other laws and regulations or guidance produced for the benefit of those charged with governance. Other responsibilities of those charged with governance include oversight of the design and effective operation of whistle blower procedures.

(c) *How the entity assigns authority and responsibility in pursuit of its objectives.* This may include considerations about:

- Key areas of authority and responsibility and appropriate lines of reporting;

- Policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties; and
- Policies and communications directed at ensuring that all personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

(d) *How the entity attracts, develops, and retains competent individuals in alignment with its objectives.* This includes how the entity ensures the individuals have the knowledge and skills necessary to accomplish the tasks that define the individual's job, such as:

- Standards for recruiting the most qualified individuals – with an emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior.
- Training policies that communicate prospective roles and responsibilities, including practices such as training schools and seminars that illustrate expected levels of performance and behavior; and
- Periodic performance appraisals driving promotions that demonstrate the entity's commitment to the advancement of qualified personnel to higher levels of responsibility.

(e) *How the entity holds individuals accountable for their responsibilities in pursuit of the objectives of the entity's system of internal control.* This may be accomplished through, for example:

- Mechanisms to communicate and hold individuals accountable for performance of controls responsibilities and implement corrective actions as necessary;
- Establishing performance measures, incentives and rewards for those responsible for the entity's system of internal control, including how the measures are evaluated and maintain their relevance;
- How pressures associated with the achievement of control objectives impact the individual's responsibilities and performance measures; and
- How the individuals are disciplined as necessary.

The appropriateness of the above matters will be different for every entity depending on its size, the complexity of its structure and the nature of its activities.

The Entity's Risk Assessment Process

7. The entity's risk assessment process is an iterative process for identifying and analyzing risks to achieving the entity's objectives, and forms the basis for how management or those charged with governance determine the risks to be managed.

8. For financial reporting purposes, the entity's risk assessment process includes how management identifies business risks relevant to the preparation of financial statements in accordance with the entity's applicable financial reporting framework, estimates their significance, assesses the likelihood of their occurrence, and decides upon actions to manage them and the results thereof. For example, the entity's risk assessment process may address how the entity considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements.

9. Risks relevant to reliable financial reporting include external and internal events, transactions or circumstances that may occur and adversely affect an entity's ability to initiate, record, process, and report financial information consistent with the assertions of management in the financial statements. Management may initiate plans, programs, or actions to address specific risks or it may decide to assume a risk because of cost or other considerations. Risks can arise or change due to circumstances such as the following:

    - *Changes in operating environment*. Changes in the regulatory, economic or operating environment can result in changes in competitive pressures and significantly different risks.
    - *New personnel*. New personnel may have a different focus on or understanding of the entity's system of internal control.
    - *New or revamped information system*. Significant and rapid changes in the information system can change the risk relating to the entity's system of internal control.
    - *Rapid growth*. Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls.
    - *New technology*. Incorporating new technologies into production processes or the information system may change the risk associated with the entity's system of internal control.
    - *New business models, products, or activities*. Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with the entity's system of internal control.
    - *Corporate restructurings*. Restructurings may be accompanied by staff reductions and changes in supervision and segregation of duties that may change the risk associated with the entity's system of internal control.

- *Expanded foreign operations*. The expansion or acquisition of foreign operations carries new and often unique risks that may affect internal control, for example, additional or changed risks from foreign currency transactions.
- *New accounting pronouncements*. Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.
- *Use of IT*. Risks relating to:
    - Maintaining the integrity of data and information processing;
    - Risks to the entity's business strategy that arise if the entity's IT strategy does not effectively support the entity's business strategy; or
    - Changes or interruptions in the entity's IT environment or turnover of IT personnel or when the entity does not make necessary updates to the IT environment or such updates are not timely.

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

10. The entity's process to monitor the system of internal control is a continual process to evaluate the effectiveness of the entity's system of internal control, and to take necessary remedial actions on a timely basis. The entity's process to monitor the entity's system of internal control may consist of ongoing activities, separate evaluations (conducted periodically), or some combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of an entity and may include regular management and supervisory activities. The entity's process will likely vary in scope and frequency depending on the assessment of the risks by the entity.

11. The objectives and scope of internal audit functions typically include activities designed to evaluate or monitor the effectiveness of the entity's system of internal control.[72] The entity's process to monitor the entity's system of internal control may include activities such as management's review of whether bank reconciliations are being prepared on a timely basis, internal auditors' evaluation of sales personnel's compliance with the entity's policies on terms of sales contracts, and a legal department's oversight of compliance with the entity's ethical or business practice policies. Monitoring is done also to ensure that controls continue to operate effectively over time. For example, if the timeliness and accuracy of bank reconciliations are not monitored, personnel are likely to stop preparing them.

12. Controls related to the entity's process to monitor the entity's system of internal control, including those that monitor underlying automated controls, may be

[72] ISA 610 (Revised 2013) and Appendix 4 of this ISA provide further guidance related to internal audit.

automated or manual, or a combination of both. For example, an entity may use automated monitoring controls over access to certain technology with automated reports of unusual activity to management, who manually investigate identified anomalies.

13. When distinguishing between a monitoring activity and a control related to the information system, the underlying details of the activity are considered, especially when the activity involves some level of supervisory review. Supervisory reviews are not automatically classified as monitoring activities and it may be a matter of judgment whether a review is classified as a control related to the information system or a monitoring activity. For example, the intent of a monthly completeness control would be to detect and correct errors, where a monitoring activity would ask why errors are occurring and assign management the responsibility of fixing the process to prevent future errors. In simple terms, a control related to the information system responds to a specific risk, whereas a monitoring activity assesses whether controls within each of the five components of the entity's system of internal control are operating as intended.

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

The Information System and Communication

15. The information system relevant to the preparation of the financial statements consists of activities and policies, and accounting and supporting records, designed and established to:

- 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 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.

16. An entity's business processes include the activities designed to:

- Develop, purchase, produce, sell and distribute an entity's products and services;
- Ensure compliance with laws and regulations; and
- Record information, including accounting and financial reporting information.

Business processes result in the transactions that are recorded, processed and reported by the information system.

17. The quality of information affects management's ability to make appropriate decisions in managing and controlling the entity's activities and to prepare reliable financial reports.

18. Communication, which involves providing an understanding of individual roles and responsibilities pertaining to the entity's system of internal control, may take such forms as policy manuals, accounting and financial reporting manuals, and memoranda. Communication also can be made electronically, orally, and through the actions of management.

19. Communication by the entity of the financial reporting roles and responsibilities and of significant matters relating to financial reporting involves providing an understanding of individual roles and responsibilities pertaining to the entity's system of internal control relevant to financial reporting. It may include such matters as the extent to which personnel understand how their activities in the information system relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity.

Control Activities

20. Controls in the control activities component are identified in accordance with paragraph 26. Such controls include information processing controls and general IT controls, both of which may be manual or automated in nature. The greater the extent of automated controls, or controls involving automated aspects, that management uses and relies on in relation to its financial reporting, the more important it may become for the entity to implement general IT controls that address the continued functioning of the automated aspects of information processing controls. Controls in the control activities component may pertain 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 policy). An authorization typically takes the form of an approval by a higher level of management or of verification and a determination if the transaction is valid. For example, a supervisor approves an expense report after reviewing whether the expenses seem reasonable and within policy. An example of an automated approval is when an invoice unit cost is automatically compared with the related purchase order unit cost within a pre-established tolerance level. Invoices within the tolerance level are automatically approved for payment. Those invoices outside the tolerance level are flagged for additional investigation.
- *Reconciliations* – Reconciliations compare two or more data elements. If differences are identified, action is taken to bring the data into agreement. Reconciliations generally address the completeness or accuracy of processing transactions.
- *Verifications* – Verifications compare two or more items with each other or compare an item with a policy, and will likely involve a follow-up action when the two items do not match or the item is not consistent with policy. Verifications generally address the completeness, accuracy, or validity of processing transactions.
- *Physical or logical controls, including those that address security of assets against unauthorized access, acquisition, use or disposal.* Controls that encompass:
    - The physical security of assets, including adequate safeguards such as secured facilities over access to assets and records.
    - The authorization for access to computer programs and data files (i.e., logical access).
    - The periodic counting and comparison with amounts shown on control records (for example, comparing the results of cash, security and inventory counts with accounting records).

  The extent to which physical controls intended to prevent theft of assets are relevant to the reliability of financial statement preparation depends on circumstances such as when assets are highly susceptible to misappropriation.
- *Segregation of duties.* Assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets. Segregation of duties is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud in the normal course of the person's duties.

  For example, a manager authorizing credit sales is not responsible for maintaining accounts receivable records or handling cash receipts. If

one person is able to perform all these activities the person 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.

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

Limitations of Internal Control

22. The entity's system of internal control, no matter how effective, can provide an entity with only reasonable assurance about achieving the entity's financial reporting objectives. The likelihood of their achievement is affected by the inherent limitations of internal control. These include the realities that human judgment in decision-making can be faulty and that breakdowns in the entity's system of internal control can occur because of human error. For example, there may be an error in the design of, or in the change to, a control. Equally, the operation of a control may not be effective, such as where information produced for the purposes of the entity's system of internal control (for example, an exception report) is not effectively used because the individual responsible for reviewing the information does not understand its purpose or fails to take appropriate action.

23. Additionally, controls can be circumvented by the collusion of two or more people or inappropriate management override of controls. For example, management may enter into side agreements with customers that alter the terms and conditions of the entity's standard sales contracts, which may result in improper revenue recognition. Also, edit checks in an IT application that are designed to identify and report transactions that exceed specified credit limits may be overridden or disabled.

24. Further, in designing and implementing controls, management may make judgments on the nature and extent of the controls it chooses to implement, and the nature and extent of the risks it chooses to assume.

Appendix 4

(Ref: Para 14(a), 24(a)(ii), A25–A28, A118)

Considerations for Understanding an Entity's Internal Audit Function

This appendix provides further considerations relating to understanding the entity's internal audit function when such a function exists.

Objectives and Scope of the Internal Audit Function

1. The objectives and scope of an internal audit function, the nature of its responsibilities and its status within the organization, including the function's authority and accountability, vary widely and depend on the size, complexity and structure of the entity and the requirements of management and, where applicable, those charged with governance. These matters may be set out in an internal audit charter or terms of reference.

2. The responsibilities of an internal audit function may include performing procedures and evaluating the results to provide assurance to management and those charged with governance regarding the design and effectiveness of risk management, the entity's system of internal control and governance processes. If so, the internal audit function may play an important role in the entity's process to monitor the entity's system of internal control. However, the responsibilities of the internal audit function may be focused on evaluating the economy, efficiency and effectiveness of operations and, if so, the work of the function may not directly relate to the entity's financial reporting.

Inquiries of the Internal Audit Function

3. If an entity has an internal audit function, inquiries of the appropriate individuals within the function may provide information that is useful to the auditor in obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control, and in identifying and assessing risks of material misstatement at the financial statement and assertion levels. In performing its work, the internal audit function is likely to have obtained insight into the entity's operations and business risks, and may have findings based on its work, such as identified control deficiencies or risks, that may provide valuable input into the auditor's understanding of the entity and its environment, the applicable financial reporting framework, the entity's system of internal control, the auditor's risk assessments or other aspects of the audit. The auditor's inquiries are therefore made whether or not 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.[73] Inquiries of particular relevance may be about matters the internal audit function has raised

[73] The relevant requirements are contained in ISA 610 (Revised 2013).

with those charged with governance and the outcomes of the function's own risk assessment process.

4. If, based on responses to the auditor's inquiries, it appears that there are findings that may be relevant to the entity's financial reporting and the audit of the financial statements, the auditor may consider it appropriate to read related reports of the internal audit function. Examples of reports of the internal audit function that may be relevant include the function's strategy and planning documents and reports that have been prepared for management or those charged with governance describing the findings of the internal audit function's examinations.

5. In addition, in accordance with ISA 240,[74] if the internal audit function provides information to the auditor regarding any actual, suspected or alleged fraud, the auditor takes this into account in the auditor's identification of risk of material misstatement due to fraud.

6. Appropriate individuals within the internal audit function with whom inquiries are made are those who, in the auditor's judgment, have the appropriate knowledge, experience and authority, such as the chief internal audit executive or, depending on the circumstances, other personnel within the function. The auditor may also consider it appropriate to have periodic meetings with these individuals.

Consideration of the Internal Audit Function in Understanding the Control Environment

7. In understanding the control environment, the auditor may consider how management has responded to the findings and recommendations of the internal audit function regarding identified control deficiencies relevant to the preparation of the financial statements, including whether and how such responses have been implemented, and whether they have been subsequently evaluated by the internal audit function.

Understanding the Role that the Internal Audit Function Plays in the Entity's Process to Monitor the System of Internal Control

8. If the nature of the internal audit function's responsibilities and assurance activities are related to the entity's financial reporting, the auditor may also be able to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed directly by the auditor in obtaining audit evidence. Auditors may be more likely to be able to use the work of an entity's internal audit function when it appears, for example, based on experience in previous audits or the auditor's risk assessment procedures, that the entity has an internal audit function that is adequately and appropriately

[74] ISA 240, paragraph 19

resourced relative to the complexity of the entity and the nature of its operations, and has a direct reporting relationship to those charged with governance.

9. If, based on the auditor's preliminary understanding of the internal audit function, the auditor expects to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed, ISA 610 (Revised 2013) applies.

10. As is further discussed in ISA 610 (Revised 2013), the activities of an internal audit function are distinct from other monitoring controls that may be relevant to financial reporting, such as reviews of management accounting information that are designed to contribute to how the entity prevents or detects misstatements.

11. Establishing communications with the appropriate individuals within an entity's internal audit function early in the engagement, and maintaining such communications throughout the engagement, can facilitate effective sharing of information. It creates an environment in which the auditor can be informed of significant matters that may come to the attention of the internal audit function when such matters may affect the work of the auditor. ISA 200 discusses the importance of the auditor planning and performing the audit with professional skepticism,[75] including being alert to information that brings into question the reliability of documents and responses to inquiries to be used as audit evidence. Accordingly, communication with the internal audit function throughout the engagement may provide opportunities for internal auditors to bring such information to the auditor's attention. The auditor is then able to take such information into account in the auditor's identification and assessment of risks of material misstatement.

[75] ISA 200, paragraph 7

Appendix 5

(Ref: Para. 25(a), 26(b)–(c), A94, A166–A172)

Considerations for Understanding Information Technology (IT)

This appendix provides further matters that the auditor may consider in understanding the entity's use of IT in its system of internal control.

Understanding the Entity's Use of Information Technology in the Components of the Entity's System of Internal Control

1. An entity's system of internal control contains manual elements and automated elements (i.e., manual and automated controls and other resources used in the entity's system of internal control). An entity's mix of manual and automated elements varies with the nature and complexity of the entity's use of IT. An entity's use of IT affects the manner in which the information relevant to the preparation of the financial statements in accordance with the applicable financial reporting framework is processed, stored and communicated, and therefore affects the manner in which the entity's system of internal control is designed and implemented. Each component of the entity's system of internal control may use some extent of IT.

   Generally, IT benefits an entity's system of internal control by enabling an entity to:

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

2. The characteristics of manual or automated elements are relevant to the auditor's identification and assessment of the risks of material misstatement, and further audit procedures based thereon. Automated controls may be more reliable than manual controls because they cannot be as easily bypassed, ignored, or overridden, and they are also less prone to simple errors and mistakes. Automated controls may be more effective than manual controls in the following circumstances:

   - High volume of recurring transactions, or in situations where errors that can be anticipated or predicted can be prevented, or detected and corrected, through automation.

- Controls where the specific ways to perform the control can be adequately designed and automated.

Understanding the Entity's Use of Information Technology in the Information System (Ref: Para. 25(a))

3. The entity's information system may include the use of manual and automated elements, which also affect the manner in which transactions are initiated, recorded, processed, and reported. In particular, procedures to initiate, record, process and report transactions may be enforced through the IT applications used by the entity, and how the entity has configured those applications. In addition, records in the form of digital information may replace or supplement records in the form of paper documents.

4. In obtaining an understanding of the IT environment relevant to the flows of transactions and information processing in the information system, the auditor gathers information about the nature and characteristics of the IT applications used, as well as the supporting IT infrastructure and IT. The following table includes examples of matters that the auditor may consider in obtaining the understanding of the IT environment and includes examples of typical characteristics of IT environments based on the complexity of IT applications used in the entity's information system. However, such characteristics are directional and may differ depending on the nature of the specific IT applications in use by an entity.

	Examples of typical characteristics of:		
	Non-complex commercial software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems)
Matters related to extent of automation and use of data:			
• The extent of automated procedures for processing, and the complexity of those procedures, including, whether there is highly automated, paperless processing.	N/A	N/A	Extensive and often complex automated procedures

	Examples of typical characteristics of:		
	Non-complex commercial software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems)
● The extent of the entity's reliance on system-generated reports in the processing of information.	Simple automated report logic	Simple relevant automated report logic	Complex automated report logic; Report-writer software
● How data is input (i.e., manual input, customer or vendor input, or file load).	Manual data inputs	Small number of data inputs or simple interfaces	Large number of data inputs or complex interfaces
● How IT facilitates communication between applications, databases or other aspects of the IT environment, internally and externally, as appropriate, through system interfaces.	No automated interfaces (manual inputs only)	Small number of data inputs or simple interfaces	Large number of data inputs or complex interfaces
● The volume and complexity of data in digital form being processed by the information system, including whether accounting records or other information are stored in digital form and the location of stored data.	Low volume of data or simple data that is able to be verified manually; Data available locally	Low volume of data or simple data	Large volume of data or complex data; Data warehouses;[76] Use of internal or external IT service providers (e.g., third-party storage or hosting of data)

[76] A data warehouse is generally described as a central repository of integrated data from one or more disparate sources (such as multiple databases) from which reports may be generated or that may be used by the entity for other data analysis activities. A report-writer is an IT application that is used to extract data from one or more sources (such as a data warehouse, a database or an IT application) and present the data in a specified format.

	Examples of typical characteristics of:		
	Non-complex commercial software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems)
Matters related to the IT applications and IT infrastructure:			
● The type of application (e.g., a commercial application with little or no customization, or a highly-customized or highly-integrated application that may have been purchased and customized, or developed in-house).	Purchased application with little or no customization	Purchased application or simple legacy or low-end ERP applications with little or no customization	Custom developed applications or more complex ERPs with significant customization
● The complexity of the nature of the IT applications and the underlying IT infrastructure.	Small, simple laptop or client server-based solution	Mature and stable mainframe, small or simple client server, software as a service cloud	Complex mainframe, large or complex client server, web-facing, infrastructure as a service cloud
● Whether there is third-party hosting or outsourcing of IT.	If outsourced, competent, mature, proven provider (e.g., cloud provider)	If outsourced, competent, mature, proven provider (e.g., cloud provider)	Competent, mature proven provider for certain applications and new or start-up provider for others
● Whether the entity is using emerging technologies that affect its financial reporting.	No use of emerging technologies	Limited use of emerging technologies in some applications	Mixed use of emerging technologies across platforms

	Examples of typical characteristics of:		
	Non-complex commercial software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems)
Matters related to IT processes:			
● The personnel involved in maintaining the IT environment (the number and skill level of the IT support resources that manage security and changes to the IT environment).	Few personnel with limited IT knowledge to process vendor upgrades and manage access	Limited personnel with IT skills / dedicated to IT	Dedicated IT departments with skilled personnel, including programming skills
● The complexity of processes to manage access rights.	Single individual with administrative access manages access rights	Few individuals with administrative access manage access rights	Complex processes managed by IT department for access rights
● The complexity of the security over the IT environment, including vulnerability of the IT applications, databases, and other aspects of the IT environment to cyber risks, particularly when there are web-based transactions or transactions involving external interfaces.	Simple on-premise access with no external web-facing elements	Some web-based applications with primarily simple, role-based security	Multiple platforms with web-based access and complex security models

	Examples of typical characteristics of:		
	Non-complex commercial software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems)
• Whether program changes have been made to the manner in which information is processed, and the extent of such changes during the period.	Commercial software with no source code installed	Some commercial applications with no source code and other mature applications with a small number or simple changes; traditional systems development lifecycle	New or large number or complex changes, several development cycles each year
• The extent of change within the IT environment (e.g., new aspects of the IT environment or significant changes in the IT applications or the underlying IT infrastructure).	Changes limited to version upgrades of commercial software	Changes consist of commercial software upgrades, ERP version upgrades, or legacy enhancements	New or large number or complex changes, several development cycles each year, heavy ERP customization
• Whether there was a major data conversion during the period and, if so, the nature and significance of the changes made, and how the conversion was undertaken.	Software upgrades provided by vendor; No data conversion features for upgrade	Minor version upgrades for commercial software applications with limited data being converted	Major version upgrade, new release, platform change

Emerging Technologies

5. Entities may use emerging technologies (e.g., blockchain, robotics or artificial intelligence) because such technologies may present specific opportunities to increase operational efficiencies or enhance financial reporting. When emerging technologies are used in the entity's information system relevant to the preparation of the financial statements, the auditor may include such technologies in the identification of IT applications and other aspects of the IT environment that are subject to risks arising from the use of IT. While emerging technologies may be seen to be more sophisticated or more complex

compared to existing technologies, the auditor's responsibilities in relation to IT applications and identified general IT controls in accordance with paragraph 26(b)–(c) remain unchanged.

Scalability

6. Obtaining an understanding of the entity's IT environment may be more easily accomplished for a less complex entity that uses commercial software and when the entity does not have access to the source code to make any program changes. Such entities may not have dedicated IT resources but may have a person assigned in an administrator role for the purpose of granting employee access or installing vendor-provided updates to the IT applications. Specific matters that the auditor may consider in understanding the nature of a commercial accounting software package, which may be the single IT application used by a less complex entity in its information system, may include:

   - The extent to which the software is well established and has a reputation for reliability;
   - The extent to which it is possible for the entity to modify the source code of the software to include additional modules (i.e., add-ons) to the base software, or to make direct changes to data;
   - The nature and extent of modifications that have been made to the software. Although an entity may not be able to modify the source code of the software, many software packages allow for configuration (e.g., setting or amending reporting parameters). These do not usually involve modifications to source code; however, the auditor may consider the extent to which the entity is able to configure the software when considering the completeness and accuracy of information produced by the software that is used as audit evidence; and
   - The extent to which data related to the preparation of the financial statements can be directly accessed (i.e., direct access to the database without using the IT application) and the volume of data that is processed. The greater the volume of data, the more likely the entity may need controls that address maintaining the integrity of the data, which may include general IT controls over unauthorized access and changes to the data.

7. Complex IT environments may include highly-customized or highly-integrated IT applications and may therefore require more effort to understand. Financial reporting processes or IT applications may be integrated with other IT applications. Such integration may involve IT applications that are used in the entity's business operations and that provide information to the IT applications relevant to the flows of transactions and information processing in the entity's information system. In such circumstances, certain IT applications used in the entity's business operations may also be relevant to the preparation of the

financial statements. Complex IT environments also may require dedicated IT departments that have structured IT processes supported by personnel that have software development and IT environment maintenance skills. In other cases, an entity may use internal or external service providers to manage certain aspects of, or IT processes within, its IT environment (e.g., third-party hosting).

Identifying IT Applications that are Subject to Risks Arising from the use of IT

8. Through understanding the nature and complexity of the entity's IT environment, including the nature and extent of information processing controls, the auditor may determine which IT applications the entity is relying upon to accurately process and maintain the integrity of financial information. The identification of IT applications on which the entity relies may affect the auditor's decision to test the automated controls within such IT applications, assuming that such automated controls address identified risks of material misstatement. Conversely, if the entity is not relying on an IT application, the automated controls within such IT application are unlikely to be appropriate or sufficiently precise for purposes of operating effectiveness tests. Automated controls that may be identified in accordance with paragraph 26(b) may include, for example, automated calculations or input, processing and output controls, such as a three-way match of a purchase order, vendor shipping document, and vendor invoice. When automated controls are identified by the auditor and the auditor determines through the understanding of the IT environment that the entity is relying on the IT application that includes those automated controls, it may be more likely for the auditor to identify the IT application as one that is subject to risks arising from the use of IT.

9. In considering whether the IT applications for which the auditor has identified automated controls are subject to risks arising from the use of IT, the auditor is likely to consider whether, and the extent to which, the entity may have access to source code that enables management to make program changes to such controls or the IT applications. The extent to which the entity makes program or configuration changes and the extent to which the IT processes over such changes are formalized may also be relevant considerations. The auditor is also likely to consider the risk of inappropriate access or changes to data.

10. System-generated reports that the auditor may intend to use as audit evidence may include, for example, a trade receivable aging report or an inventory valuation report. For such reports, the auditor may obtain audit evidence about the completeness and accuracy of the reports by substantively testing the inputs and outputs of the report. In other cases, the auditor may plan to test the operating effectiveness of the controls over the preparation and maintenance of the report, in which case the IT application from which it is produced is likely to be subject to risks arising from the use of IT. In addition to testing the completeness and accuracy of the report, the auditor may plan to test the operating effectiveness of general IT controls that address risks related to inappropriate or unauthorized program changes to, or data changes in, the report.

11. Some IT applications may include report-writing functionality within them while some entities may also utilize separate report-writing applications (i.e., report-writers). In such cases, the auditor may need to determine the sources of system-generated reports (i.e., the application that prepares the report and the data sources used by the report) to determine the IT applications subject to risks arising from the use of IT.

12. The data sources used by IT applications may be databases that, for example, can only be accessed through the IT application or by IT personnel with database administration privileges. In other cases, the data source may be a data warehouse that may itself be considered to be an IT application subject to risks arising from the use of IT.

13. The auditor may have identified a risk for which substantive procedures alone are not sufficient because of the entity's use of highly-automated and paperless processing of transactions, which may involve multiple integrated IT applications. In such circumstances, the controls identified by the auditor are likely to include automated controls. Further, the entity may be relying on general IT controls to maintain the integrity of the transactions processed and other information used in processing. In such cases, the IT applications involved in the processing and the storage of the information are likely subject to risks arising from the use of IT.

End-User Computing

14. Although audit evidence may also come in the form of system-generated output that is used in a calculation performed in an end-user computing tool (e.g., spreadsheet software or simple databases), such tools are not typically identified as IT applications in the context of paragraph 26(b). Designing and implementing controls around access and change to end-user computing tools may be challenging, and such controls are rarely equivalent to, or as effective as, general IT controls. Rather, the auditor may consider a combination of information processing controls, taking into account the purpose and complexity of the end-user computing involved, such as:

    - Information processing controls over the initiation and processing of the source data, including relevant automated or interface controls to the point from which the data is extracted (i.e., the data warehouse);
    - Controls to check that the logic is functioning as intended, for example, controls which 'prove' the extraction of data, such as reconciling the report to the data from which it was derived, comparing the individual data from the report to the source and vice versa, and controls which check the formulas or macros; or
    - Use of validation software tools, which systematically check formulas or macros, such as spreadsheet integrity tools.

Scalability

15. The entity's ability to maintain the integrity of information stored and processed in the information system may vary based on the complexity and volume of the related transactions and other information. The greater the complexity and volume of data that supports a significant class of transactions, account balance or disclosure, the less likely it may become for the entity to maintain integrity of that information through information processing controls alone (e.g., input and output controls or review controls). It also becomes less likely that the auditor will be able to obtain audit evidence about the completeness and accuracy of such information through substantive testing alone when such information is used as audit evidence. In some circumstances, when volume and complexity of transactions are lower, management may have an information processing control that is sufficient to verify the accuracy and completeness of the data (e.g., individual sales orders processed and billed may be reconciled to the hard copy originally entered into the IT application). When the entity relies on general IT controls to maintain the integrity of certain information used by IT applications, the auditor may determine that the IT applications that maintain that information are subject to risks arising from the use of IT.

Example characteristics of an IT application that is likely not subject to risks arising from IT	Example characteristics of an IT application that is likely subject to risks arising from IT
● Standalone applications. ● The volume of data (transactions) is not significant. ● The application's functionality is not complex. ● Each transaction is supported by original hard copy documentation.	● Applications are interfaced. ● The volume of data (transactions) is significant. ● The application's functionality is complex as: ○ The application automatically initiates transactions; and ○ There are a variety of complex calculations underlying automated entries.
IT application is likely not subject to risks arising from IT because: ● The volume of data is not significant and therefore management is not relying upon general IT controls to process or maintain the data.	IT application is likely subject to risks arising from IT because: ● Management relies on an application system to process or maintain data as the volume of data is significant.

• Management does not rely on automated controls or other automated functionality. The auditor has not identified automated controls in accordance with paragraph 26(a). • Although management uses system-generated reports in their controls, it does not rely on these reports. Instead, it reconciles the reports back to the hard copy documentation and verifies the calculations in the reports. • The auditor will directly test information produced by the entity used as audit evidence.	• Management relies upon the application system to perform certain automated controls that the auditor has also identified.

Other Aspects of the IT Environment that Are Subject to Risks Arising from the Use of IT

16. When the auditor identifies IT applications that are subject to risks arising from the use of IT, other aspects of the IT environment are also typically subject to risks arising from the use of IT. The IT infrastructure includes the databases, operating system, and network. Databases store the data used by IT applications and may consist of many interrelated data tables. Data in databases may also be accessed directly through database management systems by IT or other personnel with database administration privileges. The operating system is responsible for managing communications between hardware, IT applications, and other software used in the network. As such, IT applications and databases may be directly accessed through the operating system. A network is used in the IT infrastructure to transmit data and to share information, resources and services through a common communications link. The network also typically establishes a layer of logical security (enabled through the operating system) for access to the underlying resources.

17. When IT applications are identified by the auditor to be subject to risks arising from IT, the database(s) that stores the data processed by an identified IT application is typically also identified. Similarly, because an IT application's ability to operate is often dependent on the operating system and IT applications and databases may be directly accessed from the operating system, the operating system is typically subject to risks arising from the use of IT. The network may be identified when it is a central point of access to the identified IT applications and related databases or when an IT application interacts with vendors or external parties through the internet, or when web-facing IT applications are identified by the auditor.

Identifying Risks Arising from the Use of IT and General IT Controls

18. Examples of risks arising from the use of IT include risks related to inappropriate reliance on IT applications that are inaccurately processing data, processing inaccurate data, or both, such as

    - Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions, or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database.
    - The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.
    - Unauthorized changes to data in master files.
    - Unauthorized changes to IT applications or other aspects of the IT environment.
    - Failure to make necessary changes to IT applications or other aspects of the IT environment.
    - Inappropriate manual intervention.
    - Potential loss of data or inability to access data as required.

19. The auditor's consideration of unauthorized access may include risks related to unauthorized access by internal or external parties (often referred to as cybersecurity risks). Such risks may not necessarily affect financial reporting, as an entity's IT environment may also include IT applications and related data that address operational or compliance needs. It is important to note that cyber incidents usually first occur through the perimeter and internal network layers, which tend to be further removed from the IT application, database and operating systems that affect the preparation of the financial statements. Accordingly, if information about a security breach has been identified, the auditor ordinarily considers the extent to which such a breach has the potential to affect financial reporting. If financial reporting may be affected, the auditor may decide to understand, and test the related controls to determine the possible impact or scope of potential misstatements in the financial statements or may determine that the entity has provided adequate disclosures in relation to such security breach.

20. In addition, laws and regulations that may have a direct or indirect effect on the entity's financial statements may include data protection legislation. Considering an entity's compliance with such laws or regulations, in accordance with ISA 250 (Revised), may involve understanding the entity's IT processes and general IT controls that the entity has implemented to address the relevant laws or regulations.

21. General IT controls are implemented to address risks arising from the use of IT. Accordingly, the auditor uses the understanding obtained about the identified IT applications and other aspects of the IT environment and the applicable risks arising from the use of IT in determining the general IT controls to identify. In some cases, an entity may use common IT processes across its IT environment or across certain IT applications, in which case common risks arising from the use of IT and common general IT controls may be identified.

22. In general, a greater number of general IT controls related to IT applications and databases are likely to be identified than for other aspects of the IT environment. This is because these aspects are the most closely concerned with the information processing and storage of information in the entity's information system. In identifying general IT controls, the auditor may consider controls over actions of both end users and of the entity's IT personnel or IT service providers.

23. **Appendix 6** provides further explanation of the nature of the general IT controls typically implemented for different aspects of the IT environment. In addition, examples of general IT controls for different IT processes are provided.

Appendix 6

(Ref: Para. 25(c)(ii), A173–A174)

Considerations for Understanding General IT Controls

This appendix provides further matters that the auditor may consider in understanding general IT controls.

1. The nature of the general IT controls typically implemented for each of the aspects of the IT environment:

   (a) Applications

   General IT controls at the IT application layer will correlate to the nature and extent of application functionality and the access paths allowed in the technology. For example, more controls will be relevant for highly-integrated IT applications with complex security options than a legacy IT application supporting a small number of account balances with access methods only through transactions.

   (b) Database

   General IT controls at the database layer typically address risks arising from the use of IT related to unauthorized updates to financial reporting information in the database through direct database access or execution of a script or program.

   (c) Operating system

   General IT controls at the operating system layer typically address risks arising from the use of IT related to administrative access, which can facilitate the override of other controls. This includes actions such as compromising other user's credentials, adding new, unauthorized users, loading malware or executing scripts or other unauthorized programs.

   (d) Network

   General IT controls at the network layer typically address risks arising from the use of IT related to network segmentation, remote access, and authentication. Network controls may be relevant when an entity has web-facing applications used in financial reporting. Network controls may be relevant when the entity has significant business partner relationships or third-party outsourcing, which may increase data transmissions and the need for remote access.

2. Examples of general IT controls that may exist, organized by IT process include:

(a) Process to manage access:

- *Authentication*

  Controls that ensure a user accessing the IT application or other aspect of the IT environment is using the user's own log-in credentials (i.e., the user is not using another user's credentials).

- *Authorization*

  Controls that allow users to access the information necessary for their job responsibilities and nothing further, which facilitates appropriate segregation of duties.

- *Provisioning*

  Controls to authorize new users and modifications to existing users' access privileges.

- *Deprovisioning*

  Controls to remove user access upon termination or transfer.

- *Privileged access*

  Controls over administrative or powerful users' access.

- *User access reviews*

  Controls to recertify or evaluate user access for ongoing authorization over time.

- *Security configuration controls*

  Each technology generally has key configuration settings that help restrict access to the environment.

- *Physical access*

  Controls over physical access to the data center and hardware, as such access may be used to override other controls.

(b) Process to manage program or other changes to the IT environment:

- *Change management process*

  Controls over the process to design, program, test and migrate changes to a production (i.e., end user) environment.

- *Segregation of duties over change migration*

  Controls that segregate access to make and migrate changes to a production environment.

- *Systems development or acquisition or implementation*

  Controls over initial IT application development or implementation (or in relation to other aspects of the IT environment).

- *Data conversion*

  Controls over the conversion of data during development, implementation or upgrades to the IT environment.

(c) Process to manage IT operations

- *Job scheduling*

  Controls over access to schedule and initiate jobs or programs that may affect financial reporting.

- *Job monitoring*

  Controls to monitor financial reporting jobs or programs for successful execution.

- *Backup and recovery*

  Controls to ensure backups of financial reporting data occur as planned and that such data is available and able to be accessed for timely recovery in the event of an outage or attack.

- *Intrusion detection*

  Controls to monitor for vulnerabilities and or intrusions in the IT environment.

The table below illustrates examples of general IT controls to address examples of risks arising from the use of IT, including for different IT applications based on their nature.

Process	**Risks**	**Controls**	**IT Applications**		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
Manage Access	User-access privileges: Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.	Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles/roles, critical financial reporting transactions, and segregation of duties	Yes – instead of user access reviews noted below	Yes	Yes
		Access for terminated or transferred users is removed or modified in a timely manner	Yes – instead of user access reviews below	Yes	Yes
		User access is periodically reviewed	Yes – instead of provisioning/ Deprovisioning controls above	Yes – for certain applications	Yes

Process	**Risks**	**Controls**	**IT Applications**		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
		Segregation of duties is monitored and conflicting access is either removed or mapped to mitigating controls, which are documented and tested	N/A – no system enabled segregation	Yes – for certain applications	Yes
		Privileged-level access (e.g., configuration, data and security administrators) is authorized and appropriately restricted	Yes – likely at IT application layer only	Yes – at IT application and certain layers of IT environment for platform	Yes – at all layers of IT environment for platform
Manage Access	Direct data access: Inappropriate changes are made directly to financial data through means other than application transactions.	Access to application data files or database objects/tables/ data is limited to authorized personnel, based on their job responsibilities and assigned role, and such access is approved by management	N/A	Yes – for certain applications and databases	Yes

Process	**Risks**	**Controls**	**IT Applications**		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
Manage Access	System settings: Systems are not adequately configured or updated to restrict system access to properly authorized and appropriate users.	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout)	Yes – password authentication only	Yes – mix of password and multi-factor authentication	Yes
		The key attributes of the security configuration are appropriately implemented	N/A – no technical security configurations exist	Yes – for certain applications and databases	Yes

Process	**Risks**	**Controls**	**IT Applications**		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
Manage Change	Application changes: Inappropriate changes are made to application systems or programs that contain relevant automated controls (i.e., configurable settings, automated algorithms, automated calculations, and automated data extraction) or report logic.	Application changes are appropriately tested and approved before being moved into the production environment	N/A – would verify no source code installed	Yes – for non-commercial software	Yes
		Access to implement changes into the application production environment is appropriately restricted and segregated from the development environment	N/A	Yes for non-commercial software	Yes
Manage Change	Database changes: Inappropriate changes are made to the database structure and relationships between the data.	Database changes are appropriately tested and approved before being moved into the production environment	N/A – no database changes made at entity	Yes – for non-commercial software	Yes

Process	**Risks**	**Controls**	**IT Applications**		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
Manage Change	System software changes: Inappropriate changes are made to system software (e.g., operating system, network, change-management software, access-control software).	System software changes are appropriately tested and approved before being moved to production	N/A – no system software changes are made at entity	Yes	Yes
Manage Change	Data conversion: Data converted from legacy systems or previous versions introduces data errors if the conversion transfers incomplete, redundant, obsolete, or inaccurate data.	Management approves the results of the conversion of data (e.g., balancing and reconciliation activities) from the old application system or data structure to the new application system or data structure and monitors that the conversion is performed in accordance with established conversion policies and procedures	N/A – Addressed through manual controls	Yes	Yes

Process	**Risks**	**Controls**	**IT Applications**		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
IT Operations	Network: The network does not adequately prevent unauthorized users from gaining inappropriate access to information systems.	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or professional policies and standards (e.g., password minimum length and complexity, expiration, account lockout)	N/A – no separate network authentication method exists	Yes	Yes
		Network is architected to segment web-facing applications from the internal network, where ICFR relevant applications are accessed	N/A – no network segmentation employed	Yes – with judgment	Yes – with judgment

Process	**Risks**	**Controls**	**IT Applications**		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
		On a periodic basis, vulnerability scans of the network perimeter are performed by the network management team, which also investigates potential vulnerabilities	N/A	Yes – with judgment	Yes – with judgment
		On a periodic basis, alerts are generated to provide notification of threats identified by the intrusion detection systems. These threats are investigated by the network management team	N/A	Yes – with judgment	Yes – with judgment
		Controls are implemented to restrict Virtual Private Network (VPN) access to authorized and appropriate users	N/A – no VPN	Yes – with judgment	Yes – with judgment

Process	**Risks**	**Controls**	**IT Applications**		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
IT Operations	Data backup and recovery: Financial data cannot be recovered or accessed in a timely manner when there is a loss of data.	Financial data is backed up on a regular basis according to an established schedule and frequency	N/A – relying on manual backups by finance team	Yes	Yes
IT Operations	Job scheduling: Production systems, programs, or jobs result in inaccurate, incomplete, or unauthorized processing of data.	Only authorized users have access to update the batch jobs (including interface jobs) in the job scheduling software	N/A – no batch jobs	Yes – for certain applications	Yes
		Critical systems, programs, or jobs are monitored, and processing errors are corrected to ensure successful completion.	N/A – no job monitoring	Yes – for certain applications	Yes