



MALAYSIAN INSTITUTE  
OF ACCOUNTANTS

**ISA 315 (Revised 2019)**  
Issued September 2021;  
Updated July 2022

*International Standard on Auditing™*

---

**ISA 315 (Revised 2019)**

and

**Conforming and Consequential  
Amendments to Other  
International Standards Arising  
from ISA 315 (Revised 2019)**

# **INTERNATIONAL STANDARD ON AUDITING 315 (REVISED 2019)**

## **IDENTIFYING AND ASSESSING THE RISKS OF MATERIAL MISSTATEMENT**

The Malaysian Institute of Accountants has approved this standard in July 2022 for publication. This standard should be read in conjunction with the Preface to the Malaysian Quality Control, Auditing, Review, Other Assurance and Related Services Pronouncements; and the Malaysian Approved Preface to the International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements; Glossary of Terms; and International Framework for Assurance Engagements.

The status of International Standards on Auditing is set out in the Preface to the Malaysian Quality Control, Auditing, Review, Other Assurance and Related Services Pronouncements.

### **Applicability**

International Standards on Auditing are to be applied in the audit of historical financial information.

### **Changes of substance from September 2021**

1. Changes made as appropriate, for cross-referencing and other changes as necessary.

### **Effective Date in Malaysia**

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

Copyright © April 2021 by IFAC. All rights reserved. This publication may be downloaded for personal and non-commercial use (i.e., professional reference or research) or purchased from [www.iaasb.org](http://www.iaasb.org). Written permission is required to translate, reproduce, store or transmit, or to make other similar uses of, this document.

**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 15 December 2021)

**CONTENTS**

---

	Paragraph
<b>Introduction</b>	
Scope of this ISA .....	1
Key Concepts .....	2
Scalability .....	9
Effective Date .....	10
<b>Objective</b> .....	11
<b>Definitions</b> .....	12
<b>Requirements</b>	
Risk Assessment Procedures 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
<b>Application and Other Explanatory Material</b>	
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,<sup>1</sup> including to obtain sufficient appropriate audit evidence to reduce audit risk to an acceptably low level.<sup>2</sup> Audit risk is a function of the risks of material misstatement and detection risk.<sup>3</sup> ISA 200 explains that the risks of material misstatement may exist at two levels:<sup>4</sup> 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.<sup>5</sup>
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

---

<sup>1</sup> ISA 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*

<sup>2</sup> ISA 200, paragraph 17

<sup>3</sup> ISA 200, paragraph 13(c)

<sup>4</sup> ISA 200, paragraph A36

<sup>5</sup> ISA 200, paragraphs 15–16

necessary to obtain sufficient appropriate audit evidence.<sup>6</sup> For 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<sup>7</sup> 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.<sup>8</sup> 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.<sup>9</sup>

### 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.<sup>10</sup> 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,

---

<sup>6</sup> ISA 200, paragraph A43a and ISA 330, *The Auditor’s Responses to Assessed Risks*, paragraph 6

<sup>7</sup> ISA 240, *The Auditor’s Responsibilities Relating to Fraud in an Audit of Financial Statements*

<sup>8</sup> ISA 330, paragraph 5

<sup>9</sup> ISA 330, paragraph 6

<sup>10</sup> ISA 200, paragraph A65a

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.

### **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<sup>11</sup> 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).

---

<sup>11</sup> 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.<sup>12</sup>
- (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.

---

<sup>12</sup> 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

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)	
<ul style="list-style-type: none"> <li>(a) Understanding the set of controls, processes and structures that address: (Ref: Para. A101–A102)</li> <li>(i) How management’s oversight responsibilities are carried out, such as the entity’s culture and management’s commitment to integrity and ethical values;</li> </ul>	<p>and</p> <ul style="list-style-type: none"> <li>(b) Evaluating whether: (Ref: Para. A103–A108)</li> <li>(i) Management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior;</li> </ul>

<ul style="list-style-type: none"> <li>(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;</li> <li>(iii) The entity's assignment of authority and responsibility;</li> <li>(iv) How the entity attracts, develops, and retains competent individuals; and</li> <li>(v) How the entity holds individuals accountable for their responsibilities in the pursuit of the objectives of the system of internal control;</li> </ul>	<ul style="list-style-type: none"> <li>(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</li> <li>(iii) Control deficiencies identified in the control environment undermine the other components of the entity's system of internal control.</li> </ul>
---	---

The entity's risk assessment process

<p>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:</p>	
<ul style="list-style-type: none"> <li>(a) Understanding the entity's process for: (Ref: Para. A109–A110) <ul style="list-style-type: none"> <li>(i) Identifying business risks relevant to financial reporting objectives; (Ref: Para. A62)</li> <li>(ii) Assessing the significance of those risks, including the</li> </ul> </li> </ul>	<p>and</p> <ul style="list-style-type: none"> <li>(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)</li> </ul>

likelihood of their occurrence; and	
(iii) Addressing those risks;	

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

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)	
<ul style="list-style-type: none"> <li>(a) Understanding those aspects of the entity’s process that address: <ul style="list-style-type: none"> <li>(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</li> <li>(ii) The entity’s internal audit function, if any, including its nature, responsibilities and activities; (Ref: Para. A118)</li> </ul> </li> <li>(b) Understanding the sources of the information used in the</li> </ul>	<p style="text-align: center;">and</p> <ul style="list-style-type: none"> <li>(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)</li> </ul>

<p>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)</p>	
--	--

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

The information system and communication

<p>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)</p>	
<p>(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)</p> <p>(i) How information flows through the entity's information system, including how:</p> <p>a. Transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger and</p>	<p>and</p> <p>(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)</p>

<p>reported in the financial statements; and</p> <p>b. Information about events and conditions, other than transactions, is captured, processed and disclosed in the financial statements;</p>	
<p>(ii) The accounting records, specific accounts in the financial statements and other supporting records relating to the flows of information in the information system;</p> <p>(iii) The financial reporting process used to prepare the entity's financial statements, including disclosures; and</p> <p>(iv) The entity's resources, including the IT environment, relevant to (a)(i) to (a)(iii) above;</p> <p>(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)</p> <p>(i) Between people within the entity, including how financial reporting roles and responsibilities are</p>	

<p style="text-align: center;">communicated;</p> <p>(ii) Between management and those charged with governance; and</p> <p>(iii) With external parties, such as those with regulatory authorities;</p>	
---	--

Control activities

<p>26. The auditor shall obtain an understanding of the control activities component, through performing risk assessment procedures, by: (Ref: Para. A147–A157)</p>	
<p>(a) Identifying controls that address risks of material misstatement at the assertion level in the control activities component as follows:</p> <p style="padding-left: 40px;">Controls that address a risk that is determined to be a significant risk; (Ref: Para. A158–A159)</p> <p style="padding-left: 40px;">Controls over journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments; (Ref: Para. A160–A161)</p> <p style="padding-left: 40px;">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</p>	<p>and</p> <p>(d) For each control identified in (a) or (c)(ii): (Ref: Para. A175–A181)</p> <p style="padding-left: 40px;">(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</p> <p style="padding-left: 40px;">(ii) Determining whether the control has been implemented by</p>

<p>substantive procedures alone do not provide sufficient appropriate audit evidence; and (Ref: Para. A162–A164)</p>	<p>performing procedures in addition to inquiry of the entity’s personnel.</p>
<p>(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)</p> <p>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)</p> <p>For such IT applications and other aspects of the IT environment identified in (b), identifying: (Ref: Para. A173–A174)</p> <p>The related risks arising from the use of IT; and</p> <p>The entity’s general IT controls that address such risks;</p>	

*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:<sup>13</sup> (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;

---

<sup>13</sup> ISA 230, *Audit Documentation*, paragraphs 8–11, and A6–A7

- (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.

## **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,<sup>14</sup> 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

---

<sup>14</sup> ISA 580, *Written Representations*

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.

- 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.<sup>15</sup> 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)<sup>16</sup> in regard to accounting estimates;
- ISA 550 in regard to related party relationships and transactions;
- ISA 570 (Revised)<sup>17</sup> in regard to going concern; and
- ISA 600<sup>18</sup> 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)*

---

<sup>15</sup> ISA 240, paragraphs 12–27

<sup>16</sup> ISA 540 (Revised), *Auditing Accounting Estimates and Related Disclosures*

<sup>17</sup> ISA 570 (Revised), *Going Concern*

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

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.

*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<sup>19</sup>, 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.<sup>20</sup>

*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.

---

<sup>19</sup> See paragraphs A37 and A38.

<sup>20</sup> ISA 500, *Audit Evidence*, paragraph 7

**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.

- 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<sup>21</sup> 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.<sup>22</sup> 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

---

<sup>21</sup> ISA 500, paragraphs A14–A17 and A21–A25

<sup>22</sup> ISA 500, paragraph A12

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 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)<sup>23</sup> 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.

---

<sup>23</sup> ISA 260 (Revised), *Communication with Those Charged with Governance*, paragraph 4(b)

- 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.

#### 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<sup>24</sup> 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

---

<sup>24</sup> ISA 520, *Analytical Procedures*

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.

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.<sup>25</sup>
- 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.

---

<sup>25</sup> ISA 220, *Quality Control for an Audit of Financial Statements*, paragraph 12

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 a 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 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.<sup>26</sup>

- 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.

---

<sup>26</sup> ISA 240, paragraph 16

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;<sup>27</sup>
- Evaluating whether the financial statements provide adequate disclosures in accordance with ISA 700 (Revised);<sup>28</sup>
- Determining materiality or performance materiality in accordance with ISA 320;<sup>29</sup> 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;<sup>30</sup>
- 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 entities that are more complex. The depth of the understanding that is required by the

---

<sup>27</sup> ISA 250 (Revised), *Consideration of Laws and Regulations in an Audit of Financial Statements*, paragraph 14

<sup>28</sup> ISA 700 (Revised), *Forming an Opinion and Reporting on Financial Statements*, paragraph 13(e)

<sup>29</sup> ISA 320, *Materiality in Planning and Performing an Audit*, paragraphs 10–11

<sup>30</sup> ISA 520, paragraph 5

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.<sup>31</sup>
- The distinction between the owners, those charged with governance and management.

---

<sup>31</sup> 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.<sup>32</sup>

- 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.

---

<sup>32</sup> 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.

**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).

## 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.<sup>33</sup>

### 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.

---

<sup>33</sup> ISA 220, paragraph 14

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.<sup>34</sup>

#### 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.

#### 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.

---

<sup>34</sup> ISA 250 (Revised), paragraph 13

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.<sup>35</sup>

## 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.

---

<sup>35</sup> ISA 330, paragraphs A1–A3

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).

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.<sup>36</sup>

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

---

<sup>36</sup> ISA 240, paragraph 19

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)<sup>37</sup> 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

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))

---

<sup>37</sup> ISA 610 (Revised 2013), *Using the Work of Internal Auditors*

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.<sup>38</sup>

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.

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.

---

<sup>38</sup> ISA 570 (Revised), paragraphs 19–20

## 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.<sup>39</sup>

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.<sup>40</sup> 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.

**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.

---

<sup>39</sup> ISA 240, paragraph A28

<sup>40</sup> ISA 330, paragraph 21

A159. ISA 240<sup>41</sup> 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.

**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.

---

<sup>41</sup> ISA 240, paragraphs 28 and A33

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,<sup>42</sup> 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<sup>43</sup> 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 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:

---

<sup>42</sup> ISA 330, paragraph 8(b)

<sup>43</sup> ISA 330, paragraph 8(a)

- 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.<sup>44</sup>

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.

- 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.,

<sup>44</sup> ISA 402, *Audit Considerations Relating to an Entity Using a Service Organization*

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.<sup>45</sup>

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,<sup>46</sup> the auditor may determine that certain of the entity's policies in a component are not appropriate to the nature and circumstances of the entity. Such a determination may be an indicator that assists the auditor in identifying control deficiencies. 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.

---

<sup>45</sup> ISA 330, paragraphs 8–11

<sup>46</sup> Paragraphs 21(b), 22(b), 24(c), 25(c) and 26(d)

A183. If the auditor has identified one or more control deficiencies, ISA 265<sup>47</sup> 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.<sup>48</sup>

**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 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

---

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

<sup>48</sup> 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.

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.<sup>49</sup>

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:
  - (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.

---

<sup>49</sup> ISA 200, paragraph A15a

- (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.<sup>50</sup>

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 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.

---

<sup>50</sup> ISA 330, paragraph 5

**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)<sup>51</sup> 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.

*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

---

<sup>51</sup> ISA 705 (Revised), *Modifications to the Opinion in the Independent Auditor’s Report*

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.<sup>52</sup>
- ISA 330 requires the auditor to obtain more persuasive audit evidence the higher the auditor's assessment of risk.<sup>53</sup>
- ISA 260 (Revised) requires communicating with those charged with governance about the significant risks identified by the auditor.<sup>54</sup>
- 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.<sup>55</sup>
- 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.<sup>56</sup>
- 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.<sup>57</sup>

---

<sup>52</sup> ISA 330, paragraphs 15 and 21

<sup>53</sup> ISA 330, paragraph 7(b)

<sup>54</sup> ISA 260 (Revised), paragraph 15

<sup>55</sup> ISA 701, *Communicating Key Audit Matters in the Independent Auditor's Report*, paragraph 9

<sup>56</sup> ISA 220, paragraphs 17 and A19

<sup>57</sup> ISA 600, paragraphs 30 and 31

## 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.<sup>58</sup>

### **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:

- Transactions for which there are multiple acceptable accounting treatments such that subjectivity is involved.
- Accounting estimates that have high estimation uncertainty or complex models.

---

<sup>58</sup> ISA 240, paragraphs 26–28

- 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,<sup>59</sup> 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.
- 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.

---

<sup>59</sup> ISA 330, paragraph 8

**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.<sup>60</sup> 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 general IT controls that support the continued functioning of that automated control to

---

<sup>60</sup> ISA 540 (Revised), paragraphs A87–A89

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.<sup>61</sup>

*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.<sup>62</sup>

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.

---

<sup>61</sup> ISA 330, paragraphs A29–A30

<sup>62</sup> ISA 500, paragraph A1

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

A233. As explained in ISA 320,<sup>63</sup> materiality and audit risk are considered when identifying and assessing the risks of material misstatement in classes of transactions, account balances and disclosures. The auditor's determination of materiality is a matter of professional judgment, and is affected by the auditor's perception of the financial information needs of users of the financial statements.<sup>64</sup> 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.<sup>65</sup> 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

---

<sup>63</sup> ISA 320, paragraph A1

<sup>64</sup> ISA 320, paragraph 4

<sup>65</sup> ISA 330, paragraph 18

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.

**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.<sup>66</sup> 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

---

<sup>66</sup> ISA 230, paragraph A7

entity, and to determine whether one or more control deficiencies have been identified;

- Paragraph 35, which requires the auditor to take into account all audit evidence obtained from the risk assessment procedures, whether corroborative or contradictory to assertions made by management, and to evaluate whether the audit evidence obtained from the risk assessment procedures provides an appropriate basis for the identification and assessment of the risks of material misstatement; and
- 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<sup>67</sup> 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.<sup>68</sup> 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.<sup>69</sup>

---

<sup>67</sup> ISA 230, paragraph 8

<sup>68</sup> ISA 300, *Planning an Audit of Financial Statements*, paragraphs 7, 9 and A11

<sup>69</sup> 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.<sup>70</sup>
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.

---

<sup>70</sup> 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<sup>71</sup> 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

---

<sup>71</sup> 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.

<p>Relevant Inherent Risk Factor:</p>	<p>Examples of Events or Conditions That May Indicate the Existence of Risks of Material Misstatement at the Assertion Level:</p>
<p>Complexity</p>	<p>Regulatory: Operations that are subject to a high degree of complex regulation.</p> <p>Business model: The existence of complex alliances and joint ventures.</p> <p>Applicable financial reporting framework: Accounting measurements that involve complex processes.</p> <p>Transactions: Use of off-balance sheet finance, special-purpose entities, and other complex financing arrangements.</p>
<p>Subjectivity</p>	<p>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.</p> <p>Management's selection of a valuation technique or model for a non-current asset, such as investment properties.</p>
<p>Change</p>	<p>Economic conditions: Operations in regions that are economically unstable, for example, countries with significant currency devaluation or highly inflationary economies.</p> <p>Markets: Operations exposed to volatile markets, for example, futures trading.</p> <p>Customer loss: Going concern and liquidity issues including loss of significant customers.</p> <p>Industry model: Changes in the industry in which the entity operates.</p> <p>Business model:</p>

<p>Relevant Inherent Risk Factor:</p>	<p>Examples of Events or Conditions That May Indicate the Existence of Risks of Material Misstatement at the Assertion Level:</p>
	<p>Changes in the supply chain. Developing or offering new products or services, or moving into new lines of business.</p>
	<p>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.</p>
<p>Uncertainty</p>	<p>Reporting: Events or transactions that involve significant measurement uncertainty, including accounting estimates, and related disclosures.</p>

Relevant Inherent Risk Factor:	Examples of Events or Conditions That May Indicate the Existence of Risks of Material Misstatement at the Assertion Level:
	Pending litigation and contingent liabilities, for example, sales warranties, financial guarantees and environmental remediation.
Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk	<p>Reporting: Opportunities for management and employees to engage in fraudulent financial reporting, including omission, or obscuring, of significant information in disclosures.</p> <p>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.</p>

*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.<sup>72</sup> The entity's process to monitor the entity's system of internal control may include activities such as management's review of whether bank reconciliations are being prepared on a timely basis, internal auditors' evaluation of sales personnel's compliance with the entity's policies on terms of sales contracts, and a legal department's oversight of compliance with the entity's ethical or business practice policies. Monitoring is done also to ensure that controls continue to operate effectively over time. For example, if the timeliness and accuracy of bank reconciliations are not monitored, personnel are likely to stop preparing them.
12. Controls related to the entity's process to monitor the entity's system of internal control, including those that monitor underlying automated controls, may be automated or manual, or a combination of both. For example, an entity may use automated monitoring controls over access to certain technology with automated reports of unusual activity to management, who manually investigate identified anomalies.
13. When distinguishing between a monitoring activity and a control related to the information system, the underlying details of the activity are considered, especially when the activity involves some level of supervisory review. Supervisory reviews are not automatically classified as monitoring activities and it may be a matter of judgment whether a review is classified as a control related to the information system or a monitoring activity. For example, the intent of a monthly completeness control would be to detect and correct errors, where a monitoring activity would ask why

---

<sup>72</sup> ISA 610 (Revised 2013) and Appendix 4 of this ISA provide further guidance related to internal audit.

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.<sup>73</sup> Inquiries of particular relevance may be about matters the internal audit function has raised with those charged with governance

---

<sup>73</sup> The relevant requirements are contained in ISA 610 (Revised 2013).

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,<sup>74</sup> if the internal audit function provides information to the auditor regarding any actual, suspected or alleged fraud, the auditor takes this into account in the auditor's identification of risk of material misstatement due to fraud.
6. Appropriate individuals within the internal audit function with whom inquiries are made are those who, in the auditor's judgment, have the appropriate knowledge, experience and authority, such as the chief internal audit executive or, depending on the circumstances, other personnel within the function. The auditor may also consider it appropriate to have periodic meetings with these individuals.

### **Consideration of the Internal Audit Function in Understanding the Control Environment**

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

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

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

---

<sup>74</sup> ISA 240, paragraph 19

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,<sup>75</sup> 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.

---

<sup>75</sup> 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
The extent of the entity’s reliance on	Simple automated	Simple relevant automated report	Complex automated report

	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)
system-generated reports in the processing of information.	report logic	logic	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; <sup>76</sup> Use of internal or external IT service providers (e.g., third-party storage or hosting of data)
Matters related to the IT applications and IT infrastructure:			
The type of application	Purchased	Purchased	Custom

	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)
(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).	application with little or no customization	application or simple legacy or low-end ERP applications with little or no customization	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
Matters related to IT processes:			

	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 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
Whether program changes have been made to the manner in which information is	Commercial software with no source code installed	Some commercial applications with no source code and other mature	New or large number or complex changes, several

	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)
processed, and the extent of such changes during the period.		applications with a small number or simple changes; traditional systems development lifecycle	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*

- 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
<p>Standalone applications.</p> <p>The volume of data (transactions) is not significant.</p> <p>The application's functionality is not complex.</p> <p>Each transaction is supported by original hard copy documentation.</p>	<p>Applications are interfaced.</p> <p>The volume of data (transactions) is significant.</p> <p>The application's functionality is complex as:</p> <ul style="list-style-type: none"> <li>The application automatically initiates transactions; and</li> <li>There are a variety of complex calculations underlying automated entries.</li> </ul>
<p>IT application is likely not subject to risks arising from IT because:</p> <p>The volume of data is not significant and therefore management is not relying upon general IT controls to process or maintain the data.</p>	<p>IT application is likely subject to risks arising from IT because:</p> <p>Management relies on an application system to process or maintain data as the volume of data is significant.</p>
<p>Management does not rely on automated controls or other automated functionality. The auditor has not identified automated controls in accordance with paragraph 26(a).</p> <p>Although management uses system-generated reports in their</p>	<p>Management relies upon the application system to perform certain automated controls that the auditor has also identified.</p>

<p>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.</p> <p>The auditor will directly test information produced by the entity used as audit evidence.</p>	
---	--

*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:
    - o *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/De provisioning 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	Access to application data files or database objects/tables/data is limited to authorized personnel, based on their job responsibilities	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)
	application transactions.	and assigned role, and such access is approved by management			
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

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)
		The key attributes of the security configuration are appropriately implemented	N/A – no technical security configurations exist	Yes – for certain applications and databases	Yes
Manage Change	Application changes: Inappropriate changes are made to application systems or programs that contain relevant automated controls (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

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	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
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

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	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
IT Operations	Network: The network does not adequately prevent unauthorized	Access is authenticated through unique user IDs and passwords or other methods as	N/A – no separate network authentication method exists	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)
	users from gaining inappropriate access to information systems.	<p>a mechanism for validating that users are authorized to gain access to the system.</p> <p>Password parameters meet company or professional policies and standards (e.g., password minimum length and complexity, expiration, account lockout)</p>			
		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

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)
		Controls are implemented to restrict Virtual Private Network (VPN) access to authorized and appropriate users	N/A – no VPN	Yes – with judgment	Yes – with judgment
IT Operations	Data backup and recovery: Financial data cannot be recovered or accessed in a timely manner when there is a loss of data.	Financial data is backed up on a regular basis according to an established schedule and frequency	N/A – relying on manual backups by finance team	Yes	Yes
IT Operations	Job scheduling: Production systems, programs, or jobs result in inaccurate, incomplete, or unauthorized	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

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)
	processing of data.	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

# CONFORMING AND CONSEQUENTIAL AMENDMENTS TO OTHER INTERNATIONAL STANDARDS ARISING FROM ISA 315 (REVISED 2019)

**Note:** The following are conforming amendments to other International Standards as a result of the approval of ISA 315 (Revised 2019). These amendments will become effective at the same time as ISA 315 (Revised 2019), and are shown with marked changes from the latest approved versions of the International Standards that are amended. The footnote numbers within these amendments do not align with the International Standards that are amended, and reference should be made to those International Standards. These conforming amendments have received the approval of the PIOB which concluded that due process was followed in the development of the conforming amendments and that proper regard was paid to the public interest.

## ***ISA 200, Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing***

### **Scope of this ISA**

...

### **An Audit of Financial Statements**

...

7. The ISAs contain objectives, requirements and application and other explanatory material that are designed to support the auditor in obtaining reasonable assurance. The ISAs require that the auditor exercise professional judgment and maintain professional skepticism throughout the planning and performance of the audit and, among other things:

- Identify and assess risks of material misstatement, whether due to fraud or error, based on an understanding of the entity and its environment, the applicable financial reporting framework and including the entity's system of internal control.
- Obtain sufficient appropriate audit evidence about whether material misstatements exist, through designing and implementing appropriate responses to the assessed risks.
- Form an opinion on the financial statements based on conclusions drawn from the audit evidence obtained.

...

### **Effective Date**

...

## **Overall Objectives of the Auditor**

...

## **Definitions**

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

...

- (n) Risk of material misstatement – The risk that the financial statements are materially misstated prior to audit. This consists of two components, described as follows at the assertion level: (Ref: Para. A15a)
  - (i) Inherent risk – The susceptibility of an assertion about a class of transaction, account balance or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls.
  - (ii) Control risk – The risk that a misstatement that could occur in an assertion about a class of transactions, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's ~~internal~~ controls.

...

## **Requirements**

### **Ethical Requirements Relating to an Audit of Financial Statements**

...

### **Professional Skepticism**

...

### **Professional Judgment**

...

### **Sufficient Appropriate Audit Evidence and Audit Risk**

17. To obtain reasonable assurance, the auditor shall obtain sufficient appropriate audit evidence to reduce audit risk to an acceptably low level and thereby enable the auditor to draw reasonable conclusions on which to base the auditor's opinion. (Ref: Para. A30–A54)

## **Conduct of an Audit in Accordance with ISAs**

### *Complying with ISAs Relevant to the Audit*

...

19. The auditor shall have an understanding of the entire text of an ISA, including its application and other explanatory material, to understand its objectives and to apply its requirements properly. (Ref: Para. A60–A68)

...

### *Objectives Stated in Individual ISAs*

...

### *Complying with Relevant Requirements*

...

### *Failure to Achieve an Objective*

...

## **Application and Other Explanatory Material**

### **An Audit of Financial Statements**

#### *Scope of the Audit* (Ref: Para. 3)

...

#### *Preparation of the Financial Statements* (Ref: Para. 4)

...

#### Considerations Specific to Audits in the Public Sector

...

#### *Form of the Auditor's Opinion* (Ref: Para. 8)

...

### **Definitions**

#### *Financial Statements* (Ref: Para. 13(f))

...

Risk of Material Misstatement (Ref: Para. 13(n))

A15a. For the purposes of the ISAs, a risk of material misstatement exists when there is a reasonable possibility of:

- (a) A misstatement occurring (i.e., its likelihood); and
- (b) Being material if it were to occur (i.e., its magnitude).

**Ethical Requirements Relating to an Audit of Financial Statements (Ref: Para. 14)**

...

**Professional Skepticism (Ref: Para. 15)**

...

**Professional Judgment (Ref: Para. 16)**

...

**Sufficient Appropriate Audit Evidence and Audit Risk (Ref: Para. 5 and 17)**

*Sufficiency and Appropriateness of Audit Evidence*

A30. Audit evidence is necessary to support the auditor's opinion and report. It is cumulative in nature and is primarily obtained from audit procedures performed during the course of the audit. It may, however, also include information obtained from other sources such as previous audits (provided the auditor has determined whether changes have occurred since the previous audit that may affect its relevance to the current audit<sup>76</sup>) or a firm's quality control procedures for client acceptance and continuance. In addition to other sources inside and outside the entity, the entity's accounting records are an important source of audit evidence. Also, information that may be used as audit evidence may have been prepared by an expert employed or engaged by the entity. Audit evidence comprises both information that supports and corroborates management's assertions, and any information that contradicts such assertions. In addition, in some cases, the absence of information (for example, management's refusal to provide a requested representation) is used by the auditor, and therefore, also constitutes audit evidence. Most of the auditor's work in forming the auditor's opinion consists of obtaining and evaluating audit evidence.

...

---

<sup>76</sup> ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment*, paragraph 169

## Audit Risk

...

### Risks of Material Misstatement

...

A40. Inherent risk is ~~influenced by inherent risk factors, higher for some assertions and related classes of transactions, account balances, and disclosures than for others. Depending on the degree to which the inherent risk factors affect the susceptibility to misstatement of an assertion, the level of inherent risk varies on a scale that is referred to as the spectrum of inherent risk. The auditor determines significant classes of transactions, account balances and disclosures, and their relevant assertions, as part of the process of identifying and assessing the risks of material misstatement. For example, it may be higher for complex calculations or for accounts balances consisting of amounts derived from accounting estimates that are subject to significant estimation uncertainty may be identified as significant account balances, and the auditor's assessment of inherent risk for the related risks at the assertion level may be higher because of the high estimation uncertainty.~~

A40a. External circumstances giving rise to business risks may also influence inherent risk. For example, technological developments might make a particular product obsolete, thereby causing inventory to be more susceptible to overstatement. Factors in the entity and its environment that relate to several or all of the classes of transactions, account balances, or disclosures may also influence the inherent risk related to a specific assertion. Such factors may include, for example, a lack of sufficient working capital to continue operations or a declining industry characterized by a large number of business failures.

A41. Control risk is a function of the effectiveness of the design, implementation and maintenance of ~~internal controls~~ by management to address identified risks that threaten the achievement of the entity's objectives relevant to preparation of the entity's financial statements. However, internal control, no matter how well designed and operated, can only reduce, but not eliminate, risks of material misstatement in the financial statements, because of the inherent limitations of ~~internal controls~~. These include, for example, the possibility of human errors or mistakes, or of controls being circumvented by collusion or inappropriate management override. Accordingly, some control risk will always exist. The ISAs provide the conditions under which the auditor is required to, or may choose to, test the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures to be performed.<sup>77</sup>

---

<sup>77</sup> ISA 330, *The Auditor's Responses to Assessed Risks*, paragraphs 7–17

A42.<sup>78</sup>The assessment of the risks of material misstatement may be expressed in quantitative terms, such as in percentages, or in non-quantitative terms. In any case, the need for the auditor to make appropriate risk assessments is more important than the different approaches by which they may be made. The ISAs ~~typically do not ordinarily refer to inherent risk and control risk separately, but rather to a combined assessment of the “risks of material misstatement.” rather than to inherent risk and control risk separately.~~ However, ISA 540~~315~~ (Revised 2019)<sup>79</sup> requires a ~~separate assessment of inherent risk to be assessed separately from and control risk to provide a basis for de signing and performing further audit procedures to respond to the assessed risks of material misstatement at the assertion level, including significant risks, for accounting estimates at the assertion level in accordance with ISA 330.~~<sup>80</sup> ~~In identifying and assessing risks of material misstatement for significant classes of transactions, account balances or disclosures other than accounting estimates, the auditor may make separate or combined assessments of inherent and control risk depending on preferred audit techniques or methodologies and practical considerations.~~

A43a. 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.<sup>81</sup>

Detection Risk

...

*Inherent Limitations of an Audit*

...

The Nature of Financial Reporting

...

The Nature of Audit Procedures

...

Timeliness of Financial Reporting and the Balance between Benefit and Cost

...

---

<sup>78</sup> Note that paragraph A42 of ISA 200 is marked to the updated paragraph presented separately as a conforming amendment relating to ISA 540 (Revised) and its conforming amendments.

<sup>79</sup> ISA 540~~315~~ (Revised 2019), *Auditing Accounting Estimates and Disclosures*, paragraph 15 *Identifying and Assessing the Risks of Material Misstatement*

<sup>80</sup> ISA 330, paragraph 7(b)

<sup>81</sup> ISA 330, paragraph 6

A52. In light of the approaches described in paragraph A51, the ISAs contain requirements for the planning and performance of the audit and require the auditor, among other things, to:

- Have a basis for the identification and assessment of risks of material misstatement at the financial statement and assertion levels by performing risk assessment procedures and related activities;<sup>82</sup> and
- Use testing and other means of examining populations in a manner that provides a reasonable basis for the auditor to draw conclusions about the population.<sup>83</sup>

Other Matters that Affect the Inherent Limitations of an Audit

...

### **Conduct of an Audit in Accordance with ISAs**

*Nature of the ISAs* (Ref: Para. 18)

...

Considerations Specific to Audits in the Public Sector

...

*Contents of the ISAs* (Ref: Para. 19)

A60. In addition to objectives and requirements (requirements are expressed in the ISAs using “shall”), an ISA contains related guidance in the form of application and other explanatory material. It may also contain introductory material that provides context relevant to a proper understanding of the ISA, and definitions. The entire text of an ISA, therefore, is relevant to an understanding of the objectives stated in an ISA and the proper application of the requirements of an ISA.

A61. Where necessary, the application and other explanatory material provides further explanation of the requirements of an ISA and guidance for carrying them out. In particular, it may:

- Explain more precisely what a requirement means or is intended to cover, including in some ISAs such as ISA 315 (Revised 2019), why a procedure is required.
- Include examples of procedures that may be appropriate in the circumstances. In some ISAs, such as ISA 315 (Revised 2019), examples are presented in boxes.

---

<sup>82</sup> ISA 315 (Revised 2019), paragraphs 135-40

<sup>83</sup> ISA 330; ISA 500; ISA 520, *Analytical Procedures*; ISA 530, *Audit Sampling*

While such guidance does not in itself impose a requirement, it is relevant to the proper application of the requirements of an ISA. The application and other explanatory material may also provide background information on matters addressed in an ISA.

#### Considerations Specific to Smaller Entities Scalability Considerations

A65a Scalability considerations have been included in some ISAs (e.g., ISA 315 (Revised 2019)), illustrating the application of the requirements to all entities regardless of whether their nature and circumstances are less complex or more complex. Less complex entities are entities for which the characteristics in paragraph A66 may apply.

A65b. The “considerations specific to smaller entities” included in some the ISAs have been developed primarily with unlisted entities in mind. Some of the considerations, however, may be helpful in audits of smaller listed entities.

A66. For purposes of specifying additional considerations to audits of smaller entities, a “smaller entity” refers to an entity which typically possesses qualitative characteristics such as:

- (a) Concentration of ownership and management in a small number of individuals (often a single individual – either a natural person or another enterprise that owns the entity provided the owner exhibits the relevant qualitative characteristics); and
- (b) One or more of the following:
  - (i) Straightforward or uncomplicated transactions;
  - (ii) Simple record-keeping;
  - (iii) Few lines of business and few products within business lines;
  - (iv) Simpler systems of ~~Few~~ internal controls;
  - (v) Few levels of management with responsibility for a broad range of controls; or
  - (vi) Few personnel, many having a wide range of duties.

These qualitative characteristics are not exhaustive, they are not exclusive to smaller entities, and smaller entities do not necessarily display all of these characteristics.

A67. [*Moved – now A65b*]

#### Considerations Specific to Automated Tools and Techniques

A67a. The considerations specific to “automated tools and techniques” included in some ISAs (for example, ISA 315 (Revised 2019)) have been developed to explain how

the auditor may apply certain requirements when using automated tools and techniques in performing audit procedures.

*Objectives Stated in Individual ISAs* (Ref: Para. 21)

...

Use of Objectives to Determine Need for Additional Audit Procedures (Ref: Para. 21(a))

...

Use of Objectives to Evaluate Whether Sufficient Appropriate Audit Evidence Has Been Obtained (Ref: Para. 21(b))

...

*Complying with Relevant Requirements*

Relevant Requirements (Ref: Para. 22)

...

Departure from a Requirement (Ref: Para. 23)

...

*Failure to Achieve an Objective* (Ref: Para. 24)

...

## ***ISA 210, Agreeing the Terms of Audit Engagements***

**Application and Other Explanatory Material**

...

**Preconditions for an Audit**

...

*Agreement of the Responsibilities of Management*

...

**Internal Control**

...

A18. It is for management to determine what internal control is necessary to enable the preparation of the financial statements. The term “internal control” encompasses a

wide range of activities within components of the system of internal control that may be described as the control environment; the entity's risk assessment process; the entity's process to monitor the system of internal control, the information system, ~~including the related business processes relevant to financial reporting,~~ and communication; ~~and~~ control activities; ~~and~~ monitoring of controls. This division, however, does not necessarily reflect how a particular entity may design, implement and maintain its internal control, or how it may classify any particular component.<sup>84</sup> An entity's internal control (in particular, its accounting books and records, or accounting systems) will reflect the needs of management, the complexity of the business, the nature of the risks to which the entity is subject, and relevant laws or regulation.

## **ISA 230, *Audit Documentation***

### **Application and Other Explanatory Material**

...

#### **Documentation of the Audit Procedures Performed and Audit Evidence Obtained**

...

*Identification of Specific Items or Matters Tested, and of the Preparer and Reviewer* (Ref: Para. 9)

...

Considerations Specific to Smaller Entities (Ref. Para 8)

...

A17. When preparing audit documentation, the auditor of a smaller entity may also find it helpful and efficient to record various aspects of the audit together in a single document, with cross-references to supporting working papers as appropriate. Examples of matters that may be documented together in the audit of a smaller entity include the understanding of the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control, the overall audit strategy and audit plan, materiality determined in accordance with ISA 320,<sup>85</sup> assessed risks, significant matters noted during the audit, and conclusions reached.

...

---

<sup>84</sup> ISA 315 (Revised 2019), paragraph A9159 and Appendix 34

<sup>85</sup> ISA 320, *Materiality in Planning and Performing an Audit*

## **ISA 250 (Revised), *Consideration of Laws and Regulations in an Audit of Financial Statements***

### **Application and Other Explanatory Material**

...

### **Audit Procedures When Non-Compliance is Identified or Suspected**

...

#### *Evaluating the Implications of Identified or Suspected Non-Compliance (Ref: Para. 22)*

A23. As required by paragraph 22, the auditor evaluates the implications of identified or suspected non-compliance in relation to other aspects of the audit, including the auditor's risk assessment and the reliability of written representations. The implications of particular identified or suspected non-compliance will depend on the relationship of the perpetration and concealment, if any, of the act to specific controls activities and the level of management or individuals working for, or under the direction of, the entity involved, especially implications arising from the involvement of the highest authority within the entity. As noted in paragraph 9, the auditor's compliance with law, regulation or relevant ethical requirements may provide further information that is relevant to the auditor's responsibilities in accordance with paragraph 22.

...

## **ISA 260 (Revised), *Communication with Those Charged with Governance***

### **Application and Other Explanatory Material**

...

### **Matters to Be Communicated**

...

#### *Planned Scope and Timing of the Audit (Ref: Para. 15)*

...

A12. Communicating significant risks identified by the auditor helps those charged with governance understand those matters and why they were determined to be significant risks ~~require special audit consideration~~. The communication about significant risks may assist those charged with governance in fulfilling their responsibility to oversee the financial reporting process.

A13. Matters communicated may include: ...

- How the auditor plans to address the significant risks of material misstatement, whether due to fraud or error.
- How the auditor plans to address areas of higher assessed risks of material misstatement.
- The auditor's approach to the entity's system of internal control, ~~relevant to the audit.~~
- The application of the concept of materiality in the context of an audit.
- ...

## **Appendix 2**

(Ref: Para. 16(a), A19–A20)

### **Qualitative Aspects of Accounting Practices**

The communication required by paragraph 16(a), and discussed in paragraphs A19–A20, may include such matters as:

...

#### **Accounting Estimates**

- For items for which estimates are significant, issues discussed in ISA 540 (Revised),<sup>1</sup> including, for example:
  - How management identifies those transactions, events ~~and~~ **or** conditions that may give rise to the need for accounting estimates to be recognized or disclosed in the financial statements.

...

### ***ISA 265, Communicating Deficiencies in Internal Control to Those Charged with Governance***

#### **Introduction**

##### **Scope of this ISA**

1. This International Standard on Auditing (ISA) deals with the auditor's responsibility to communicate appropriately to those charged with governance and management deficiencies in internal control that the auditor has identified in an audit of financial statements. This ISA does not impose additional responsibilities on the auditor regarding obtaining an understanding of the entity's system of internal control and designing and performing tests of controls over and above the

requirements of ISA 315 (Revised 2019)<sup>86</sup> and ISA 330. ISA 260 (Revised) establishes further requirements and provides guidance regarding the auditor's responsibility to communicate with those charged with governance in relation to the audit.

2. The auditor is required to obtain an understanding of the entity's system of internal control relevant to the audit when identifying and assessing the risks of material misstatement.<sup>4</sup> In making those risk assessments, the auditor considers the entity's system of internal control in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of internal control. The auditor may identify control deficiencies in the entity's system of internal control not only during this risk assessment process but also at any other stage of the audit. This ISA specifies which identified deficiencies the auditor is required to communicate to those charged with governance and management.

...

## **Application and Other Explanatory Material**

### **Determination of Whether Deficiencies in Internal Control Have Been Identified**

(Ref: Para 7)

...

#### *Considerations Specific to Smaller Entities*

- A3. While the concepts underlying controls in the control activities component in smaller entities are likely to be similar to those in larger entities, the formality with which they operate will vary. Further, smaller entities may find that certain types of controls activities are not necessary because of controls applied by management. For example, management's sole authority for granting credit to customers and approving significant purchases can provide effective control over important account balances and transactions, lessening or removing the need for more detailed controls activities.

...

### **Significant Deficiencies in Internal Control** (Ref: Para. 6(b), 8)

- A8. Controls may be designed to operate individually or in combination to effectively prevent, or detect and correct, misstatements. For example, controls over accounts receivable may consist of both automated and manual controls designed to operate together to prevent, or detect and correct, misstatements in the account balance. A

---

<sup>86</sup> ISA 315 (Revised 2019), Identifying and Assessing the Risks of Material Misstatement, paragraphs 12(c) and (m), and paragraphs 21 to 27.

deficiency in internal control on its own may not be sufficiently important to constitute a significant deficiency. However, a combination of deficiencies affecting the same account balance or disclosure, ~~relevant~~ assertion, or component of the entity's system of internal control may increase the risks of misstatement to such an extent as to give rise to a significant deficiency.

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

### **Introduction**

#### **Scope of this ISA**

...

#### **Characteristics of Fraud**

...

#### **Responsibility for the Prevention and Detection of Fraud**

...

#### ***Responsibilities of the Auditor***

...

7. Furthermore, the risk of the auditor not detecting a material misstatement resulting from management fraud is greater than for employee fraud, because management is frequently in a position to directly or indirectly manipulate accounting records, present fraudulent financial information or override controls ~~procedures~~ designed to prevent similar frauds by other employees.

...

#### **Effective Date**

...

#### **Objectives**

...

#### **Definitions**

...

# Requirements

## Professional Skepticism

13. In accordance with ISA 200,<sup>87</sup> the auditor shall maintain professional skepticism throughout the audit, recognizing the possibility that a material misstatement due to fraud could exist, notwithstanding the auditor's past experience of the honesty and integrity of the entity's management and those charged with governance. (Ref: Para. A7–A8)
14. Unless the auditor has reason to believe the contrary, the auditor may accept records and documents as genuine. If conditions identified during the audit cause the auditor to believe that a document may not be authentic or that terms in a document have been modified but not disclosed to the auditor, the auditor shall investigate further. (Ref: Para. A9)
15. Where responses to inquiries of management or those charged with governance are inconsistent, the auditor shall investigate the inconsistencies.

## Discussion among the Engagement Team

16. ISA 315 (Revised 2019) requires a discussion among the engagement team members and a determination by the engagement partner of which matters are to be communicated to those team members not involved in the discussion.<sup>88</sup> This discussion shall place particular emphasis on how and where the entity's financial statements may be susceptible to material misstatement due to fraud, including how fraud might occur. The discussion shall occur setting aside beliefs that the engagement team members may have that management and those charged with governance are honest and have integrity. (Ref: Para. A10–A11)

## Risk Assessment Procedures and Related Activities

17. When performing risk assessment procedures and related activities to obtain an understanding of the entity and its environment, the applicable financial reporting framework and including the entity's system of internal control, required by ISA 315 (Revised 2019),<sup>89</sup> the auditor shall perform the procedures in paragraphs 2317–4324 to obtain information for use in identifying the risks of material misstatement due to fraud.

## *Management and Others within the Entity*

...

---

<sup>87</sup> ISA 200, paragraph 15

<sup>88</sup> ISA 315 (Revised 2019), paragraph 17–18~~40~~

<sup>89</sup> ~~ISA 315 (Revised), paragraphs 5–24~~

### ***Those Charged with Governance***

21. Unless all of those charged with governance are involved in managing the entity,<sup>90</sup> the auditor shall obtain an understanding of how those charged with governance exercise oversight of management's processes for identifying and responding to the risks of fraud in the entity and the ~~internal controls~~ that management has established to mitigate these risks. (Ref: Para. A19–A21)

...

### ***Unusual or Unexpected Relationships Identified***

...

### ***Other Information***

24. The auditor shall consider whether other information obtained by the auditor indicates risks of material misstatement due to fraud. (Ref: Para. A22)

### ***Evaluation of Fraud Risk Factors***

25. The auditor shall evaluate whether the information obtained from the other risk assessment procedures and related activities performed indicates that one or more fraud risk factors are present. While fraud risk factors may not necessarily indicate the existence of fraud, they have often been present in circumstances where frauds have occurred and therefore may indicate risks of material misstatement due to fraud. (Ref: Para. A23–A27)

### **Identification and Assessment of the Risks of Material Misstatement Due to Fraud**

26. In accordance with ISA 315 (Revised 2019), the auditor shall identify and assess the risks of material misstatement due to fraud at the financial statement level, and at the assertion level for classes of transactions, account balances and disclosures.<sup>91</sup>
27. When identifying and assessing the risks of material misstatement due to fraud, the auditor shall, based on a presumption that there are risks of fraud in revenue recognition, evaluate which types of revenue, revenue transactions or assertions give rise to such risks. Paragraph 47 specifies the documentation required where the auditor concludes that the presumption is not applicable in the circumstances of the engagement and, accordingly, has not identified revenue recognition as a risk of material misstatement due to fraud. (Ref: Para. A28–A30)
28. The auditor shall treat those assessed risks of material misstatement due to fraud as significant risks and accordingly, to the extent not already done so, the auditor shall ~~obtain an understanding of the entity's related~~ identify the entity's controls,

---

<sup>90</sup> ISA 260 (Revised), *Communication with Those Charged with Governance*, paragraph 13

<sup>91</sup> ISA 315 (Revised 2019), paragraph 282

~~including control activities, relevant to that address such risks, and evaluate their design and determine whether they have been implemented.~~<sup>92</sup> (Ref: Para. A31–A32)

## **Responses to the Assessed Risks of Material Misstatement Due to Fraud**

### *Overall Responses*

...

### ***Audit Procedures Responsive to Assessed Risks of Material Misstatement Due to Fraud at the Assertion Level***

...

### ***Audit Procedures Responsive to Risks Related to Management Override of Controls***

...

33. Irrespective of the auditor's assessment of the risks of management override of controls, the auditor shall design and perform audit procedures to:

- (a) Test the appropriateness of journal entries recorded in the general ledger and other adjustments made in the preparation of the financial statements. In designing and performing audit procedures for such tests, the auditor shall:
  - (i) Make inquiries of individuals involved in the financial reporting process about inappropriate or unusual activity relating to the processing of journal entries and other adjustments;
  - (ii) Select journal entries and other adjustments made at the end of a reporting period; and
  - (iii) Consider the need to test journal entries and other adjustments throughout the period. (Ref: Para. A41–A44)

...

## **Evaluation of Audit Evidence (Ref: Para. A49)**

...

## **Auditor Unable to Continue the Engagement**

...

## **Written Representations**

---

<sup>92</sup> ISA 315 (Revised 2019), paragraph 26(a)(i) and 26(d)

...

## Communications to Management and with Those Charged with Governance

...

## Communications to Regulatory and Enforcement Authorities

...

## Documentation

45. The auditor shall include the following in the audit documentation<sup>93</sup> ~~of the auditor's understanding of the entity and its environment and of the identification and the assessment of the risks of material misstatement required by ISA 315 (Revised 2019):~~<sup>94</sup>

- (a) The significant decisions reached during the discussion among the engagement team regarding the susceptibility of the entity's financial statements to material misstatement due to fraud; ~~and~~
- (b) The identified and assessed risks of material misstatement due to fraud at the financial statement level and at the assertion level; ~~and~~
- (c) Identified controls in the control activities component that address assessed risks of material misstatement due to fraud.

...

## Application and Other Explanatory Material

Characteristics of Fraud (Ref: Para. 3)

...

### *Professional Skepticism (Ref: Para. 12–14)*

A8. Maintaining professional skepticism requires an ongoing questioning of whether the information and audit evidence obtained suggests that a material misstatement due to fraud may exist. It includes considering the reliability of the information to be used as audit evidence and the identified controls in the control activities component, if any, over its preparation and maintenance, ~~where relevant.~~ Due to the characteristics of fraud, the auditor's professional skepticism is particularly important when considering the risks of material misstatement due to fraud.

...

---

<sup>93</sup> ISA 230, *Audit Documentation*, paragraphs 8–11, and paragraph A6

<sup>94</sup> ISA 315 (Revised 2019), paragraph 38~~32~~

*Discussion Among the Engagement Team (Ref: Para. 15)*

...

**Risk Assessment Procedures and Related Activities**

*Inquiries of Management*

Management's Assessment of the Risk of Material Misstatement Due to Fraud (Ref: Para. 17(a))

...

*Inquiry of Internal Audit (Ref: Para. 19)*

A19. ISA 315 (Revised 2019) and ISA 610 (Revised 2013) establish requirements and provide guidance relevant to audits of those entities that have an internal audit function.<sup>95</sup> In carrying out the requirements of those ISAs in the context of fraud, the auditor may inquire about specific activities of the function including, for example:

- The procedures performed, if any, by the internal auditor function during the year to detect fraud.
- Whether management has satisfactorily responded to any findings resulting from those procedures.

*Obtaining an Understanding of Oversight Exercised by Those Charged with Governance (Ref: Para. 20)*

A20. Those charged with governance of an entity oversee the entity's systems for monitoring risk, financial control and compliance with the law. In many countries, corporate governance practices are well developed and those charged with governance play an active role in oversight of the entity's assessment of the risks of fraud and of the relevant internal control the controls that address such risks. Since the responsibilities of those charged with governance and management may vary by entity and by country, it is important that the auditor understands their respective responsibilities to enable the auditor to obtain an understanding of the oversight exercised by the appropriate individuals.<sup>96</sup>

A21. An understanding of the oversight exercised by those charged with governance may provide insights regarding the susceptibility of the entity to management fraud, the adequacy of ~~internal controls~~ the controls that address ~~over~~ risks of fraud, and the competency

---

<sup>95</sup> ISA 315 (Revised 2019), paragraphs 14(a) and ~~24(a)(ii)6 and 23~~, and ISA 610 (Revised 2013), *Using the Work of Internal Auditors*

<sup>96</sup> ISA 260 (Revised), paragraphs A1–A8, discuss with whom the auditor communicates when the entity's governance structure is not well defined.

and integrity of management. The auditor may obtain this understanding in a number of ways, such as by attending meetings where such discussions take place, reading the minutes from such meetings or making inquiries of those charged with governance.

### Considerations Specific to Smaller Entities

...

#### *Consideration of Other Information* (Ref: Para. 23)

A23. In addition to information obtained from applying analytical procedures, other information obtained about the entity and its environment, the applicable financial reporting framework and the entity's system of internal control may be helpful in identifying the risks of material misstatement due to fraud. The discussion among team members may provide information that is helpful in identifying such risks. In addition, information obtained from the auditor's client acceptance and retention processes, and experience gained on other engagements performed for the entity, for example, engagements to review interim financial information, may be relevant in the identification of the risks of material misstatement due to fraud.

#### *Evaluation of Fraud Risk Factors* (Ref: Para. 24)

...

A26. Examples of fraud risk factors related to fraudulent financial reporting and misappropriation of assets are presented in Appendix 1. These illustrative risk factors are classified based on the three conditions that are generally present when fraud exists:

- An incentive or pressure to commit fraud;
- A perceived opportunity to commit fraud; and
- An ability to rationalize the fraudulent action.

Fraud risk factors may relate to incentives, pressures or opportunities that arise from conditions that create susceptibility to misstatement, before consideration of controls. Fraud risk factors, which include intentional management bias, are, insofar as they affect inherent risk, inherent risk factors.<sup>97</sup> Fraud risk factors may also relate to conditions within the entity's system of internal control that provide opportunity to commit fraud or that may affect management's attitude or ability to rationalize fraudulent actions. Fraud rRisk factors reflective of an attitude that permits rationalization of the fraudulent action may not be susceptible to observation by the auditor. Nevertheless, the auditor may become aware of the existence of such information through, for example, the required understanding of

---

<sup>97</sup> ISA 315 (Revised 2019), paragraph 12(f)

the entity's control environment.<sup>98</sup> Although the fraud risk factors described in Appendix 1 cover a broad range of situations that may be faced by auditors, they are only examples and other risk factors may exist.

...

## **Identification and Assessment of the Risks of Material Misstatement Due to Fraud**

*Risks of Fraud in Revenue Recognition* (Ref: Para. 26)

...

*Identifying and Assessing the Risks of Material Misstatement Due to Fraud and Understanding the Entity's Related Controls* (Ref: Para. 27)

A32. 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. In determining which controls to implement to prevent and detect fraud, management considers the risks that the financial statements may be materially misstated as a result of fraud. As part of this consideration, management may conclude that it is not cost effective to implement and maintain a particular control in relation to the reduction in the risks of material misstatement due to fraud to be achieved.

A33. It is therefore important for the auditor to obtain an understanding of the controls that management has designed, implemented and maintained to prevent and detect fraud. ~~In doing so, In identifying the controls that address the risks of material misstatement due to fraud,~~ the auditor may learn, for example, that management has consciously chosen to accept the risks associated with a lack of segregation of duties. Information from ~~obtaining this understanding identifying these controls, and evaluating their design and determining whether they have been implemented,~~ may also be useful in identifying fraud risks factors that may affect the auditor's assessment of the risks that the financial statements may contain material misstatement due to fraud.

## **Responses to the Assessed Risks of Material Misstatement Due to Fraud**

*Overall Responses* (Ref: Para. 28)

...

*Assignment and Supervision of Personnel* (Ref: Para. 29(a))

...

*Unpredictability in the Selection of Audit Procedures* (Ref: Para. 29(c))

---

<sup>98</sup> ISA 315 (Revised 2019), paragraph 21

...

*Audit Procedures Responsive to Assessed Risks of Material Misstatement Due to Fraud at the Assertion Level* (Ref: Para. 30)

...

Audit Procedures Responsive to Risks Related to Management Override of Controls

Journal Entries and Other Adjustments (Ref: Para. 32(a))

...

- A43. Further, the auditor's consideration of the risks of material misstatement associated with inappropriate override of controls over journal entries<sup>99</sup> is important since automated processes and controls may reduce the risk of inadvertent error but do not overcome the risk that individuals may inappropriately override such automated processes, for example, by changing the amounts being automatically passed to the general ledger or to the financial reporting system. Furthermore, where IT is used to transfer information automatically, there may be little or no visible evidence of such intervention in the information systems.
- A44. When identifying and selecting journal entries and other adjustments for testing and determining the appropriate method of examining the underlying support for the items selected, the following matters are of relevance:
- *The identification and assessment of the risks of material misstatement due to fraud* – the presence of fraud risk factors and other information obtained during the auditor's identification and assessment of the risks of material misstatement due to fraud may assist the auditor to identify specific classes of journal entries and other adjustments for testing.
  - *Controls that have been implemented over journal entries and other adjustments* – effective controls over the preparation and posting of journal entries and other adjustments may reduce the extent of substantive testing necessary, provided that the auditor has tested the operating effectiveness of the controls.
  - *The entity's financial reporting process and the nature of evidence that can be obtained* – for many entities routine processing of transactions involves a combination of manual and automated ~~steps and procedures~~ controls. Similarly, the processing of journal entries and other adjustments may involve both manual and automated ~~procedures and~~ controls. Where information technology is used in the financial reporting process, journal entries and other adjustments may exist only in electronic form.

---

<sup>99</sup> ISA 315 (Revised 2019), paragraph 26(a)(ii)

- *The characteristics of fraudulent journal entries or other adjustments* – inappropriate journal entries or other adjustments often have unique identifying characteristics. Such characteristics may include entries (a) made to unrelated, unusual, or seldom-used accounts, (b) made by individuals who typically do not make journal entries, (c) recorded at the end of the period or as post-closing entries that have little or no explanation or description, (d) made either before or during the preparation of the financial statements that do not have account numbers, or (e) containing round numbers or consistent ending numbers.
- *The nature and complexity of the accounts* – inappropriate journal entries or adjustments may be applied to accounts that (a) contain transactions that are complex or unusual in nature, (b) contain significant estimates and period-end adjustments, (c) have been prone to misstatements in the past, (d) have not been reconciled on a timely basis or contain unreconciled differences, (e) contain inter-company transactions, or (f) are otherwise associated with an identified risk of material misstatement due to fraud. In audits of entities that have several locations or components, consideration is given to the need to select journal entries from multiple locations.
- *Journal entries or other adjustments processed outside the normal course of business* – non standard journal entries may not be subject to the same level of internal nature and extent of controls as those journal entries used on a recurring basis to record transactions such as monthly sales, purchases and cash disbursements.

...

Accounting Estimates (Ref: Para. 32(b))

...

Business Rationale for Significant Transactions (Ref: Para. 32(c))

...

**Evaluation of Audit Evidence** (Ref: Para. 34–37)

...

*Analytical Procedures Performed Near the End of the Audit in Forming an Overall Conclusion* (Ref: Para. 34)

...

*Consideration of Identified Misstatements* (Ref: Para. 35–37)

...

**Auditor Unable to Continue the Engagement** (Ref: Para. 38)

...

**Written Representations** (Ref: Para. 39)

...

**Communications to Management and with Those Charged with Governance**

*Communication to Management* (Ref: Para. 40)

...

*Communication with Those Charged with Governance* (Ref: Para. 41)

...

*Other Matters Related to Fraud* (Ref: Para. 42)

...

**Communications to Regulatory and Enforcement Authorities** (Ref: Para. 43)

...

**Appendix 1**

(Ref: Para. A25)

**Examples of Fraud Risk Factors**

The fraud risk factors identified in this Appendix are examples of such factors that may be faced by auditors in a broad range of situations. Separately presented are examples relating to the two types of fraud relevant to the auditor's consideration – that is, fraudulent financial reporting and misappropriation of assets. For each of these types of fraud, the risk factors are further classified based on the three conditions generally present when material misstatements due to fraud occur: (a) incentives/pressures, (b) opportunities, and (c) attitudes/rationalizations. Although the risk factors cover a broad range of situations, they are only examples and, accordingly, the auditor may identify additional or different risk factors. Not all of these examples are relevant in all circumstances, and some may be of greater or lesser significance in entities of different size or with different ownership characteristics or circumstances. Also, the order of the examples of risk factors provided is not intended to reflect their relative importance or frequency of occurrence.

Fraud risk factors may relate to incentives or pressures, or opportunities, that arise from conditions that create susceptibility to misstatement before consideration of controls (i.e., the inherent risk). Such factors are inherent risk factors, insofar as they affect inherent risk, and may be due to management bias. Fraud risk factors related to opportunities may also arise from other identified inherent risk factors (for example, complexity or uncertainty may create opportunities that result in susceptibility to misstatement due to fraud). Fraud risk factors related to opportunities may also relate to conditions within the entity's system

of internal control, such as limitations or deficiencies in the entity's internal control that create such opportunities. Fraud risk factors related to attitudes or rationalizations may arise, in particular, from limitations or deficiencies in the entity's control environment.

### **Risk Factors Relating to Misstatements Arising from Fraudulent Financial Reporting**

The following are examples of risk factors relating to misstatements arising from fraudulent financial reporting.

#### *Incentives/Pressures*

Financial stability or profitability is threatened by economic, industry, or entity operating conditions, such as (or as indicated by):

...

Excessive pressure exists for management to meet the requirements or expectations of third parties due to the following:

...

Information available indicates that the personal financial situation of management or those charged with governance is threatened by the entity's financial performance arising from the following:

...

#### *Opportunities*

The nature of the industry or the entity's operations provides opportunities to engage in fraudulent financial reporting that can arise from the following:

...

The monitoring of management is not effective as a result of the following:

...

There is a complex or unstable organizational structure, as evidenced by the following:

...

~~Internal control components are deficient~~ Deficiencies in internal control as a result of the following:

- ~~Inadequate monitoring of controls process to monitor the entity's system of internal control,~~ including automated controls and controls over interim financial reporting

(where external reporting is required).

- High turnover rates or employment of staff in accounting, information technology, or the internal audit function that are not effective.
- Accounting and information systems that are not effective, including situations involving significant deficiencies in internal control.

#### *Attitudes/Rationalizations*

...

### **Risk Factors Arising from Misstatements Arising from Misappropriation of Assets**

Risk factors that relate to misstatements arising from misappropriation of assets are also classified according to the three conditions generally present when fraud exists: incentives/pressures, opportunities, and attitudes/rationalization. Some of the risk factors related to misstatements arising from fraudulent financial reporting also may be present when misstatements arising from misappropriation of assets occur. For example, ineffective monitoring of management and other deficiencies in internal control may be present when misstatements due to either fraudulent financial reporting or misappropriation of assets exist. The following are examples of risk factors related to misstatements arising from misappropriation of assets.

#### *Incentives/Pressures*

...

#### *Opportunities*

Certain characteristics or circumstances may increase the susceptibility of assets to misappropriation. For example, opportunities to misappropriate assets increase when there are the following:

...

Inadequate internal controls over assets may increase the susceptibility of misappropriation of those assets. For example, misappropriation of assets may occur because there is the following:

- Inadequate segregation of duties or independent checks.
- Inadequate oversight of senior management expenditures, such as travel and other re-imbursements.
- Inadequate management oversight of employees responsible for assets, for example, inadequate supervision or monitoring of remote locations.
- Inadequate job applicant screening of employees with access to assets.

- Inadequate record keeping with respect to assets.
- Inadequate system of authorization and approval of transactions (for example, in purchasing).
- Inadequate physical safeguards over cash, investments, inventory, or fixed assets.
- Lack of complete and timely reconciliations of assets.
- Lack of timely and appropriate documentation of transactions, for example, credits for merchandise returns.
- Lack of mandatory vacations for employees performing key control functions.
- Inadequate management understanding of information technology, which enables information technology employees to perpetrate a misappropriation.
- Inadequate access controls over automated records, including controls over and review of computer systems event logs.

#### *Attitudes/Rationalizations*

- Disregard for the need for monitoring or reducing risks related to misappropriations of assets.
- Disregard for ~~internal controls~~ over misappropriation of assets by overriding existing controls or by failing to take appropriate remedial action on known deficiencies in internal control.
- Behavior indicating displeasure or dissatisfaction with the entity or its treatment of the employee.
- Changes in behavior or lifestyle that may indicate assets have been misappropriated.
- Tolerance of petty theft.

## **Appendix 2**

(Ref: Para. A40)

### **Examples of Possible Audit Procedures to Address the Assessed Risks of Material Misstatement Due to Fraud**

The following are examples of possible audit procedures to address the assessed risks of material misstatement due to fraud resulting from both fraudulent financial reporting and misappropriation of assets. Although these procedures cover a broad range of situations, they are only examples and, accordingly they may not be the most appropriate nor necessary in each circumstance. Also the order of the procedures provided is not intended to reflect their relative importance.

#### **Consideration at the Assertion Level**

Specific responses to the auditor's assessment of the risks of material misstatement due to fraud will vary depending upon the types or combinations of fraud risk factors or conditions identified, and the classes of transactions, account balances, disclosures and assertions they may affect.

The following are specific examples of responses:

...

- If the work of an expert becomes particularly significant with respect to a financial statement item for which the assessed risk of **material** misstatement due to fraud is high, performing additional procedures relating to some or all of the expert's assumptions, methods or findings to determine that the findings are not unreasonable, or engaging another expert for that purpose.

...

### **Specific Responses—Misstatement Resulting from Fraudulent Financial Reporting**

Examples of responses to the auditor's assessment of the risks of material misstatement due to fraudulent financial reporting are as follows:

...

## **Appendix 3**

(Ref: Para. A49)

### **Examples of Circumstances that Indicate the Possibility of Fraud**

The following are examples of circumstances that may indicate the possibility that the financial statements may contain a material misstatement resulting from fraud.

...

### **ISA 300, *Planning an Audit of Financial Statements***

#### **Application and Other Explanatory Material**

...

#### **Documentation (Ref: Para. 12)**

...

#### *Considerations Specific to Smaller Entities*

A21. As discussed in paragraph A11, a suitable, brief memorandum may serve as the

documented strategy for the audit of a smaller entity. For the audit plan, standard audit programs or checklists (see paragraph A19) drawn up on the assumption of few ~~relevant~~ controls<sup>100</sup> ~~activities~~, as is likely to be the case in a smaller entity, may be used provided that they are tailored to the circumstances of the engagement, including the auditor's risk assessments.

...

## **ISA 402, *Audit Considerations Relating to an Entity Using a Service Organization***

### **Introduction**

#### **Scope of this ISA**

1. This International Standard on Auditing (ISA) deals with the user auditor's responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations. Specifically, it expands on how the user auditor applies ISA 315 (Revised 2019)<sup>101</sup> and ISA 330<sup>102</sup> in obtaining an understanding of the user entity, including the entity's system of internal control relevant to the preparation of the financial statements relevant to the audit, sufficient to identify and assess the risks of material misstatement and in designing and performing further audit procedures responsive to those risks.

...

3. Services provided by a service organization are relevant to the audit of a user entity's financial statements when those services, and the controls over them, are part of the user entity's information system, ~~including related business processes, relevant to financial reporting the preparation of the financial statements. Although~~ Most controls at the service organization are likely to relate to financial reporting be part of the user entity's information system relevant to the preparation of the financial statements, there may be other or related controls that may also be relevant to the audit, such as controls over the safeguarding of assets. A service organization's services are part of a user entity's information system, ~~including related business processes, relevant to financial reporting~~ if these services affect any of the following:
  - (a) How information relating to significant classes of transactions, account balances and disclosures flows through the user entity's information system, whether manually or using IT, and whether obtained from within or outside the general ledger and subsidiary ledgers. The classes of transactions in the user entity's operations that are significant to the user entity's financial

---

<sup>100</sup> ISA 315 (Revised 2019), paragraph 26(a)

<sup>101</sup> ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement*

<sup>102</sup> ISA 330, *The Auditor's Responses to Assessed Risks*

statements; This includes when the service organization's services affect how:

- (i) ~~(b) The procedures, within both information technology (IT) and manual systems, by which the user entity's transactions are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in the financial statements; Transactions of the user entity are initiated, and how information about them is recorded, processed, corrected as necessary, and incorporated in the general ledger and reported in the financial statements; and~~
- (ii) Information about events or conditions, other than transactions, is captured, processed and disclosed by the user entity in the financial statements.
- (b) ~~(e) The related accounting records, either in electronic or manual form, supporting information and specific accounts in the user entity's financial statements and other supporting records relating to the flows of information in paragraph 3(a) that are used to initiate, record, process and report the user entity's transactions; this includes the correction of incorrect information and how information is transferred to the general ledger;~~
- (d) ~~How the user entity's information system captures events and conditions, other than transactions, that are significant to the financial statements;~~
- (ce) ~~The financial reporting process used to prepare the user entity's financial statements from the records described in paragraph 3(b), including as it relates to disclosures and to accounting estimates relating to significant classes of transactions, account balances and disclosures accounting estimates and disclosures; and~~
- (d) The entity's IT environment relevant to (a) to (c) above.
- (f) ~~Controls surrounding journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments.~~

...

## Objectives

7. The objectives of the user auditor, when the user entity uses the services of a service organization, are:
  - (a) To obtain an understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's system of internal control relevant to the audit, sufficient to provide an appropriate basis for the identification and assessment of ~~identify and assess~~ the risks of material misstatement; and
  - (b) To design and perform audit procedures responsive to those risks.

...

## Requirements

### Obtaining an Understanding of the Services Provided by a Service Organization, Including Internal Control

...

10. When obtaining an understanding of ~~the entity's system of~~ internal control ~~relevant to the audit~~ in accordance with ISA 315 (Revised 2019),<sup>103</sup> the user auditor shall identify controls in the control activities component<sup>104</sup> ~~evaluate the design and implementation of relevant controls at the user entity, from those that relate to the services provided by the service organization, including those that are applied to the transactions processed by the service organization, and evaluate their design and determine whether they have been implemented.~~<sup>105</sup> (Ref: Para. A12–A14)
11. The user auditor shall determine whether a sufficient understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's ~~system of~~ internal control ~~relevant to the audit~~ has been obtained to provide a appropriate basis for the identification and assessment of the risks of material misstatement.
12. If the user auditor is unable to obtain a sufficient understanding from the user entity, the user auditor shall obtain that understanding from one or more of the following procedures:
  - ...
  - (c) Visiting the service organization and performing procedures that will provide the necessary information about the relevant controls at the service organization; or
  - (d) Using another auditor to perform procedures that will provide the necessary information about ~~the relevant~~ controls at the service organization. (Ref: Para. A15–A20)

### *Using a Type 1 or Type 2 Report to Support the User Auditor's Understanding of the Service Organization*

...

14. If the user auditor plans to use a type 1 or type 2 report as audit evidence to support the user auditor's understanding about the design and implementation of controls at the service organization, the user auditor shall:

---

<sup>103</sup> ISA 315 (Revised), paragraph 12

<sup>104</sup> ISA 315 (Revised 2019), paragraphs 26(a)

<sup>105</sup> ISA 315 (Revised 2019), paragraph 26(d)

...

- (b) Evaluate the sufficiency and appropriateness of the evidence provided by the report for the understanding of the ~~user entity's internal controls at the service organization relevant to the audit~~; and

...

## Application and Other Explanatory Material

### Obtaining an Understanding of the Services Provided by a Service Organization, Including Internal Control

...

*Further Procedures When a Sufficient Understanding Cannot Be Obtained from the User Entity* (Ref: Para. 12)

...

A19. Another auditor may be used to perform procedures that will provide the necessary information about the relevant—controls at the service organization related to services provided to the user entity. If a type 1 or type 2 report has been issued, the user auditor may use the service auditor to perform these procedures as the service auditor has an existing relationship with the service organization. The user auditor using the work of another auditor may find the guidance in ISA 600<sup>106</sup> useful as it relates to understanding another auditor (including that auditor's independence and professional competence), involvement in the work of another auditor in planning the nature, timing and extent of such work, and in evaluating the sufficiency and appropriateness of the audit evidence obtained.

...

*Using a Type 1 or Type 2 Report to Support the User Auditor's Understanding of the Service Organization* (Ref: Para. 13–14)

...

A22. A type 1 or type 2 report, along with information about the user entity, may assist the user auditor in obtaining an understanding of:

- (a) The aspects of controls at the service organization that may affect the processing of the user entity's transactions, including the use of subservice organizations;

---

<sup>106</sup> ISA 600, *Special Considerations—Audits of Group Financial Statements (Including the Work of Component Auditors)*, paragraph 2, states: "An auditor may find this ISA, adapted as necessary in the circumstances, useful when that auditor involves other auditors in the audit of financial statements that are not group financial statements ..." See also paragraph 19 of ISA 600.

- (b) The flow of significant transactions through the service organization to determine the points in the transaction flow where material misstatements in the user entity's financial statements could occur;
- (c) The control objectives at the service organization that are relevant to the user entity's financial statement assertions; and
- (d) Whether controls at the service organization are suitably designed and implemented to prevent, or detect and correct processing errors that could result in material misstatements in the user entity's financial statements.

A type 1 or type 2 report may assist the user auditor in obtaining a sufficient understanding to identify and assess the risks of material misstatement. A type 1 report, however, does not provide any evidence of the operating effectiveness of the ~~relevant~~ controls.

### **Responding to the Assessed Risks of Material Misstatement**

...

#### *Test of Controls*

A29. The user auditor is required by ISA 330 to design and perform tests of controls to obtain sufficient appropriate audit evidence as to the operating effectiveness of ~~relevant~~ controls in certain circumstances. In the context of a service organization, this requirement applies when:

...

A30. If a type 2 report is not available, a user auditor may contact the service organization, through the user entity, to request that a service auditor be engaged to provide a type 2 report that includes tests of the operating effectiveness of the ~~relevant~~ controls or the user auditor may use another auditor to perform procedures at the service organization that test the operating effectiveness of those controls. A user auditor may also visit the service organization and perform tests of ~~relevant~~ controls if the service organization agrees to it. The user auditor's risk assessments are based on the combined evidence provided by the work of another auditor and the user auditor's own procedures.

Using a Type 2 Report as Audit Evidence that Controls at the Service Organization Are Operating Effectively

...

A33. It may also be necessary for the user auditor to obtain additional evidence about significant changes to the ~~relevant~~ controls at the service organization outside of the period covered by the type 2 report or determine additional audit procedures to be performed. Relevant factors in determining what additional audit evidence to obtain about controls at the service organization that were operating outside of the period covered by the service auditor's report may include:

...

- The effectiveness of the control environment and the user entity's process to monitor the system of internal control ~~monitoring of controls at the user entity.~~

A34. Additional audit evidence may be obtained, for example, by extending tests of controls over the remaining period or testing the user entity's process to monitor the system of internal control ~~monitoring of controls.~~

...

A39. The user auditor is required to communicate in writing significant deficiencies identified during the audit to both management and those charged with governance on a timely basis.<sup>11</sup> The user auditor is also required to communicate to management at an appropriate level of responsibility on a timely basis other deficiencies in internal control identified during the audit that, in the user auditor's professional judgment, are of sufficient importance to merit management's attention.<sup>12</sup> Matters that the user auditor may identify during the audit and may communicate to management and those charged with governance of the user entity include:

- Any controls within the entity's process to monitor the system of internal control ~~monitoring of controls~~ that could be implemented by the user entity, including those identified as a result of obtaining a type 1 or type 2 report;

...

## **ISA 330, *The Auditor's Responses to Assessed Risks***

### **Introduction**

#### **Scope of this ISA**

1. This International Standard on Auditing (ISA) deals with the auditor's responsibility to design and implement responses to the risks of material misstatement identified and assessed by the auditor in accordance with ISA 315 (Revised 2019)<sup>107</sup> in an audit of financial statements.

#### **Effective Date**

2. This ISA is effective for audits of financial statements for periods beginning on or after December 15, 2009.

---

<sup>107</sup> ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment*

## Objective

3. The objective of the auditor is to obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatement, through designing and implementing appropriate responses to those risks.

## Definitions

4. For purposes of the ISAs, the following terms have the meanings attributed below:
  - (a) Substantive procedure – An audit procedure designed to detect material misstatements at the assertion level. Substantive procedures comprise:
    - (i) Tests of details (of classes of transactions, account balances, and disclosures); and
    - (ii) Substantive analytical procedures.
  - (b) Test of controls – An audit procedure designed to evaluate the operating effectiveness of controls in preventing, or detecting and correcting, material misstatements at the assertion level.

## Requirements

### Overall Responses

5. The auditor shall design and implement overall responses to address the assessed risks of material misstatement at the financial statement level. (Ref: Para. A1–A3)

### Audit Procedures Responsive to the Assessed Risks of Material Misstatement at the Assertion Level

6. The auditor shall 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. (Ref: Para. A4–A8; A42-A52)
7. In designing the further audit procedures to be performed, the auditor shall:
  - (a) Consider the reasons for the assessment given to the risk of material misstatement at the assertion level for each significant class of transactions, account balance, and disclosure, including:
    - (i) The likelihood and magnitude of ~~material~~ misstatement due to the particular characteristics of the ~~relevant~~ significant class of transactions, account balance, or disclosure (that is, the inherent risk); and

- (ii) Whether the risk assessment takes account of ~~relevant controls that address the risk of material misstatement~~ (that is, the control risk), thereby requiring the auditor to obtain audit evidence to determine whether the controls are operating effectively (that is, the auditor ~~intends to rely on plans to test~~ the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures); and (Ref: Para. A9–A18)
- (b) Obtain more persuasive audit evidence the higher the auditor’s assessment of risk. (Ref: Para. A19)

### *Tests of Controls*

- 8. The auditor shall design and perform tests of controls to obtain sufficient appropriate audit evidence as to the operating effectiveness of ~~relevant~~ controls if:
  - (a) The auditor’s assessment of risks of material misstatement at the assertion level includes an expectation that the controls are operating effectively (that is, the auditor ~~intends plans to test to rely on~~ the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures); or
  - (b) Substantive procedures alone cannot provide sufficient appropriate audit evidence at the assertion level. (Ref: Para. A20–A24)
- 9. In designing and performing tests of controls, the auditor shall obtain more persuasive audit evidence the greater the reliance the auditor places on the effectiveness of a control. (Ref: Para. A25)

### *Nature and Extent of Tests of Controls*

- 10. In designing and performing tests of controls, the auditor shall:
  - (a) Perform other audit procedures in combination with inquiry to obtain audit evidence about the operating effectiveness of the controls, including:
    - (i) How the controls were applied at relevant times during the period under audit;
    - (ii) The consistency with which they were applied; and
    - (iii) By whom or by what means they were applied. (Ref: Para. A26–A29~~a~~)
  - (b) ~~To the extent not already addressed, d~~Determine whether the controls to be tested depend upon other controls (indirect controls), and, if so, whether it is necessary to obtain audit evidence supporting the effective operation of those indirect controls. (Ref: Para. A30–A31)

## Timing of Tests of Controls

11. The auditor shall test controls for the particular time, or throughout the period, for which the auditor intends to rely on those controls, subject to paragraphs 12 and 15 below, in order to provide an appropriate basis for the auditor's intended reliance. (Ref: Para. A32)

### Using audit evidence obtained during an interim period

12. If the auditor obtains audit evidence about the operating effectiveness of controls during an interim period, the auditor shall:
  - (a) Obtain audit evidence about significant changes to those controls subsequent to the interim period; and
  - (b) Determine the additional audit evidence to be obtained for the remaining period. (Ref: Para. A33–A34)

### Using audit evidence obtained in previous audits

13. In determining whether it is appropriate to use audit evidence about the operating effectiveness of controls obtained in previous audits, and, if so, the length of the time period that may elapse before retesting a control, the auditor shall consider the following:
  - (a) The effectiveness of other ~~elements~~ components of the entity's system of internal control, including the control environment, the entity's process to monitoring of the system of internal controls, and the entity's risk assessment process;
  - (b) The risks arising from the characteristics of the control, including whether it is manual or automated;
  - (c) The effectiveness of general IT controls;
  - (d) The effectiveness of the control and its application by the entity, including the nature and extent of deviations in the application of the control noted in previous audits, and whether there have been personnel changes that significantly affect the application of the control;
  - (e) Whether the lack of a change in a particular control poses a risk due to changing circumstances; and
  - (f) The risks of material misstatement and the extent of reliance on the control. (Ref: Para. A35)
14. If the auditor plans to use audit evidence from a previous audit about the operating effectiveness of specific controls, the auditor shall establish the continuing relevance and reliability of that evidence by obtaining audit evidence about whether significant changes in those controls have occurred subsequent to the previous audit. The auditor shall obtain this evidence by performing inquiry combined with

observation or inspection, to confirm the understanding of those specific controls, and:

- (a) If there have been changes that affect the continuing relevance of the audit evidence from the previous audit, the auditor shall test the controls in the current audit. (Ref: Para. A36)
- (b) If there have not been such changes, the auditor shall test the controls at least once in every third audit, and shall test some controls each audit to avoid the possibility of testing all the controls on which the auditor intends to rely in a single audit period with no testing of controls in the subsequent two audit periods. (Ref: Para. A37–A39)

#### Controls over significant risks

15. If the auditor ~~plans~~intends to rely ~~test~~ on controls over a risk the auditor has determined to be a significant risk, the auditor shall test those controls in the current period.

#### Evaluating the Operating Effectiveness of Controls

16. When evaluating the operating effectiveness of ~~relevant~~ controls upon which the auditor intends to rely, the auditor shall evaluate whether misstatements that have been detected by substantive procedures indicate that controls are not operating effectively. The absence of misstatements detected by substantive procedures, however, does not provide audit evidence that controls related to the assertion being tested are effective. (Ref: Para. A40)
17. If deviations from controls upon which the auditor intends to rely are detected, the auditor shall make specific inquiries to understand these matters and their potential consequences, and shall determine whether: (Ref: Para. A41)
  - (a) The tests of controls that have been performed provide an appropriate basis for reliance on the controls;
  - (b) Additional tests of controls are necessary; or
  - (c) The ~~potential~~ risks of material misstatement need to be addressed using substantive procedures.

#### *Substantive Procedures*

18. Irrespective of the assessed risks of material misstatement, the auditor shall design and perform substantive procedures for each material class of transactions, account balance, and disclosure. (Ref: Para. A42–A47)
19. The auditor shall consider whether external confirmation procedures are to be performed as substantive audit procedures. (Ref: Para. A48–A51)

## Substantive Procedures Related to the Financial Statement Closing Process

20. The auditor's substantive procedures shall include the following audit procedures related to the financial statement closing process:
  - (a) Agreeing or reconciling information in the financial statements with the underlying accounting records, including agreeing or reconciling information in disclosures, whether such information is obtained from within or outside of the general and subsidiary ledgers; and
  - (b) Examining material journal entries and other adjustments made during the course of preparing the financial statements. (Ref: Para. A52)

## Substantive Procedures Responsive to Significant Risks

21. If the auditor has determined that an assessed risk of material misstatement at the assertion level is a significant risk, the auditor shall perform substantive procedures that are specifically responsive to that risk. When the approach to a significant risk consists only of substantive procedures, those procedures shall include tests of details. (Ref: Para. A53)

## Timing of Substantive Procedures

22. If substantive procedures are performed at an interim date, the auditor shall cover the remaining period by performing:
  - (a) substantive procedures, combined with tests of controls for the intervening period; or
  - (b) if the auditor determines that it is sufficient, further substantive procedures only,that provide a reasonable basis for extending the audit conclusions from the interim date to the period end. (Ref: Para. A54–A57)
23. If misstatements that the auditor did not expect when assessing the risks of material misstatement are detected at an interim date, the auditor shall evaluate whether the related assessment of risk and the planned nature, timing or extent of substantive procedures covering the remaining period need to be modified. (Ref: Para. A58)

## Adequacy of Presentation of the Financial Statements

24. The auditor shall perform audit procedures to evaluate whether the overall presentation of the financial statements is in accordance with the applicable financial reporting framework. In making this evaluation, the auditor shall consider whether the financial statements are presented in a manner that reflects the appropriate:
  - Classification and description of financial information and the underlying transactions, events and conditions; and

- Presentation, structure and content of the financial statements. (Ref: Para. A59)

### **Evaluating the Sufficiency and Appropriateness of Audit Evidence**

25. Based on the audit procedures performed and the audit evidence obtained, the auditor shall evaluate before the conclusion of the audit whether the assessments of the risks of material misstatement at the assertion level remain appropriate. (Ref: Para. A60–A61)
26. The auditor shall conclude whether sufficient appropriate audit evidence has been obtained. In forming an opinion, the auditor shall consider all relevant audit evidence, regardless of whether it appears to corroborate or to contradict the assertions in the financial statements. (Ref: Para. A62)
27. If the auditor has not obtained sufficient appropriate audit evidence ~~as to related to a material financial statement~~ relevant assertion about a class of transactions, account balance or disclosure, the auditor shall attempt to obtain further audit evidence. If the auditor is unable to obtain sufficient appropriate audit evidence, the auditor shall express a qualified opinion or disclaim an opinion on the financial statements.

### **Documentation**

28. The auditor shall include in the audit documentation:<sup>108</sup>
  - (a) The overall responses to address the assessed risks of material misstatement at the financial statement level, and the nature, timing and extent of the further audit procedures performed;
  - (b) The linkage of those procedures with the assessed risks at the assertion level; and
  - (c) The results of the audit procedures, including the conclusions where these are not otherwise clear. (Ref: Para. A63)
29. If the auditor plans to use audit evidence about the operating effectiveness of controls obtained in previous audits, the auditor shall include in the audit documentation the conclusions reached about relying on such controls that were tested in a previous audit.
30. The auditor's documentation shall demonstrate that information in the financial statements agrees or reconciles with the underlying accounting records, including agreeing or reconciling disclosures, whether such information is obtained from within or outside of the general and subsidiary ledgers.

---

<sup>108</sup> ISA 230, *Audit Documentation*, paragraphs 8–11, and A6

# Application and Other Explanatory Material

## Overall Responses (Ref: Para.5)

A1. Overall responses to address the assessed risks of material misstatement at the financial statement level may include:

- Emphasizing to the engagement team the need to maintain professional skepticism.
- Assigning more experienced staff or those with special skills or using experts.
- ~~Providing more supervision~~ Changes to the nature, timing and extent of direction and supervision of members of the engagement team and the review of the work performed.
- Incorporating additional elements of unpredictability in the selection of further audit procedures to be performed.
- ~~Changes to the overall audit strategy as required by ISA 300, or planned audit procedures, and may include changes to:~~
  - ~~The auditor's determination of performance materiality in accordance with ISA 320.~~
  - ~~The auditor's plans to test, the operating effectiveness of controls, and the persuasiveness of audit evidence needed to support the planned reliance on the operating effectiveness of the controls, particularly when deficiencies in the control environment or the entity's monitoring activities are identified.~~
  - ~~The nature, timing and extent of substantive procedures. For example, it may be appropriate to perform substantive procedures at or near the date of the financial statements when the risk of material misstatement is assessed as higher.~~
- ~~Making general changes to the nature, timing or extent of audit procedures, for example: performing substantive procedures at the period end instead of at an interim date; or modifying the nature of audit procedures to obtain more persuasive audit evidence.~~

A2. The assessment of the risks of material misstatement at the financial statement level, and thereby the auditor's overall responses, is affected by the auditor's understanding of the control environment. An effective control environment may allow the auditor to have more confidence in internal control and the reliability of audit evidence generated internally within the entity and thus, for example, allow the auditor to conduct some audit procedures at an interim date rather than at the period end. Deficiencies in the control environment, however, have the opposite effect; for example, the auditor may respond to an ineffective control environment by:

- Conducting more audit procedures as of the period end rather than at an interim date.

- Obtaining more extensive audit evidence from substantive procedures.
- Increasing the number of locations to be included in the audit scope.

A3. Such considerations, therefore, have a significant bearing on the auditor's general approach, for example, an emphasis on substantive procedures (substantive approach), or an approach that uses tests of controls as well as substantive procedures (combined approach).

### **Audit Procedures Responsive to the Assessed Risks of Material Misstatement at the Assertion Level**

*The Nature, Timing and Extent of Further Audit Procedures (Ref: Para. 6)*

A4. The auditor's assessment of the identified risks of material misstatement at the assertion level provides a basis for considering the appropriate audit approach for designing and performing further audit procedures. For example, the auditor may determine that:

- Only by performing tests of controls may the auditor achieve an effective response to the assessed risk of material misstatement for a particular assertion;
- Performing only substantive procedures is appropriate for particular assertions and, therefore, the auditor excludes the effect of controls from the ~~relevant risk~~ assessment of the risk of material misstatement. This may be because the ~~auditor's risk assessment procedures have not identified any effective controls relevant to the assertion, or because auditor has not identified a risk for which~~ substantive procedures alone cannot provide sufficient appropriate audit evidence and therefore is not required to test the operating effectiveness of controls, testing controls would be inefficient and therefore, the auditor does not intend to rely on plan to test the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures; or
- A combined approach using both tests of controls and substantive procedures is an effective approach.

The auditor need not design and perform further audit procedures where the assessment of the risk of material misstatement is below the acceptably low level. However, as required by paragraph 18, irrespective of the approach selected and the assessed risk of material misstatement, the auditor designs and performs substantive procedures for each material class of transactions, account balance, and disclosure.

A5. The nature of an audit procedure refers to its purpose (that is, test of controls or substantive procedure) and its type (that is, inspection, observation, inquiry, confirmation, recalculation, reperformance, or analytical procedure). The nature of the audit procedures is of most importance in responding to the assessed risks.

A6. Timing of an audit procedure refers to when it is performed, or the period or date to which the audit evidence applies.

- A7. Extent of an audit procedure refers to the quantity to be performed, for example, a sample size or the number of observations of a control ~~activity~~.
- A8. Designing and performing 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 provides a clear linkage between the auditor's further audit procedures and the risk assessment.

#### Responding to the Assessed Risks at the Assertion Level (Ref: Para. 7(a))

##### Nature

- A9. ISA 315 (Revised 2019) requires that the auditor's assessment of the risks of material misstatement at the assertion level is performed by assessing inherent risk and control risk. The auditor assesses inherent risk by assessing the likelihood and magnitude of a misstatement taking into account how, and the degree to which the inherent risk factors affect the susceptibility to misstatement of relevant assertions.<sup>109</sup> The auditor's assessed risks, including the reasons for those assessed risks, may affect both the types of audit procedures to be performed and their combination. For example, when an assessed risk is high, the auditor may confirm the completeness of the terms of a contract with the counterparty, in addition to inspecting the document. Further, certain audit procedures may be more appropriate for some assertions than others. For example, in relation to revenue, tests of controls may be most responsive to the assessed risk of material misstatement of the completeness assertion, whereas substantive procedures may be most responsive to the assessed risk of material misstatement of the occurrence assertion.
- A10. The reasons for the assessment given to a risk are relevant in determining the nature of audit procedures. For example, if an assessed risk is lower because of the particular characteristics of a class of transactions without consideration of the related controls, then the auditor may determine that substantive analytical procedures alone provide sufficient appropriate audit evidence. On the other hand, if the assessed risk is lower because ~~of internal~~ the auditor plans to test the operating effectiveness of controls, and the auditor intends to base the substantive procedures on that low assessment, then the auditor performs tests of those controls, as required by paragraph 8(a). This may be the case, for example, for a class of transactions of reasonably uniform, non-complex characteristics that are routinely processed and controlled by the entity's information system.

##### Timing

- A11. The auditor may perform tests of controls or substantive procedures at an interim date or at the period end. The higher the risk of material misstatement, the more likely it is that the auditor may decide it is more effective to perform substantive procedures nearer to, or at, the period end rather than at an earlier date, or to perform

---

<sup>109</sup> ISA 315 (Revised 2019), paragraphs 31 and 34

audit procedures unannounced or at unpredictable times (for example, performing audit procedures at selected locations on an unannounced basis). This is particularly relevant when considering the response to the risks of fraud. For example, the auditor may conclude that, when the risks of intentional misstatement or manipulation have been identified, audit procedures to extend audit conclusions from interim date to the period end would not be effective.

A12. On the other hand, performing audit procedures before the period end may assist the auditor in identifying significant matters at an early stage of the audit, and consequently resolving them with the assistance of management or developing an effective audit approach to address such matters.

A13. In addition, certain audit procedures can be performed only at or after the period end, for example:

- Agreeing or reconciling information in the financial statements with the underlying accounting records, including agreeing or reconciling disclosures, whether such information is obtained from within or outside of the general and subsidiary ledgers;
- Examining adjustments made during the course of preparing the financial statements; and
- Procedures to respond to a risk that, at the period end, the entity may have entered into improper sales contracts, or transactions may not have been finalized.

A14. Further relevant factors that influence the auditor's consideration of when to perform audit procedures include the following:

- The control environment.
- When relevant information is available (for example, electronic files may subsequently be overwritten, or procedures to be observed may occur only at certain times).
- The nature of the risk (for example, if there is a risk of inflated revenues to meet earnings expectations by subsequent creation of false sales agreements, the auditor may wish to examine contracts available on the date of the period end).
- The period or date to which the audit evidence relates.
- The timing of the preparation of the financial statements, particularly for those disclosures that provide further explanation about amounts recorded in the statement of financial position, the statement of comprehensive income, the statement of changes in equity or the statement of cash flows.

Extent

A15. The extent of an audit procedure judged necessary is determined after considering

the materiality, the assessed risk, and the degree of assurance the auditor plans to obtain. When a single purpose is met by a combination of procedures, the extent of each procedure is considered separately. In general, the extent of audit procedures increases as the risk of material misstatement increases. For example, in response to the assessed risk of material misstatement due to fraud, increasing sample sizes or performing substantive analytical procedures at a more detailed level may be appropriate. However, increasing the extent of an audit procedure is effective only if the audit procedure itself is relevant to the specific risk.

- A16. The use of computer-assisted audit techniques (CAATs) may enable more extensive testing of electronic transactions and account files, which may be useful when the auditor decides to modify the extent of testing, for example, in responding to the risks of material misstatement due to fraud. Such techniques can be used to select sample transactions from key electronic files, to sort transactions with specific characteristics, or to test an entire population instead of a sample.

#### Considerations specific to public sector entities

- A17. For the audits of public sector entities, the audit mandate and any other special auditing requirements may affect the auditor's consideration of the nature, timing and extent of further audit procedures.

#### Considerations specific to smaller entities

- A18. In the case of very small entities, there may not be many controls ~~activities~~ that could be identified by the auditor, or the extent to which their existence or operation have been documented by the entity may be limited. In such cases, it may be more efficient for the auditor to perform further audit procedures that are primarily substantive procedures. In some rare cases, however, the absence of controls ~~activities~~ or of other components of the system of internal control may make it impossible to obtain sufficient appropriate audit evidence.

#### Higher Assessments of Risk (Ref: Para 7(b))

- A19. When obtaining more persuasive audit evidence because of a higher assessment of risk, the auditor may increase the quantity of the evidence, or obtain evidence that is more relevant or reliable, for example, by placing more emphasis on obtaining third party evidence or by obtaining corroborating evidence from a number of independent sources.

#### *Tests of Controls*

#### Designing and Performing Tests of Controls (Ref: Para. 8)

- A20. Tests of controls are performed only on those controls that the auditor has determined are suitably designed to prevent, or detect and correct, a material misstatement in a relevant assertion, and the auditor plans to test those controls. If

substantially different controls were used at different times during the period under audit, each is considered separately.

- A21. Testing the operating effectiveness of controls is different from obtaining an understanding of and evaluating the design and implementation of controls. However, the same types of audit procedures are used. The auditor may, therefore, decide it is efficient to test the operating effectiveness of controls at the same time as evaluating their design and determining that they have been implemented.
- A22. Further, although some risk assessment procedures may not have been specifically designed as tests of controls, they may nevertheless provide audit evidence about the operating effectiveness of the controls and, consequently, serve as tests of controls. For example, the auditor's risk assessment procedures may have included:
- Inquiring about management's use of budgets.
  - Observing management's comparison of monthly budgeted and actual expenses.
  - Inspecting reports pertaining to the investigation of variances between budgeted and actual amounts.

These audit procedures provide knowledge about the design of the entity's budgeting policies and whether they have been implemented, but may also provide audit evidence about the effectiveness of the operation of budgeting policies in preventing or detecting material misstatements in the classification of expenses.

- A23. In addition, the auditor may design a test of controls to be performed concurrently with a test of details on the same transaction. Although the purpose of a test of controls is different from the purpose of a test of details, both may be accomplished concurrently by performing a test of controls and a test of details on the same transaction, also known as a dual-purpose test. For example, the auditor may design, and evaluate the results of, a test to examine an invoice to determine whether it has been approved and to provide substantive audit evidence of a transaction. A dual-purpose test is designed and evaluated by considering each purpose of the test separately.
- A24. In some cases, the auditor may find it impossible to design effective substantive procedures that by themselves provide sufficient appropriate audit evidence at the assertion level.<sup>110</sup> This may occur when an entity conducts its business using IT and no documentation of transactions is produced or maintained, other than through the IT system. In such cases, paragraph 8(b) requires the auditor to perform tests of relevant controls that address the risk for which substantive procedures alone cannot provide sufficient appropriate audit evidence.

---

<sup>110</sup> ISA 315 (Revised 2019), paragraph 33-39

## Audit Evidence and Intended Reliance (Ref: Para. 9)

A25. A higher level of assurance may be sought about the operating effectiveness of controls when the approach adopted consists primarily of tests of controls, in particular where it is not possible or practicable to obtain sufficient appropriate audit evidence only from substantive procedures.

## Nature and Extent of Tests of Controls

### Other audit procedures in combination with inquiry (Ref: Para. 10(a))

A26. Inquiry alone is not sufficient to test the operating effectiveness of controls. Accordingly, other audit procedures are performed in combination with inquiry. In this regard, inquiry combined with inspection or reperformance may provide more assurance than inquiry and observation, since an observation is pertinent only at the point in time at which it is made.

A27. The nature of the particular control influences the type of procedure required to obtain audit evidence about whether the control was operating effectively. For example, if operating effectiveness is evidenced by documentation, the auditor may decide to inspect it to obtain audit evidence about operating effectiveness. For other controls, however, documentation may not be available or relevant. For example, documentation of operation may not exist for some factors in the control environment, such as assignment of authority and responsibility, or for some types of controls—activities, such as ~~automated controls activities performed by a computer~~. In such circumstances, audit evidence about operating effectiveness may be obtained through inquiry in combination with other audit procedures such as observation or the use of CAATs.

## Extent of tests of controls

A28. When more persuasive audit evidence is needed regarding the effectiveness of a control, it may be appropriate to increase the extent of testing of the control. As well as the degree of reliance on controls, matters the auditor may consider in determining the extent of tests of controls include the following:

- The frequency of the performance of the control by the entity during the period.
- The length of time during the audit period that the auditor is relying on the operating effectiveness of the control.
- The expected rate of deviation from a control.
- The relevance and reliability of the audit evidence to be obtained regarding the operating effectiveness of the control at the assertion level.
- The extent to which audit evidence is obtained from tests of other controls related to the assertion.

ISA 530<sup>111</sup> contains further guidance on the extent of testing.

A29. Because of the inherent consistency of IT processing, it may not be necessary to increase the extent of testing of an automated control. An automated controls can be expected to function consistently unless the ~~program~~ IT application (including the tables, files, or other permanent data used by the ~~program~~ IT application) is changed. Once the auditor determines that an automated control is functioning as intended (which could be done at the time the control is initially implemented or at some other date), the auditor may consider performing tests to determine that the control continues to function effectively. Such tests ~~might~~ may include testing the general IT controls related to the IT application, determining that:

- ~~• Changes to the program are not made without being subject to the appropriate program change controls;~~
- ~~• The authorized version of the program is used for processing transactions; and~~
- ~~• Other relevant general controls are effective.~~

~~Such tests also might include determining that changes to the programs have not been made, as may be the case when the entity uses packaged software applications without modifying or maintaining them. For example, the auditor may inspect the record of the administration of IT security to obtain audit evidence that unauthorized access has not occurred during the period.~~

A29a. Similarly, the auditor may perform tests of controls that address risks of material misstatement related to the integrity of the entity's data, or the completeness and accuracy of the entity's system-generated reports, or to address risks of material misstatement for which substantive procedures alone cannot provide sufficient appropriate audit evidence. These tests of controls may include tests of general IT controls that address the matters in paragraph 10(a). When this is the case, the auditor may not need to perform any further testing to obtain audit evidence about the matters in paragraph 10(a).

A29b. When the auditor determines that a general IT control is deficient, the auditor may consider the nature of the related risk(s) arising from the use of IT that were identified in accordance with ISA 315 (Revised 2019)<sup>112</sup> to provide the basis for the design of the auditor's additional procedures to address the assessed risk of material misstatement. Such procedures may address determining whether:

- ~~• The related risk(s) arising from IT has occurred. For example, if users have unauthorized access to an IT application (but cannot access or modify the system logs that track access), the auditor may inspect the system logs to obtain audit evidence that those users did not access the IT application during the period.~~

---

<sup>111</sup> ISA 530, *Audit Sampling*

<sup>112</sup> ISA 315 (Revised 2019), paragraph 26(c)(i)

- There are any alternate or redundant general IT controls, or any other controls, that address the related risk(s) arising from the use of IT. If so, the auditor may identify such controls (if not already identified) and therefore evaluate their design, determine that they have been implemented and perform tests of their operating effectiveness. For example, if a general IT control related to user access is deficient, the entity may have an alternate control whereby IT management reviews end user access reports on a timely basis. Circumstances when an application control may address a risk arising from the use of IT may include when the information that may be affected by the general IT control deficiency can be reconciled to external sources (e.g., a bank statement) or internal sources not affected by the general IT control deficiency (e.g., a separate IT application or data source).

#### Testing of indirect controls (Ref: Para. 10(b))

- A30. In some circumstances, it may be necessary to obtain audit evidence supporting the effective operation of indirect controls (e.g., general IT controls). As explained in paragraphs A29 to A29b, general IT controls may have been identified in accordance with ISA 315 (Revised 2019) because of their support of the operating effectiveness of automated controls or due to their support in maintaining the integrity of information used in the entity's financial reporting, including system-generated reports. The requirement in paragraph 10(b) acknowledges that the auditor may have already tested certain indirect controls to address the matters in paragraph 10(a). For example, when the auditor decides to test the effectiveness of a user review of exception reports detailing sales in excess of authorized credit limits, the user review and related follow up is the control that is directly of relevance to the auditor. Controls over the accuracy of the information in the reports (for example, general IT controls) are described as "indirect" controls.
- A31. ~~Because of the inherent consistency of IT processing, audit evidence about the implementation of an automated application control, when considered in combination with audit evidence about the operating effectiveness of the entity's general controls (in particular, change controls), may also provide substantial audit evidence about its operating effectiveness.~~

#### Timing of Tests of Controls

##### Intended period of reliance (Ref: Para. 11)

- A32. Audit evidence pertaining only to a point in time may be sufficient for the auditor's purpose, for example, when testing controls over the entity's physical inventory counting at the period end. If, on the other hand, the auditor intends to rely on a control over a period, tests that are capable of providing audit evidence that the control operated effectively at relevant times during that period are appropriate. Such tests may include tests of controls in the entity's process to monitoring of the system of internal controls.

Using audit evidence obtained during an interim period (Ref: Para. 12(b))

A33. Relevant factors in determining what additional audit evidence to obtain about controls that were operating during the period remaining after an interim period, include:

- The significance of the assessed risks of material misstatement at the assertion level.
- The specific controls that were tested during the interim period, and significant changes to them since they were tested, including changes in the information system, processes, and personnel.
- The degree to which audit evidence about the operating effectiveness of those controls was obtained.
- The length of the remaining period.
- The extent to which the auditor intends to reduce further substantive procedures based on the reliance of controls.
- The control environment.

A34. Additional audit evidence may be obtained, for example, by extending tests of controls over the remaining period or testing the entity's monitoring of controls.

Using audit evidence obtained in previous audits (Ref: Para. 13)

A35. In certain circumstances, audit evidence obtained from previous audits may provide audit evidence where the auditor performs audit procedures to establish its continuing relevance and reliability. For example, in performing a previous audit, the auditor may have determined that an automated control was functioning as intended. The auditor may obtain audit evidence to determine whether changes to the automated control have been made that affect its continued effective functioning through, for example, inquiries of management and the inspection of logs to indicate what controls have been changed. Consideration of audit evidence about these changes may support either increasing or decreasing the expected audit evidence to be obtained in the current period about the operating effectiveness of the controls.

Controls that have changed from previous audits (Ref: Para. 14(a))

A36. Changes may affect the relevance and reliability of the audit evidence obtained in previous audits such that there may no longer be a basis for continued reliance. For example, changes in a system that enable an entity to receive a new report from the system probably do not affect the relevance of audit evidence from a previous audit; however, a change that causes data to be accumulated or calculated differently does affect it.

Controls that have not changed from previous audits (Ref: Para. 14(b))

A37. The auditor's decision on whether to rely on audit evidence obtained in previous audits for controls that:

- (a) have not changed since they were last tested; and
- (b) are not controls that mitigate a significant risk,

is a matter of professional judgment. In addition, the length of time between retesting such controls is also a matter of professional judgment, but is required by paragraph 14 (b) to be at least once in every third year.

A38. In general, the higher the risk of material misstatement, or the greater the reliance on controls, the shorter the time period elapsed, if any, is likely to be. Factors that may decrease the period for retesting a control, or result in not relying on audit evidence obtained in previous audits at all, include the following:

- A deficient control environment.
- ~~A Deficiency in the entity's process to monitoring of the system of internal controls.~~
- A significant manual element to the relevant controls.
- Personnel changes that significantly affect the application of the control.
- Changing circumstances that indicate the need for changes in the control.
- Deficient general IT controls.

A39. When there are a number of controls for which the auditor intends to rely on audit evidence obtained in previous audits, testing some of those controls in each audit provides corroborating information about the continuing effectiveness of the control environment. This contributes to the auditor's decision about whether it is appropriate to rely on audit evidence obtained in previous audits.

#### Evaluating the Operating Effectiveness of Controls (Ref: Para.16–17)

A40. A material misstatement detected by the auditor's procedures is a strong indicator of the existence of a significant deficiency in internal control.

A41. The concept of effectiveness of the operation of controls recognizes that some deviations in the way controls are applied by the entity may occur. Deviations from prescribed controls may be caused by such factors as changes in key personnel, significant seasonal fluctuations in volume of transactions and human error. The detected rate of deviation, in particular in comparison with the expected rate, may indicate that the control cannot be relied on to reduce risk at the assertion level to that assessed by the auditor.

#### Substantive Procedures (Ref: Para. 6, 18)

A42. Paragraph 18 requires the auditor to design and perform substantive procedures for each material-class of transactions, account balance, and disclosure, ~~irrespective of~~

the assessed risks of material misstatement. For significant classes of transactions, account balances and disclosures, substantive procedures may have already been performed because paragraph 6 requires the auditor to design and perform further audit procedures that are responsive to the assessed risks of material misstatement at the assertion level. Accordingly, substantive procedures are required to be designed and performed in accordance with paragraph 18:

- When the further audit procedures for significant classes of transactions, account balances or disclosures, designed and performed in accordance with paragraph 6, did not include substantive procedures; or
- For each class of transactions, account balance or disclosure that is not a significant class of transactions, account balance or disclosure, but that has been identified as material in accordance with ISA 315 (Revised 2019).<sup>113</sup>

This requirement reflects the facts that: (a) the auditor's assessment of risk is judgmental and so may not identify all risks of material misstatement; and (b) there are inherent limitations to ~~internal~~ controls, including management override.

A42a. Not all assertions within a material class of transactions, account balance or disclosure are required to be tested. Rather, in designing the substantive procedures to be performed, the auditor's consideration of the assertion(s) in which, if a misstatement were to occur, there is a reasonable possibility of the misstatement being material, may assist in identifying the appropriate nature, timing and extent of the procedures to be performed.

## Nature and Extent of Substantive Procedures

A43. Depending on the circumstances, the auditor may determine that:

- Performing only substantive analytical procedures will be sufficient to reduce audit risk to an acceptably low level. For example, where the auditor's assessment of risk is supported by audit evidence from tests of controls.
- Only tests of details are appropriate.
- A combination of substantive analytical procedures and tests of details are most responsive to the assessed risks.

A44. Substantive analytical procedures are generally more applicable to large volumes of transactions that tend to be predictable over time. ISA 520<sup>114</sup> establishes requirements and provides guidance on the application of analytical procedures during an audit.

A45. The nature assessment of the risk ~~and or the nature of the~~ assertion is relevant to the design of tests of details. For example, tests of details related to the existence or

---

<sup>113</sup> ISA 315 (Revised 2019), paragraph 36

<sup>114</sup> ISA 520, *Analytical Procedures*

occurrence assertion may involve selecting from items contained in a financial statement amount and obtaining the relevant audit evidence. On the other hand, tests of details related to the completeness assertion may involve selecting from items that are expected to be included in the relevant financial statement amount and investigating whether they are included.

- A46. Because the assessment of the risk of material misstatement takes account of ~~internal controls that the auditor plans to test~~, the extent of substantive procedures may need to be increased when the results from tests of controls are unsatisfactory. However, increasing the extent of an audit procedure is appropriate only if the audit procedure itself is relevant to the specific risk.
- A47. In designing tests of details, the extent of testing is ordinarily thought of in terms of the sample size. However, other matters are also relevant, including whether it is more effective to use other selective means of testing. See ISA 500.<sup>115</sup>

Considering Whether External Confirmation Procedures Are to Be Performed (Ref: Para. 19)

A48. External confirmation procedures frequently are relevant when addressing assertions associated with account balances and their elements, but need not be restricted to these items. For example, the auditor may request external confirmation of the terms of agreements, contracts, or transactions between an entity and other parties. External confirmation procedures also may be performed to obtain audit evidence about the absence of certain conditions. For example, a request may specifically seek confirmation that no “side agreement” exists that may be relevant to an entity’s revenue cutoff assertion. Other situations where external confirmation procedures may provide relevant audit evidence in responding to assessed risks of material misstatement include:

- Bank balances and other information relevant to banking relationships.
- Accounts receivable balances and terms.
- Inventories held by third parties at bonded warehouses for processing or on consignment.
- Property title deeds held by lawyers or financiers for safe custody or as security.
- Investments held for safekeeping by third parties, or purchased from stockbrokers but not delivered at the balance sheet date.
- Amounts due to lenders, including relevant terms of repayment and restrictive covenants.
- Accounts payable balances and terms.

---

<sup>115</sup> ISA 500, *Audit Evidence*, paragraph 10

A49. Although external confirmations may provide relevant audit evidence relating to certain assertions, there are some assertions for which external confirmations provide less relevant audit evidence. For example, external confirmations provide less relevant audit evidence relating to the recoverability of accounts receivable balances, than they do of their existence.

A50. The auditor may determine that external confirmation procedures performed for one purpose provide an opportunity to obtain audit evidence about other matters. For example, confirmation requests for bank balances often include requests for information relevant to other financial statement assertions. Such considerations may influence the auditor's decision about whether to perform external confirmation procedures.

A51. Factors that may assist the auditor in determining whether external confirmation procedures are to be performed as substantive audit procedures include:

- The confirming party's knowledge of the subject matter – responses may be more reliable if provided by a person at the confirming party who has the requisite knowledge about the information being confirmed.
- The ability or willingness of the intended confirming party to respond – for example, the confirming party:
  - May not accept responsibility for responding to a confirmation request;
  - May consider responding too costly or time consuming;
  - May have concerns about the potential legal liability resulting from responding;
  - May account for transactions in different currencies; or
  - May operate in an environment where responding to confirmation requests is not a significant aspect of day-to-day operations.

In such situations, confirming parties may not respond, may respond in a casual manner or may attempt to restrict the reliance placed on the response.

- The objectivity of the intended confirming party – if the confirming party is a related party of the entity, responses to confirmation requests may be less reliable.

Substantive Procedures Related to the Financial Statement Closing Process (Ref: Para. 20)

A52. The nature, and also the extent, of the auditor's substantive procedures related to the financial statement closing process depends on the nature and complexity of the entity's financial reporting process and the related risks of material misstatement.

*Substantive Procedures Responsive to Significant Risks (Ref: Para. 21)*

A53. Paragraph 21 of this ISA requires the auditor to perform substantive procedures that are specifically responsive to risks the auditor has determined to be significant risks. Audit evidence in the form of external confirmations received directly by the auditor from appropriate confirming parties may assist the auditor in obtaining audit evidence with the high level of reliability that the auditor requires to respond to significant risks of material misstatement, whether due to fraud or error. For example, if the auditor identifies that management is under pressure to meet earnings expectations, there may be a risk that management is inflating sales by improperly recognizing revenue related to sales agreements with terms that preclude revenue recognition or by invoicing sales before shipment. In these circumstances, the auditor may, for example, design external confirmation procedures not only to confirm outstanding amounts, but also to confirm the details of the sales agreements, including date, any rights of return and delivery terms. In addition, the auditor may find it effective to supplement such external confirmation procedures with inquiries of non-financial personnel in the entity regarding any changes in sales agreements and delivery terms.

*Timing of Substantive Procedures (Ref: Para. 22–23)*

A54. In most cases, audit evidence from a previous audit's substantive procedures provides little or no audit evidence for the current period. There are, however, exceptions, for example, a legal opinion obtained in a previous audit related to the structure of a securitization to which no changes have occurred, may be relevant in the current period. In such cases, it may be appropriate to use audit evidence from a previous audit's substantive procedures if that evidence and the related subject matter have not fundamentally changed, and audit procedures have been performed during the current period to establish its continuing relevance.

*Using audit evidence obtained during an interim period (Ref: Para. 22)*

A55. In some circumstances, the auditor may determine that it is effective to perform substantive procedures at an interim date, and to compare and reconcile information concerning the balance at the period end with the comparable information at the interim date to:

- (a) Identify amounts that appear unusual;
- (b) Investigate any such amounts; and
- (c) Perform substantive analytical procedures or tests of details to test the intervening period.

A56. Performing substantive procedures at an interim date without undertaking additional procedures at a later date increases the risk that the auditor will not detect misstatements that may exist at the period end. This risk increases as the remaining period is lengthened. Factors such as the following may influence whether to perform substantive procedures at an interim date:

- The control environment and other ~~relevant~~ controls.
- The availability at a later date of information necessary for the auditor's procedures.
- The purpose of the substantive procedure.
- The assessed risk of material misstatement.
- The nature of the class of transactions or account balance and related assertions.
- The ability of the auditor to perform appropriate substantive procedures or substantive procedures combined with tests of controls to cover the remaining period in order to reduce the risk that misstatements that may exist at the period end will not be detected.

A57. Factors such as the following may influence whether to perform substantive analytical procedures with respect to the period between the interim date and the period end:

- Whether the period-end balances of the particular classes of transactions or account balances are reasonably predictable with respect to amount, relative significance, and composition.
- Whether the entity's procedures for analyzing and adjusting such classes of transactions or account balances at interim dates and for establishing proper accounting cutoffs are appropriate.
- Whether the information system ~~relevant to financial reporting~~ will provide information concerning the balances at the period end and the transactions in the remaining period that is sufficient to permit investigation of:
  - (a) Significant unusual transactions or entries (including those at or near the period end);
  - (b) Other causes of significant fluctuations, or expected fluctuations that did not occur; and
  - (c) Changes in the composition of the classes of transactions or account balances.

Misstatements detected at an interim date (Ref: Para. 23)

A58. When the auditor concludes that the planned nature, timing or extent of substantive procedures covering the remaining period need to be modified as a result of unexpected misstatements detected at an interim date, such modification may include extending or repeating the procedures performed at the interim date at the period end.

**Adequacy of Presentation of the Financial Statements** (Ref: Para. 24)

A59. Evaluating the appropriate presentation, arrangement and content of the financial statements includes, for example, consideration of the terminology used as required by the applicable financial reporting framework, the level of detail provided, the aggregation and disaggregation of amounts and the bases of amounts set forth.

### **Evaluating the Sufficiency and Appropriateness of Audit Evidence** (Ref: Para. 25–27)

A60. An audit of financial statements is a cumulative and iterative process. As the auditor performs planned audit procedures, the audit evidence obtained may cause the auditor to modify the nature, timing or extent of other planned audit procedures. Information may come to the auditor's attention that differs significantly from the information on which the risk assessment was based. For example:

- The extent of misstatements that the auditor detects by performing substantive procedures may alter the auditor's judgment about the risk assessments and may indicate a significant deficiency in internal control.
- The auditor may become aware of discrepancies in accounting records, or conflicting or missing evidence.
- Analytical procedures performed at the overall review stage of the audit may indicate a previously unrecognized risk of material misstatement.

In such circumstances, the auditor may need to reevaluate the planned audit procedures, based on the revised consideration of assessed risks of material misstatement for all or some of and the effect on the significant classes of transactions, account balances, or disclosures and related their relevant assertions. ISA 315 (Revised 2019) contains further guidance on revising the auditor's risk assessment.<sup>116</sup>

A61. The auditor cannot assume that an instance of fraud or error is an isolated occurrence. Therefore, the consideration of how the detection of a misstatement affects the assessed risks of material misstatement is important in determining whether the assessment remains appropriate.

A62. The auditor's judgment as to what constitutes sufficient appropriate audit evidence is influenced by such factors as the following:

- Significance of the potential misstatement in the assertion and the likelihood of its having a material effect, individually or aggregated with other potential misstatements, on the financial statements.
- Effectiveness of management's responses and controls to address the risks.
- Experience gained during previous audits with respect to similar potential misstatements.
- Results of audit procedures performed, including whether such audit procedures identified specific instances of fraud or error.

---

<sup>116</sup> ISA 315 (Revised 2019), paragraph 37-4

- Source and reliability of the available information.
- Persuasiveness of the audit evidence.
- Understanding of the entity and its environment, the applicable financial reporting framework and including the entity's system of internal control.

**Documentation** (Ref: Para.28)

A63. The form and extent of audit documentation is a matter of professional judgment, and is influenced by the nature, size and complexity of the entity and its system of internal control, availability of information from the entity and the audit methodology and technology used in the audit.

**ISA 500, Audit Evidence**

**Application and Other Explanatory Material**

**Sufficient Appropriate Audit Evidence** (Ref: Para.6)

A1. Audit evidence is necessary to support the auditor's opinion and report. It is cumulative in nature and is primarily obtained from audit procedures performed during the course of the audit. It may, however, also include information obtained from other sources such as previous audits (provided the auditor has evaluated whether such information remains relevant and reliable as audit evidence for the current audit<sup>117</sup> ~~determined whether changes have occurred since the previous audit that may affect its relevance to the current audit~~) or a firm's quality control procedures for client acceptance and continuance. In addition to other sources inside and outside the entity, the entity's accounting records are an important source of audit evidence. Also, information that may be used as audit evidence may have been prepared using the work of a management's expert. Audit evidence comprises both information that supports and corroborates management's assertions, and any information that contradicts such assertions. In addition, in some cases the absence of information (for example, management's refusal to provide a requested representation) is used by the auditor, and therefore, also constitutes audit evidence.

...

*Audit Procedures for Obtaining Audit Evidence*

...

Observation

A17. Observation consists of looking at a process or procedure being performed by others, for example, the auditor's observation of inventory counting by the entity's personnel,

---

<sup>117</sup> ISA 315 (Revised 2019), paragraph 9.16

or of the performance of controls ~~activities~~. Observation provides audit evidence about the performance of a process or procedure, but is limited to the point in time at which the observation takes place, and by the fact that the act of being observed may affect how the process or procedure is performed. See ISA 501 for further guidance on observation of the counting of inventory.

...

## **ISA 501, *Audit Evidence—Special Considerations for Selected Items***

### **Application and Other Explanatory Material**

#### **Inventory**

*Attendance at Physical Inventory Counting* (Ref: Para. 4(a))

...

Evaluate Management's Instructions and Procedures (Ref: Para. 4(a)(i))

- A4. Matters relevant in evaluating management's instructions and procedures for recording and controlling the physical inventory counting include whether they address, for example:
- The application of appropriate controls ~~activities~~, for example, collection of used physical inventory count records, accounting for unused physical inventory count records, and count and re-count procedures.

...

## **ISA 530, *Audit Sampling***

### **Application and Other Explanatory Material**

...

#### **Sample Design, Size, and Selection of Items for Testing**

*Sample Design* (Ref: Para. 6)

...

- A7. In considering the characteristics of a population, for tests of controls, the auditor makes an assessment of the expected rate of deviation based on the auditor's understanding of the ~~relevant~~ controls or on the examination of a small number of items from the population. This assessment is made in order to design an audit sample and to determine sample size....

...

## Appendix 2

(Ref: Para. A11)

### Example of Factors Influencing Sample Size for Test of Controls

The following are factors that the auditor may consider when determining the sample size for tests of controls. These factors, which need to be considered together, assume the auditor does not modify the nature or timing of tests of controls or otherwise modify the approach to substantive procedures in response to assessed risks.

Factor 1                    An increase in the extent to which the auditor's risk assessment takes into account ~~relevant~~ plans to test the operating effectiveness of controls.

...

### ISA 550, *Related Parties*

#### Application and Other Explanatory Material

...

#### Risk Assessment Procedures and Related Activities

...

#### *Understanding the Entity's Related Party Relationships and Transactions*

Discussion among the Engagement Team (Ref: Para. 12)

A9. Matters that may be addressed in the discussion among the engagement team include:

- ...
- The importance that management and those charged with governance attach to the identification, appropriate accounting for, and disclosure of related party relationships and transactions (if the applicable financial reporting framework establishes related party requirements), and the related risk of management override of ~~relevant~~ controls.

...

The Identity of the Entity's Related Parties (Ref: Para. 13(a))

...

A12. However, where the framework does not establish related party requirements, the entity may not have such information systems in place. Under such circumstances, it

is possible that management may not be aware of the existence of all related parties. Nevertheless, the requirement to make the inquiries specified by paragraph 13 still applies because management may be aware of parties that meet the related party definition set out in this ISA. In such a case, however, the auditor's inquiries regarding the identity of the entity's related parties are likely to form part of the auditor's risk assessment procedures and related activities performed in accordance with ISA 315 (Revised 2019) to obtain information regarding the entity's organizational structure, ownership, governance and business model:-

- ~~The entity's ownership and governance structures;~~
- ~~The types of investments that the entity is making and plans to make; and~~
- ~~The way the entity is structured and how it is financed.~~

In the particular case of common control relationships, as management is more likely to be aware of such relationships if they have economic significance to the entity, the auditor's inquiries are likely to be more effective if they are focused on whether parties with which the entity engages in significant transactions, or shares resources to a significant degree, are related parties.

...

#### Considerations specific to smaller entities

A20. ~~Controls activities~~ in smaller entities are likely to be less formal and smaller entities may have no documented processes for dealing with related party relationships and transactions. An owner-manager may mitigate some of the risks arising from related party transactions, or potentially increase those risks, through active involvement in all the main aspects of the transactions. For such entities, the auditor may obtain an understanding of the related party relationships and transactions, and any controls that may exist over these, through inquiry of management combined with other procedures, such as observation of management's oversight and review activities, and inspection of available relevant documentation.

...

#### *Sharing Related Party Information with the Engagement Team* (Ref: Para. 17)

A28. Relevant related party information that may be shared among the engagement team members includes, for example:

- The identity of the entity's related parties.
- The nature of the related party relationships and transactions.
- Significant or complex related party relationships or transactions that may be determined to be significant risks ~~require special audit consideration~~, in particular transactions in which management or those charged with governance are financially involved.

...

## **Responses to the Risks of Material Misstatement Associated with Related Party Relationships and Transactions (Ref: Para. 20)**

...

A34. Depending upon the results of the auditor's risk assessment procedures, the auditor may consider it appropriate to obtain audit evidence without testing the entity's controls over related party relationships and transactions. In some circumstances, however, it may not be possible to obtain sufficient appropriate audit evidence from substantive audit procedures alone in relation to the risks of material misstatement associated with related party relationships and transactions. For example, where intra-group transactions between the entity and its components are numerous and a significant amount of information regarding these transactions is initiated, recorded, processed or reported electronically in an integrated system, the auditor may determine that it is not possible to design effective substantive audit procedures that by themselves would reduce the risks of material misstatement associated with these transactions to an acceptably low level. In such a case, in meeting the ISA 330 requirement to obtain sufficient appropriate audit evidence as to the operating effectiveness of ~~relevant~~ controls,<sup>118</sup> the auditor is required to test the entity's controls over the completeness and accuracy of the recording of the related party relationships and transactions.

...

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

### **Introduction**

#### **Scope of this ISA**

1. This International Standard on Auditing (ISA) deals with the auditor's responsibilities relating to accounting estimates and related disclosures in an audit of financial statements. Specifically, it includes requirements and guidance that refer to, or expand on, how ISA 315 (Revised 2019),<sup>119</sup> ISA 330,<sup>120</sup> ISA 450,<sup>121</sup> ISA 500<sup>122</sup> and other relevant ISAs are to be applied in relation to accounting estimates and related disclosures. It also includes requirements and guidance on the

---

<sup>118</sup> ISA 330, paragraph 8(b)

<sup>119</sup> ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment*

<sup>120</sup> ISA 330, *The Auditor's Responses to Assessed Risks*

<sup>121</sup> ISA 450, *Evaluation of Misstatements Identified during the Audit*

<sup>122</sup> ISA 500, *Audit Evidence*

evaluation of misstatements of accounting estimates and related disclosures, and indicators of possible management bias.

### **Nature of Accounting Estimates**

2. Accounting estimates vary widely in nature and are required to be made by management when the monetary amounts cannot be directly observed. The measurement of these monetary amounts is subject to estimation uncertainty, which reflects inherent limitations in knowledge or data. These limitations give rise to inherent subjectivity and variation in the measurement outcomes. The process of making accounting estimates involves selecting and applying a method using assumptions and data, which requires judgment by management and can give rise to complexity in measurement. The effects of complexity, subjectivity or other inherent risk factors on the measurement of these monetary amounts affects their susceptibility to misstatement. (Ref: Para. A1–A6, Appendix 1)
3. Although this ISA applies to all accounting estimates, the degree to which an accounting estimate is subject to estimation uncertainty will vary substantially. The nature, timing and extent of the risk assessment and further audit procedures required by this ISA will vary in relation to the estimation uncertainty and the assessment of the related risks of material misstatement. For certain accounting estimates, estimation uncertainty may be very low, based on their nature, and the complexity and subjectivity involved in making them may also be very low. For such accounting estimates, the risk assessment procedures and further audit procedures required by this ISA would not be expected to be extensive. When estimation uncertainty, complexity or subjectivity are very high, such procedures would be expected to be much more extensive. This ISA contains guidance on how the requirements of this ISA can be scaled. (Ref: Para. A7)

### **Key Concepts of This ISA**

4. ~~This ISA 315 (Revised 2019) requires a separate assessment of inherent risk for identified risks of material misstatement at the assertion level.<sup>123</sup> purposes of assessing the risks of material misstatement at the assertion level for accounting estimates. In the context of ISA 540 (Revised), and D~~ Depending on the nature of a particular accounting estimate, the susceptibility of an assertion to a misstatement that could be material may be subject to or affected by estimation uncertainty, complexity, subjectivity or other inherent risk factors, and the interrelationship among them. ~~As explained in ISA 200,<sup>124</sup> inherent risk is higher for some assertions and related classes of transactions, account balances and disclosures than for others.~~ Accordingly, the assessment of inherent risk depends on the degree to which the inherent risk factors affect the likelihood or magnitude of misstatement, and varies

---

<sup>123</sup> ISA 315 (Revised 2019), paragraph 31

<sup>124</sup> ISA 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*, paragraph A40

on a scale that is referred to ~~in this ISA~~ as the spectrum of inherent risk. (Ref: Para. A8–A9, A65–A66, Appendix 1)

5. This ISA refers to relevant requirements in ISA 315 (Revised 2019) and ISA 330, and provides related guidance, to emphasize the importance of the auditor’s decisions about controls relating to accounting estimates, including decisions about whether:
  - There are controls ~~relevant to the audit~~ required to be identified by ISA 315 (Revised 2019), for which the auditor is required to evaluate their design and determine whether they have been implemented.
  - To test the operating effectiveness of ~~relevant~~ controls.
6. ~~This ISA 315 (Revised 2019) also requires a separate assessment of control risk when assessing the risks of material misstatement at the assertion level for accounting estimates. In assessing control risk, the auditor takes into account whether the auditor’s further audit procedures contemplate planned reliance on the operating effectiveness of controls. If the auditor does not perform plan to tests the operating effectiveness of controls, or does not intend to rely on the operating effectiveness of controls, the auditor’s assessment of the risk of material misstatement at the assertion level control risk cannot be reduced for the effective operation of controls with respect to the particular assertion is such that the assessment of the risk of material misstatement is the same as the assessment of inherent risk.~~<sup>125</sup> (Ref: Para. A10)
7. This ISA emphasizes that the auditor’s further audit procedures (including, where appropriate, tests of controls) need to be responsive to the reasons for the assessed risks of material misstatement at the assertion level, taking into account the effect of one or more inherent risk factors and the auditor’s assessment of control risk.
8. The exercise of professional skepticism in relation to accounting estimates is affected by the auditor’s consideration of inherent risk factors, and its importance increases when accounting estimates are subject to a greater degree of estimation uncertainty or are affected to a greater degree by complexity, subjectivity or other inherent risk factors. Similarly, the exercise of professional skepticism is important when there is greater susceptibility to misstatement due to management bias or ~~fraud~~ other fraud risk factors insofar as they affect inherent risk. (Ref: Para. A11)

...

...

## Objective

...

---

<sup>125</sup> ISA 530, *Audit Sampling*, Appendix 3

## Definitions

...

## Requirements

### Risk Assessment Procedures and Related Activities

13. When obtaining an understanding of the entity and its environment, the applicable financial reporting framework and ~~including~~ the entity's system of internal control, as required by ISA 315 (Revised 2019),<sup>126</sup> the auditor shall obtain an understanding of the following matters related to the entity's accounting estimates. The auditor's procedures to obtain the understanding shall be performed to the extent necessary to obtain audit evidence that provides an appropriate basis for the identification and assessment of risks of material misstatement at the financial statement and assertion levels. (Ref: Para. A19–A22)

#### *Obtaining an Understanding of tThe Entity and Its Environment and the Applicable Financial Reporting Framework*

- (a) The entity's transactions and other events ~~and~~ conditions that may give rise to the need for, or changes in, accounting estimates to be recognized or disclosed in the financial statements. (Ref: Para. A23)
- (b) The requirements of the applicable financial reporting framework related to accounting estimates (including the recognition criteria, measurement bases, and the related presentation and disclosure requirements); and how they apply in the context of the nature and circumstances of the entity and its environment, including how ~~transactions and other events or conditions are subject to, or affected by,~~ the inherent risk factors affect susceptibility to misstatement of assertions. (Ref: Para. A24–A25)
- (c) Regulatory factors relevant to the entity's accounting estimates, including, when applicable, regulatory frameworks related to prudential supervision. (Ref: Para. A26)
- (d) The nature of the accounting estimates and related disclosures that the auditor expects to be included in the entity's financial statements, based on the auditor's understanding of the matters in 13(a)–(c) above. (Ref: Para. A27)

#### *Obtaining an Understanding of tThe Entity's System of Internal Control*

- (e) The nature and extent of oversight and governance that the entity has in place over management's financial reporting process relevant to accounting estimates. (Ref: Para. A28–A30).

---

<sup>126</sup> ISA 315 (Revised 2019), paragraphs ~~3, 5–6, 9, 11–12, 15–17, and 20–21~~ 19–27

- (f) How management identifies the need for, and applies, specialized skills or knowledge related to accounting estimates, including with respect to the use of a management's expert. (Ref: Para. A31)
- (g) How the entity's risk assessment process identifies and addresses risks relating to accounting estimates. (Ref: Para. A32–A33)
- (h) The entity's information system as it relates to accounting estimates, including:
  - (i) ~~How information relating to accounting estimates and related disclosures for significant classes of transactions, account balances or disclosures flows through the entity's information system. The classes of transactions, events and conditions, that are significant to the financial statements and that give rise to the need for, or changes in, accounting estimates and related disclosures; and~~ (Ref: Para. A34–A35)
  - (ii) For such accounting estimates and related disclosures, how management:
    - a. Identifies the relevant methods, assumptions or sources of data, and the need for changes in them, that are appropriate in the context of the applicable financial reporting framework, including how management: (Ref: Para. A36–A37)
      - i. Selects or designs, and applies, the methods used, including the use of models; (Ref: Para. A38–A39)
      - ii. Selects the assumptions to be used, including consideration of alternatives, and identifies significant assumptions; (Ref: Para. A40–A43); and
      - iii. Selects the data to be used; (Ref: Para. A44)
    - b. Understands the degree of estimation uncertainty, including through considering the range of possible measurement outcomes; and (Ref: Para. A45)
    - c. Addresses the estimation uncertainty, including selecting a point estimate and related disclosures for inclusion in the financial statements. (Ref: Para. A46–A49)
  - (i) ~~Identified controls in the control activities component~~<sup>127</sup> ~~activities relevant to the audit~~ over management's process for making accounting estimates as described in paragraph 13(h)(ii). (Ref: Para. A50–A54)
  - (j) How management reviews the outcome(s) of previous accounting estimates and responds to the results of that review.

<sup>127</sup> ISA 315 (Revised 2019), paragraphs 26(a)(i)–(iv)

14. The auditor shall review the outcome of previous accounting estimates, or, where applicable, their subsequent re-estimation to assist in identifying and assessing the risks of material misstatement in the current period. The auditor shall take into account the characteristics of the accounting estimates in determining the nature and extent of that review. The review is not intended to call into question judgments about previous period accounting estimates that were appropriate based on the information available at the time they were made. (Ref: Para. A55–A60)

...

### **Identifying and Assessing the Risks of Material Misstatement**

16. In identifying and assessing the risks of material misstatement relating to an accounting estimate and related disclosures at the assertion level, including separately assessing inherent risk and control risk at the assertion level, as required by ISA 315 (Revised 2019),<sup>128</sup> the auditor shall ~~separately assess inherent risk and control risk. The auditor shall~~ take the following into account in identifying the risks of material misstatement and in assessing inherent risk: (Ref: Para. A64–A71)
- (a) The degree to which the accounting estimate is subject to estimation uncertainty; and (Ref: Para. A72–A75)
  - (b) The degree to which the following are affected by complexity, subjectivity, or other inherent risk factors: (Ref: Para. A76–A79)
    - (i) The selection and application of the method, assumptions and data in making the accounting estimate; or
    - (ii) The selection of management’s point estimate and related disclosures for inclusion in the financial statements.
17. The auditor shall determine whether any of the risks of material misstatement identified and assessed in accordance with paragraph 16 are, in the auditor’s judgment, a significant risk.<sup>129</sup> If the auditor has determined that a significant risk exists, the auditor shall identify controls that obtain an understanding of the entity’s controls, including control activities, relevant to address that risk,<sup>130</sup> and evaluate whether such controls have been designed effectively, and determine whether they have been implemented.<sup>131</sup> (Ref: Para. A80)

...

19. As required by ISA 330,<sup>132</sup> the auditor shall design and perform tests to obtain

---

<sup>128</sup> ISA 315 (Revised 2019), paragraph ~~25 and 26~~ 31 and 34

<sup>129</sup> ISA 315 (Revised 2019), paragraph ~~32~~ 27

<sup>130</sup> ISA 315 (Revised 2019), paragraph ~~26(a)(i)~~ 29

<sup>131</sup> ISA 315 (Revised 2019), paragraph 26(a)

<sup>132</sup> ISA 330, paragraph 8

sufficient appropriate audit evidence as to the operating effectiveness of ~~relevant~~ controls, if:

- (a) The auditor's assessment of risks of material misstatement at the assertion level includes an expectation that the controls are operating effectively; or
- (b) Substantive procedures alone cannot provide sufficient appropriate audit evidence at the assertion level.

In relation to accounting estimates, the auditor's tests of such controls shall be responsive to the reasons for the assessment given to the risks of material misstatement. In designing and performing tests of controls, the auditor shall obtain more persuasive audit evidence the greater the reliance the auditor places on the effectiveness of a control.<sup>133</sup> (Ref: Para. A85–A89)

...

#### *Other Considerations Relating to Audit Evidence*

30. In obtaining audit evidence regarding the risks of material misstatement relating to accounting estimates, irrespective of the sources of information to be used as audit evidence, the auditor shall comply with the relevant requirements in ISA 500.

When using the work of a management's expert, the requirements in paragraphs 21–29 of this ISA may assist the auditor in evaluating the appropriateness of the expert's work as audit evidence for a relevant assertion in accordance with paragraph 8(c) of ISA 500. In evaluating the work of the management's expert, the nature, timing and extent of the further audit procedures are affected by the auditor's evaluation of the expert's competence, capabilities and objectivity, the auditor's understanding of the nature of the work performed by the expert, and the auditor's familiarity with the expert's field of expertise. (Ref: Para. A126–A132)

...

#### **Documentation**

39. The auditor shall include in the audit documentation:<sup>134</sup> (Ref: Para. A149–A152)
- (a) Key elements of the auditor's understanding of the entity and its environment, including the entity's internal control related to the entity's accounting estimates;
  - (b) The linkage of the auditor's further audit procedures with the assessed risks of material misstatement at the assertion level,<sup>135</sup> taking into account the reasons (whether related to inherent risk or control risk) given to the assessment of those risks;

---

<sup>133</sup> ISA 330, paragraph 9

<sup>134</sup> ISA 230, *Audit Documentation*, paragraphs 8–11, A6, A7 and A10

<sup>135</sup> ISA 330, paragraph 28(b)

- (c) The auditor's response(s) when management has not taken appropriate steps to understand and address estimation uncertainty;
- (d) Indicators of possible management bias related to accounting estimates, if any, and the auditor's evaluation of the implications for the audit, as required by paragraph 32; and
- (e) Significant judgments relating to the auditor's determination of whether the accounting estimates and related disclosures are reasonable in the context of the applicable financial reporting framework, or are misstated.

## **Application and Other Explanatory Material**

### **Nature of Accounting Estimates** (Ref: Para. 2)

#### *Examples of Accounting Estimates*

...

#### *Methods*

- A2. A method is a measurement technique used by management to make an accounting estimate in accordance with the required measurement basis. For example, one recognized method used to make accounting estimates relating to share-based payment transactions is to determine a theoretical option call price using the Black Scholes option pricing formula. A method is applied using a computational tool or process, sometimes referred to as a model, and involves applying assumptions and data and taking into account a set of relationships between them.

#### *Assumptions and Data*

- A3. Assumptions involve judgments based on available information about matters such as the choice of an interest rate, a discount rate, or judgments about future conditions or events. An assumption may be selected by management from a range of appropriate alternatives. Assumptions that may be made or identified by a management's expert become management's assumptions when used by management in making an accounting estimate.
- A4. For purposes of this ISA, data is information that can be obtained through direct observation or from a party external to the entity. Information obtained by applying analytical or interpretive techniques to data is referred to as derived data when such techniques have a well-established theoretical basis and therefore less need for management judgment. Otherwise, such information is an assumption.
- A5. Examples of data include:
- Prices agreed in market transactions;
  - Operating times or quantities of output from a production machine;

- Historical prices or other terms included in contracts, such as a contracted interest rate, a payment schedule, and term included in a loan agreement;
- Forward-looking information such as economic or earnings forecasts obtained from an external information source, or
- A future interest rate determined using interpolation techniques from forward interest rates (derived data).

A6. Data can come from a wide range of sources. For example, data can be:

- Generated within the organization or externally;
- Obtained from a system that is either within or outside the general or subsidiary ledgers;
- Observable in contracts; or
- Observable in legislative or regulatory pronouncements.

*Scalability* (Ref: Para. 3)

A7. Examples of paragraphs that include guidance on how the requirements of this ISA can be scaled include paragraphs A20–A22, A63, A67, and A84.

## Key Concepts of This ISA

*Inherent Risk Factors* (Ref: Para. 4)

- A8. Inherent risk factors are characteristics of ~~conditions and events~~ and conditions that ~~may affect the susceptibility of an assertion to misstatement, whether due to fraud or error, of an assertion about a class of transactions, account balance or disclosures, before consideration of controls.~~<sup>136</sup> Appendix 1 further explains the nature of these inherent risk factors, and their inter-relationships, in the context of making accounting estimates and their presentation in the financial statements.
- A9. ~~In addition to the inherent risk factors of estimation uncertainty, complexity or subjectivity, other inherent risk factors that the auditor may consider in identifying and~~ When assessing the risks of material misstatement at the assertion level<sup>137</sup>, in addition to estimation uncertainty, complexity, and subjectivity, the auditor also takes into account the degree ~~may include the extent to which inherent risk factors included in ISA 315 (Revised 2019); (other than estimation uncertainty, complexity, and subjectivity); affect susceptibility to misstatement of assertions to misstatement about the accounting estimate. Such additional inherent risk factors include~~ is subject to, or affected by:

<sup>136</sup> ISA 315 (Revised 2019), paragraph 12(f)

<sup>137</sup> ISA 315 (Revised 2019), paragraph 31

- Change in the nature or circumstances of the relevant financial statement items, or requirements of the applicable financial reporting framework which may give rise to the need for changes in the method, assumptions or data used to make the accounting estimate.
- Susceptibility to misstatement due to management bias, or other fraud risk factors insofar as they affect inherent risk, in making the accounting estimate.
- Uncertainty, other than estimation uncertainty.

*Control Risk* (Ref: Para. 6)

A10. ~~An important consideration for the auditor is~~ In assessing control risk at the assertion level in accordance with ISA 315 (Revised 2019), the auditor takes into account is the effectiveness of the design of the controls that whether the auditor intends plans to rely test on the operating effectiveness of controls, and the extent to which the controls address the assessed inherent risks at the assertion level. When the auditor is considering whether to test the operating effectiveness of controls. The auditor's evaluation that controls are effectively designed and have been implemented supports an expectation, by the auditor, about the operating effectiveness of the controls in determining whether establishing the plan to test them.

*Professional Skepticism* (Ref: Para. 8)

....

*Concept of "Reasonable"* (Ref: Para. 9, 35)

...

**Risk Assessment Procedures and Related Activities**

*Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework, and the Entity's System of Internal Control* (Ref: Para. 13)

A19. Paragraphs ~~1944–2724~~ of ISA 315 (Revised 2019) require the auditor to obtain an understanding of certain matters about the entity and its environment, the applicable financial reporting framework and including the entity's system of internal control. The requirements in paragraph 13 of this ISA relate more specifically to accounting estimates and build on the broader requirements in ISA 315 (Revised 2019).

*Scalability*

A20. The nature, timing, and extent of the auditor's procedures to obtain the understanding of the entity and its environment, including the applicable financial reporting framework, and the entity's system of internal control, related to the entity's accounting estimates, may depend, to a greater or lesser degree, on the extent to which the individual matter(s) apply in the circumstances. For example,

the entity may have few transactions or other events ~~and or~~ conditions that give rise to the need for accounting estimates, the applicable financial reporting requirements may be simple to apply, and there may be no relevant regulatory factors. Further, the accounting estimates may not require significant judgments, and the process for making the accounting estimates may be less complex. In these circumstances, the accounting estimates may be subject to, or affected by, estimation uncertainty, complexity, subjectivity, or other inherent risk factors to a lesser degree, and there may be fewer identified controls in the control activities component relevant to the audit. If so, the auditor's risk identification and assessment procedures are likely to be less extensive and may be obtained primarily through inquiries of management with appropriate responsibilities for the financial statements, such as and simple walk-throughs of management's process for making the accounting estimate (including when evaluating whether identified controls in that process are designed effectively and when determining whether the control has been implemented).

- A21. By contrast, the accounting estimates may require significant judgments by management, and the process for making the accounting estimates may be complex and involve the use of complex models. In addition, the entity may have a more sophisticated information system, and more extensive controls over accounting estimates. In these circumstances, the accounting estimates may be subject to or affected by estimation uncertainty, subjectivity, complexity or other inherent risk factors to a greater degree. If so, the nature or timing of the auditor's risk assessment procedures are likely to be different, or be more extensive, than in the circumstances in paragraph A20.
- A22. The following considerations may be relevant for entities with only simple businesses, which may include many smaller entities:
- Processes relevant to accounting estimates may be uncomplicated because the business activities are simple or the required estimates may have a lesser degree of estimation uncertainty.
  - Accounting estimates may be generated outside of the general and subsidiary ledgers, controls over their development may be limited, and an owner-manager may have significant influence over their determination. The owner-manager's role in making the accounting estimates may need to be taken into account by the auditor both when identifying the risks of material misstatement and when considering the risk of management bias.

## The Entity and Its Environment

The entity's transactions and other events ~~and or~~ conditions (Ref: Para. 13(a))

- A23. Changes in circumstances that may give rise to the need for, or changes in, accounting estimates may include, for example, whether:
- The entity has engaged in new types of transactions;

- Terms of transactions have changed; or
- New events or conditions have occurred.

The requirements of the applicable financial reporting framework (Ref: Para. 13(b))

A24. Obtaining an understanding of the requirements of the applicable financial reporting framework provides the auditor with a basis for discussion with management and, where applicable, those charged with governance about how management has applied ~~these~~ requirements of the applicable financial reporting framework relevant to the accounting estimates, and about the auditor's determination of whether they have been applied appropriately. This understanding also may assist the auditor in communicating with those charged with governance when the auditor considers a significant accounting practice that is acceptable under the applicable financial reporting framework, not to be the most appropriate in the circumstances of the entity.<sup>138</sup>

A25. In obtaining this understanding, the auditor may seek to understand whether:

- The applicable financial reporting framework:
  - Prescribes certain criteria for the recognition, or methods for the measurement of accounting estimates;
  - Specifies certain criteria that permit or require measurement at a fair value, for example, by referring to management's intentions to carry out certain courses of action with respect to an asset or liability; or
  - Specifies required or suggested disclosures, including disclosures concerning judgments, assumptions, or other sources of estimation uncertainty relating to accounting estimates; and
- Changes in the applicable financial reporting framework require changes to the entity's accounting policies relating to accounting estimates.

Regulatory factors (Ref: Para. 13(c))

...

The nature of the accounting estimates and related disclosures that the auditor expects to be included in the financial statements (Ref: Para. 13(d))

...

---

<sup>138</sup> ISA 260 (Revised), paragraph 16(a)

*The Entity's System of Internal Control Relevant to the Audit*

The nature and extent of oversight and governance (Ref: Para. 13(e))

A28. In applying ISA 315 (Revised 2019),<sup>139</sup> the auditor's understanding of the nature and extent of oversight and governance that the entity has in place over management's process for making accounting estimates may be important to the auditor's required evaluation ~~of as it relates to~~ whether:

- Management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior; ~~and~~
- The ~~strengths in the entity's control environment~~ elements collectively provides an appropriate foundation for the other components of the system of internal control considering the nature and size of the entity; ~~and whether~~
- ~~those other components are undermined by~~ Control deficiencies identified in the control environment undermine the other components of the system of internal control.

...

A30. Obtaining an understanding of the oversight by those charged with governance may be important when there are accounting estimates that:

- Require significant judgment by management to address subjectivity;
- Have high estimation uncertainty;
- Are complex to make, for example, because of the extensive use of information technology, large volumes of data or the use of multiple data sources or assumptions with complex-interrelationships;
- Had, or ought to have had, a change in the method, assumptions or data compared to previous periods; or
- Involve significant assumptions.

Management's application of specialized skills or knowledge, including the use of management's experts (Ref: Para. 13(f))

...

The entity's risk assessment process (Ref: Para. 13(g))

A32. Understanding how the entity's risk assessment process identifies and addresses risks relating to accounting estimates may assist the auditor in considering changes in:

---

<sup>139</sup> ISA 315 (Revised 2019), paragraph 21(a)+4

- The requirements of the applicable financial reporting framework related to the accounting estimates;
- The availability or nature of data sources that are relevant to making the accounting estimates or that may affect the reliability of the data used;
- The entity's information system<sup>g</sup> or IT environment; and
- Key personnel.

A33. Matters that the auditor may consider in obtaining an understanding of how management identified and addresses the susceptibility to misstatement due to management bias or fraud in making accounting estimates, include whether, and if so how, management:

- Pays particular attention to selecting or applying the methods, assumptions and data used in making accounting estimates.
- Monitors key performance indicators that may indicate unexpected or inconsistent performance compared with historical or budgeted performance or with other known factors.
- Identifies financial or other incentives that may be a motivation for bias.
- Monitors the need for changes in the methods, significant assumptions or the data used in making accounting estimates.
- Establishes appropriate oversight and review of models used in making accounting estimates.
- Requires documentation of the rationale for, or an independent review of, significant judgments made in making accounting estimates.

The entity's information system relating to accounting estimates (Ref: Para. 13(h)(i))

A34. The significant classes of transactions, events and conditions within the scope of paragraph 13(h) are the same as the significant classes of transactions, events and conditions relating to accounting estimates and related disclosures that are subject to paragraphs ~~25(a)18(a) and (d)~~ of ISA 315 (Revised 2019). In obtaining the understanding of the entity's information system as it relates to accounting estimates, the auditor may consider:

- Whether the accounting estimates arise from the recording of routine and recurring transactions or whether they arise from non-recurring or unusual transactions.
- How the information system addresses the completeness of accounting estimates and related disclosures, in particular for accounting estimates related to liabilities.

A35. During the audit, the auditor may identify classes of transactions, events ~~and or~~ conditions that give rise to the need for accounting estimates and related disclosures

that management failed to identify. ISA 315 (Revised 2019) deals with circumstances where the auditor identifies risks of material misstatement that management failed to identify, including ~~determining whether there is a significant deficiency in internal control with regard to considering the implications for the auditor's evaluation of~~ the entity's risk assessment process.<sup>140</sup>

Management's Identification of the Relevant Methods, Assumptions and Sources of Data  
(Ref: Para. 13(h)(ii)(a))

...

Methods (Ref: Para. 13(h)(ii)(a)(i))

...

Models

A39. Management may design and implement specific controls around models used for making accounting estimates, whether management's own model or an external model. When the model itself has an increased level of complexity or subjectivity, such as an expected credit loss model or a fair value model using level 3 inputs, controls that address such complexity or subjectivity may be more likely to be identified as relevant to the audit. When complexity in relation to models is present, controls over data integrity are also more likely to be identified controls in accordance with ISA 315 (Revised 2019)~~relevant to the audit~~. Factors that may be appropriate for the auditor to consider in obtaining an understanding of the model and ~~of related identified controls activities relevant to the audit~~ include the following:

- How management determines the relevance and accuracy of the model;
- The validation or back testing of the model, including whether the model is validated prior to use and revalidated at regular intervals to determine whether it remains suitable for its intended use. The entity's validation of the model may include evaluation of:
  - The model's theoretical soundness;
  - The model's mathematical integrity; and
  - The accuracy and completeness of the data and the appropriateness of data and assumptions used in the model.
- How the model is appropriately changed or adjusted on a timely basis for changes in market or other conditions and whether there are appropriate change control policies over the model;

---

<sup>140</sup> ISA 315 (Revised 2019), paragraph ~~22(b)~~47

- Whether adjustments, also referred to as overlays in certain industries, are made to the output of the model and whether such adjustments are appropriate in the circumstances in accordance with the requirements of the applicable financial reporting framework. When the adjustments are not appropriate, such adjustments may be indicators of possible management bias; and
- Whether the model is adequately documented, including its intended applications, limitations, key parameters, required data and assumptions, the results of any validation performed on it and the nature of, and basis for, any adjustments made to its output.

Assumptions (Ref: Para. 13(h)(ii)(a)(ii))

...

Data (Ref: Para. 13(h)(ii)(a)(iii))

A44. Matters that the auditor may consider in obtaining an understanding of how management selects the data on which the accounting estimates are based include:

- The nature and source of the data, including information obtained from an external information source.
- How management evaluates whether the data is appropriate.
- The accuracy and completeness of the data.
- The consistency of the data used with data used in previous periods.
- The complexity of IT applications or other aspects of the entity's IT environment ~~the information technology systems~~ used to obtain and process the data, including when this involves handling large volumes of data.
- How the data is obtained, transmitted and processed and how its integrity is maintained.

How management understands and addresses estimation uncertainty (Ref: Para. 13(h)(ii)(b)–13(h)(ii)(c))

...

Identified Controls Activities Relevant to the Audit Over Management's Process for Making Accounting Estimates (Ref: Para 13(i))

A50. The auditor's judgment in identifying controls ~~relevant to the audit~~ in the controls activities component, and therefore the need to evaluate the design of those controls and determine whether they have been implemented, relates to management's process described in paragraph 13(h)(ii). The auditor may not identify ~~relevant~~ controls ~~activities~~ in relation to all ~~the elements~~ aspects of paragraph 13(h)(ii), ~~depending on the complexity associated with the accounting estimate.~~

A51. As part of ~~obtaining an understanding of~~ identifying the controls activities relevant to the audit, and ~~evaluating their design and determining whether they have been implemented,~~ the auditor may consider:

- How management determines the appropriateness of the data used to develop the accounting estimates, including when management uses an external information source or data from outside the general and subsidiary ledgers.
- The review and approval of accounting estimates, including the assumptions or data used in their development, by appropriate levels of management and, where appropriate, those charged with governance.
- The segregation of duties between those responsible for making the accounting estimates and those committing the entity to the related transactions, including whether the assignment of responsibilities appropriately takes account of the nature of the entity and its products or services. For example, in the case of a large financial institution, relevant segregation of duties may consist of an independent function responsible for estimation and validation of fair value pricing of the entity's financial products staffed by individuals whose remuneration is not tied to such products.
- The effectiveness of the design of the controls, ~~activities.~~ Generally, it may be more difficult for management to design controls that address subjectivity and estimation uncertainty in a manner that effectively prevents, or detects and corrects, material misstatements, than it is to design controls that address complexity. Controls that address subjectivity and estimation uncertainty may need to include more manual elements, which may be less reliable than automated controls as they can be more easily bypassed, ignored or overridden by management. The design effectiveness of controls addressing complexity may vary depending on the reason for, and the nature of, the complexity. For example, it may be easier to design more effective controls related to a method that is routinely used or over the integrity of data.

A52. When management makes extensive use of information technology in making an accounting estimate, identified controls relevant to the audit in the control activities component are likely to include general IT controls and application-information processing controls. Such controls may address risks related to:

- Whether the IT applications or other aspects of the IT environment information technology system ~~have~~ the capability and is appropriately configured to process large volumes of data;
- Complex calculations in applying a method. When diverse IT applications systems are required to process complex transactions, regular reconciliations between the IT applications systems are made, in particular when the IT applications systems do not have automated interfaces or may be subject to manual intervention;

- Whether the design and calibration of models is periodically evaluated;
- The complete and accurate extraction of data regarding accounting estimates from the entity's records or from external information sources;
- Data, including the complete and accurate flow of data through the entity's information system, the appropriateness of any modification to the data used in making accounting estimates, the maintenance of the integrity and security of the data. When using external information sources, risks related to processing or recording the data;
- Whether management has controls around access, change and maintenance of individual models to maintain a strong audit trail of the accredited versions of models and to prevent unauthorized access or amendments to those models; and
- Whether there are appropriate controls over the transfer of information relating to accounting estimates into the general ledger, including appropriate controls over journal entries.

A53. In some industries, such as banking or insurance, the term governance may be used to describe activities within the control environment, the entity's process to monitor the system of internal control ~~monitoring of controls~~, and other components of the system of internal control, as described in ISA 315 (Revised 2019).<sup>141</sup>

A54. For entities with an internal audit function, its work may be particularly helpful to the auditor in obtaining an understanding of:

- The nature and extent of management's use of accounting estimates;
- The design and implementation of controls ~~activities~~ that address the risks related to the data, assumptions and models used to make the accounting estimates;
- The aspects of the entity's information system that generate the data on which the accounting estimates are based; and
- How new risks relating to accounting estimates are identified, assessed and managed.

*Reviewing the Outcome or Re-Estimation of Previous Accounting Estimates* (Ref: Para. 14)

...

A58. Based on the auditor's previous assessment of the risks of material misstatement, for example, if inherent risk is assessed as higher for one or more risks of material misstatement, the auditor may judge that a more detailed retrospective review is

---

<sup>141</sup> ISA 315 (Revised 2019), Appendix 3 ~~paragraph A77~~

required. As part of the detailed retrospective review, the auditor may pay particular attention, when practicable, to the effect of data and significant assumptions used in making the previous accounting estimates. On the other hand, for example, for accounting estimates that arise from the recording of routine and recurring transactions, the auditor may judge that the application of analytical procedures as risk assessment procedures is sufficient for purposes of the review.

- A59. The measurement objective for fair value accounting estimates and other accounting estimates, based on current conditions at the measurement date, deals with perceptions about value at a point in time, which may change significantly and rapidly as the environment in which the entity operates changes. The auditor may therefore focus the review on obtaining information that may be relevant to identifying and assessing risks of material misstatement. For example, in some cases, obtaining an understanding of changes in marketplace participant assumptions that affected the outcome of a previous period's fair value accounting estimates may be unlikely to provide relevant audit evidence. In this case, audit evidence may be obtained by understanding the outcomes of assumptions (such as a cash flow projections) and understanding the effectiveness of management's prior estimation process that supports the identification and assessment of the risks of material misstatement in the current period.
- A60. A difference between the outcome of an accounting estimate and the amount recognized in the previous period's financial statements does not necessarily represent a misstatement of the previous period's financial statements. However, such a difference may represent a misstatement if, for example, the difference arises from information that was available to management when the previous period's financial statements were finalized, or that could reasonably be expected to have been obtained and taken into account in the context of the applicable financial reporting framework.<sup>142</sup> Such a difference may call into question management's process for taking information into account in making the accounting estimate. As a result, the auditor may reassess any plan to test related controls and the related assessment of control risk ~~and/or~~ may determine that more persuasive audit evidence needs to be obtained about the matter. Many financial reporting frameworks contain guidance on distinguishing between changes in accounting estimates that constitute misstatements and changes that do not, and the accounting treatment required to be followed in each case.

*Specialized Skills or Knowledge* (Ref: Para. 15)

...

#### **Identifying and Assessing the Risks of Material Misstatement** (Ref: Para. 4, 16)

- A64. Identifying and assessing risks of material misstatement at the assertion level relating to accounting estimates is important for all accounting estimates, including

---

<sup>142</sup> ISA 560, Subsequent Events, paragraph 14

not only those that are recognized in the financial statements, but also those that are included in the notes to the financial statements.

A65. Paragraph A42 of ISA 200 states that the ISAs ~~do not ordinarily refer to inherent risk and control risk separately~~ typically refer to the “risks of material misstatement” rather than to inherent risk and control risk separately. However, this ISA 315 (Revised 2019) requires a separate assessment of inherent risk and control risk to provide a basis for designing and performing further audit procedures to respond to the risks of material misstatement at the assertion level.<sup>143</sup> including significant risks, ~~at the assertion level for accounting estimates~~ in accordance with ISA 330.<sup>144</sup>

A66. In identifying the risks of material misstatement and in assessing inherent risk for accounting estimates in accordance with ISA 315 (Revised 2019).<sup>145</sup> the auditor is required to take into account ~~the degree to which the accounting estimate is subject to, or affected by, the inherent risk factors that affect susceptibility to misstatement of assertions, and how they do so~~ estimation uncertainty, complexity, subjectivity, or other inherent risk factors. The auditor’s consideration of the inherent risk factors may also provide information to be used in determining:

- Assessing the likelihood and magnitude of misstatement (i.e., Where inherent risk is assessed on the spectrum of inherent risk); and
- Determining The reasons for the assessment given to the risks of material misstatement at the assertion level, and that the auditor’s further audit procedures in accordance with paragraph 18 are responsive to those reasons.

The interrelationships between the inherent risk factors are further explained in Appendix 1.

A67. The reasons for the auditor’s assessment of inherent risk at the assertion level may result from one or more of the inherent risk factors of estimation uncertainty, complexity, subjectivity or other inherent risk factors. For example:

- (a) Accounting estimates of expected credit losses are likely to be complex because the expected credit losses cannot be directly observed and may require the use of a complex model. The model may use a complex set of historical data and assumptions about future developments in a variety of entity specific scenarios that may be difficult to predict. Accounting estimates for expected credit losses are also likely to be subject to high estimation uncertainty and significant subjectivity in making judgments about future events or conditions. Similar considerations apply to insurance contract liabilities.

---

<sup>143</sup> ISA 315 (Revised 2019), paragraphs 31 and 34

<sup>144</sup> ISA 330, paragraph 7(b)

<sup>145</sup> ISA 315 (Revised 2019), paragraph 31(a)

- (b) An accounting estimate for an obsolescence provision for an entity with a wide range of different inventory types may require complex systems and processes, but may involve little subjectivity and the degree of estimation uncertainty may be low, depending on the nature of the inventory.
  - (c) Other accounting estimates may not be complex to make but may have high estimation uncertainty and require significant judgment, for example, an accounting estimate that requires a single critical judgment about a liability, the amount of which is contingent on the outcome of the litigation.
- A68. The relevance and significance of inherent risk factors may vary from one estimate to another. Accordingly, the inherent risk factors may, either individually or in combination, affect simple accounting estimates to a lesser degree and the auditor may identify fewer risks or assess inherent risk ~~at~~ close to the lower end of the spectrum of inherent risk.
- A69. Conversely, the inherent risk factors may, either individually or in combination, affect complex accounting estimates to a greater degree, and may lead the auditor to assess inherent risk at the higher end of the spectrum of inherent risk. For these accounting estimates, the auditor's consideration of the effects of the inherent risk factors is likely to directly affect the number and nature of identified risks of material misstatement, the assessment of such risks, and ultimately the persuasiveness of the audit evidence needed in responding to the assessed risks. Also, for these accounting estimates the auditor's application of professional skepticism may be particularly important.
- A70. Events occurring after the date of the financial statements may provide additional information relevant to the auditor's assessment of the risks of material misstatement at the assertion level. For example, the outcome of an accounting estimate may become known during the audit. In such cases, the auditor may assess or revise the assessment of the risks of material misstatement at the assertion level,<sup>146</sup> regardless of how the inherent risk factors affect susceptibility of assertions to misstatement relating to ~~degree to which~~ the accounting estimate, ~~was subject to, or affected by, estimation uncertainty, complexity, subjectivity or other inherent risk factors.~~ Events occurring after the date of the financial statements also may influence the auditor's selection of the approach to testing the accounting estimate in accordance with paragraph 18. For example, for a simple bonus accrual that is based on a straightforward percentage of compensation for selected employees, the auditor may conclude that there is relatively little complexity or subjectivity in making the accounting estimate, and therefore may assess inherent risk at the assertion level ~~at~~ close to the lower end of the spectrum of inherent risk. The payment of the bonuses subsequent to period end may provide sufficient appropriate audit evidence regarding the assessed risks of material misstatement at the assertion level.

---

<sup>146</sup> ISA 315 (Revised 2019), paragraph ~~37~~34

A71. The auditor's assessment of control risk may be done in different ways depending on preferred audit techniques or methodologies. The control risk assessment may be expressed using qualitative categories (for example, control risk assessed as maximum, moderate, minimum) or in terms of the auditor's expectation of how effective the control(s) is in addressing the identified risk, that is, the planned reliance on the effective operation of controls. For example, if control risk is assessed as maximum, the auditor contemplates no reliance on the effective operation of controls. If control risk is assessed at less than maximum, the auditor contemplates reliance on the effective operation of controls.

*Estimation Uncertainty* (Ref: Para. 16(a))

A72. In taking into account the degree to which the accounting estimate is subject to estimation uncertainty, the auditor may consider:

- Whether the applicable financial reporting framework requires:
  - The use of a method to make the accounting estimate that inherently has a high level of estimation uncertainty. For example, the financial reporting framework may require the use of unobservable inputs.
  - The use of assumptions that inherently have a high level of estimation uncertainty, such as assumptions with a long forecast period, assumptions that are based on data that is unobservable and are therefore difficult for management to develop, or the use of various assumptions that are interrelated.
  - Disclosures about estimation uncertainty.
- The business environment. An entity may be active in a market that experiences turmoil or possible disruption (for example, from major currency movements or inactive markets) and the accounting estimate may therefore be dependent on data that is not readily observable.
- Whether it is possible (or practicable, insofar as permitted by the applicable financial reporting framework) for management:
  - To make a precise and reliable prediction about the future realization of a past transaction (for example, the amount that will be paid under a contingent contractual term), or about the incidence and impact of future events or conditions (for example, the amount of a future credit loss or the amount at which an insurance claim will be settled and the timing of its settlement); or
  - To obtain precise and complete information about a present condition (for example, information about valuation attributes that would reflect the perspective of market participants at the date of the financial statements, to develop a fair value estimate).

- A73. The size of the amount recognized or disclosed in the financial statements for an accounting estimate is not, in itself, an indicator of its susceptibility to misstatement because, for example, the accounting estimate may be understated.
- A74. In some circumstances, the estimation uncertainty may be so high that a reasonable accounting estimate cannot be made. The applicable financial reporting framework may preclude recognition of an item in the financial statements, or its measurement at fair value. In such cases, there may be risks of material misstatement that relate not only to whether an accounting estimate should be recognized, or whether it should be measured at fair value, but also to the reasonableness of the disclosures. With respect to such accounting estimates, the applicable financial reporting framework may require disclosure of the accounting estimates and the estimation uncertainty associated with them (see paragraphs A112–A113, A143–A144).
- A75. In some cases, the estimation uncertainty relating to an accounting estimate may cast significant doubt about the entity’s ability to continue as a going concern. ISA 570 (Revised)<sup>147</sup> establishes requirements and provides guidance in such circumstances.

*Complexity or Subjectivity* (Ref: Para. 16(b))

The Degree to Which Complexity Affects the Selection and Application of the Method

- A76. In taking into account the degree to which the selection and application of the method used in making the accounting estimate are affected by complexity, the auditor may consider:
- The need for specialized skills or knowledge by management which may indicate that the method used to make an accounting estimate is inherently complex and therefore the accounting estimate may have a greater susceptibility to material misstatement. There may be a greater susceptibility to material misstatement when management has developed a model internally and has relatively little experience in doing so, or uses a model that applies a method that is not established or commonly used in a particular industry or environment.
  - The nature of the measurement basis required by the applicable financial reporting framework, which may result in the need for a complex method that requires multiple sources of historical and forward-looking data or assumptions, with multiple interrelationships between them. For example, an expected credit loss provision may require judgments about future credit repayments and other cash flows, based on consideration of historical experience data and the application of forward looking assumptions. Similarly, the valuation of an insurance contract liability may require judgments about future insurance contract payments to be projected based on historical

---

<sup>147</sup> ISA 570, (Revised), *Going Concern*

experience and current and assumed future trends.

#### The Degree to Which Complexity Affects the Selection and Application of the Data

A77. In taking into account the degree to which the selection and application of the data used in making the accounting estimate are affected by complexity, the auditor may consider:

- The complexity of the process to derive the data, taking into account the relevance and reliability of the data source. Data from certain sources may be more reliable than from others. Also, for confidentiality or proprietary reasons, some external information sources will not (or not fully) disclose information that may be relevant in considering the reliability of the data they provide, such as the sources of the underlying data they used or how it was accumulated and processed.
- The inherent complexity in maintaining the integrity of the data. When there is a high volume of data and multiple sources of data, there may be inherent complexity in maintaining the integrity of data that is used to make an accounting estimate.
- The need to interpret complex contractual terms. For example, the determination of cash inflows or outflows arising from a commercial supplier or customer rebates may depend on very complex contractual terms that require specific experience or competence to understand or interpret.

#### The Degree to Which Subjectivity Affects the Selection and Application of the Method, Assumptions or Data

A78. In taking into account the degree to which the selection and application of method, assumptions or data are affected by subjectivity, the auditor may consider:

- The degree to which the applicable financial reporting framework does not specify the valuation approaches, concepts, techniques and factors to use in the estimation method.
- The uncertainty regarding the amount or timing, including the length of the forecast period. The amount and timing is a source of inherent estimation uncertainty, and gives rise to the need for management judgment in selecting a point estimate, which in turn creates an opportunity for management bias. For example, an accounting estimate that incorporates forward looking assumptions may have a high degree of subjectivity which may be susceptible to management bias.

#### *Other Inherent Risk Factors* (Ref: Para. 16(b))

A79. The degree of subjectivity associated with an accounting estimate influences the susceptibility of the accounting estimate to misstatement due to management bias or ~~fraud~~ other fraud risk factors insofar as they affect inherent risk. For example, when

an accounting estimate is subject to a high degree of subjectivity, the accounting estimate is likely to be more susceptible to misstatement due to management bias or fraud and this may result in a wide range of possible measurement outcomes. Management may select a point estimate from that range that is inappropriate in the circumstances, or that is inappropriately influenced by unintentional or intentional management bias, and that is therefore misstated. For continuing audits, indicators of possible management bias identified during the audit of preceding periods may influence the planning and risk assessment procedures in the current period.

*Significant Risks* (Ref: Para. 17)

A80. The auditor's assessment of inherent risk, which takes into account the degree to which an accounting estimate is subject to, or affected by estimation uncertainty, complexity, subjectivity or other inherent risk factors, assists the auditor in determining whether any of the risks of material misstatement identified and assessed are a significant risk.

...

*When the Auditor Intends to Rely on the Operating Effectiveness of ~~Relevant~~ Controls*  
(Ref: Para: 19)

A85. Testing the operating effectiveness of ~~relevant~~ controls may be appropriate when inherent risk is assessed as higher on the spectrum of inherent risk, including for significant risks. This may be the case when the accounting estimate is subject to or affected by a high degree of complexity. When the accounting estimate is affected by a high degree of subjectivity, and therefore requires significant judgment by management, inherent limitations in the effectiveness of the design of controls may lead the auditor to focus more on substantive procedures than on testing the operating effectiveness of controls.

...

**Overall Evaluation Based on Audit Procedures Performed** (Ref: Para. 33)

...

*Determining Whether the Accounting Estimates are Reasonable or Misstated* (Ref: Para. 9, 35)

...

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

**Requirements**

## Understanding the Group, Its Components and Their Environments

17. The auditor is required to identify and assess the risks of material misstatement through obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the system of internal control.<sup>148</sup> The group engagement team shall:

(a) ...

## Application and Other Explanatory Material

...

### Definitions

...

*Significant Component* (Ref: Para. 9(m))

...

A6. The group engagement team may also identify a component as likely to include significant risks of material misstatement of the group financial statements due to its specific nature or circumstances, ~~(that is, risks that require special audit consideration<sup>149</sup>)~~. For example, a component could be responsible for foreign exchange trading and thus expose the group to a significant risk of material misstatement, even though the component is not otherwise of individual financial significance to the group.

...

## Understanding the Group, Its Components, and Their Environments

*Matters about Which the Group Engagement Team Obtains an Understanding* (Ref: Para. 17)

A23. ISA 315 (Revised 2019) contains guidance on matters the auditor may consider when obtaining an understanding of the industry, regulatory, and other external factors that affect the entity, including the applicable financial reporting framework; the nature of the entity; objectives and strategies and related business risks; and measurement and review of the entity's financial performance.<sup>150</sup> Appendix 2 of this ISA contains guidance on matters specific to a group including the consolidation process.

---

<sup>148</sup> ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment*.

<sup>149</sup> ISA 315 (Revised), paragraphs 27–29

<sup>150</sup> ISA 315 (Revised 2019), paragraphs A6.225–A6.449 and Appendix J

## Appendix 2

### Examples of Matters about Which the Group Engagement Team Obtains an Understanding

...

#### Group-Wide Controls

1. Group-wide controls may include a combination of the following:
  - Regular meetings between group and component management to discuss business developments and to review performance.
  - ...
  - Controls ~~activities~~ within an IT system that is common for all or some components.
  - ~~Controls within the group's process to monitor~~ Monitoring the system of internal controls, including activities of the internal audit function and self-assessment programs.
  - ...

## Appendix 5

### Required and Additional Matters Included in the Group Engagement Team's Letter of Instruction

Matters that are relevant to the planning of the work of the component auditor:

- ...
- ...

Matters that are relevant to the conduct of the work of the component auditor:

- The findings of the group engagement team's tests of controls ~~activities~~ of a processing system that is common for all or some components, and tests of controls to be performed by the component auditor.
- ...

### ISA 610 (Revised 2013), *Using the Work of Internal Auditors*

#### Introduction

...

Relationship between ISA 315 (Revised 2019) and ISA 610 (Revised 2013)

...

7. ISA 315 (Revised 2019) addresses how the knowledge and experience of the internal audit function can inform the external auditor's understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control, and identification and assessment of risks of material misstatement. ISA 315 (Revised 2019)<sup>151</sup> also explains how effective communication between the internal and external auditors also creates an environment in which the external auditor can be informed of significant matters that may affect the external auditor's work.

...

## **Application and Other Explanatory Material**

### **Definition of Internal Audit Function (Ref: Para. 2, 14(a))**

...

- A3. In addition, those in the entity with operational and managerial duties and responsibilities outside of the internal audit function would ordinarily face threats to their objectivity that would preclude them from being treated as part of an internal audit function for the purpose of this ISA, although they may perform controls ~~activities~~ that can be tested in accordance with ISA 330.<sup>12</sup> For this reason, monitoring controls performed by an owner-manager would not be considered equivalent to an internal audit function.

...

### *Evaluating the Internal Audit Function*

...

### **Application of a Systematic and Disciplined Approach (Ref: Para. 15(c))**

- A10. The application of a systematic and disciplined approach to planning, performing, supervising, reviewing and documenting its activities distinguishes the activities of the internal audit function from other monitoring controls ~~activities~~ that may be performed within the entity.

...

- A21. As explained in ISA 315 (Revised 2019),<sup>152</sup> significant risks ~~require special audit consideration~~ are risks assessed close to the upper end of the spectrum of inherent risk and therefore the external auditor's ability to use the work of the internal audit

---

<sup>151</sup> ISA 315 (Revised 2019), paragraph 24(a)(ii)(e) and Appendix 4

<sup>152</sup> ISA 315 (Revised 2019), paragraph 4(e)~~12(d)~~

function in relation to significant risks will be restricted to procedures that involve limited judgment. In addition, where the risks of material misstatement is other than low, the use of the work of the internal audit function alone is unlikely to reduce audit risk to an acceptably low level and eliminate the need for the external auditor to perform some tests directly.

...

## ***ISA 620, Using the Work of an Auditor's Expert***

### **Application and Other Explanatory Material**

...

#### **Determining the Need for an Auditor's Expert (Ref: Para.7)**

A4. An auditor's expert may be needed to assist the auditor in one or more of the following:

- Obtaining an understanding of the entity and its environment the applicable financial reporting framework and the, including its entity's system of internal control.
- ...

## ***ISA 701, Communicating Key Audit Matters in eth Independent Auditor's Report***

### **Application and Other Explanatory Material**

...

#### **Determining Key Audit Matters (Ref: Para.9–10)**

...

*Considerations in Determining Those Matters that Required Significant Auditor Attention*  
(Ref: Para.9)

...

Areas of Higher Assessed Risk of Material Misstatement, or Significant Risks Identified in Accordance with ISA 315 (Revised 2019) (Ref: Para. 9(a))

...

A20. ISA 315 (Revised 2019) defines a significant risk as an identified ~~and assessed~~ risk of material misstatement for which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk due to the degree to which the

~~inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur that, in the auditor's judgment, requires special audit consideration.~~<sup>153</sup> Areas of significant management judgment and significant unusual transactions may often be identified as significant risks. Significant risks are therefore often areas that require significant auditor attention.

...

## **ISA 720 (Revised), *The Auditor's Responsibilities Relating to Other Information***

### **Application and Other Explanatory Material**

...

#### **Reading and Considering the Other Information (Ref: Para. 14–15)**

...

*Considering Whether There Is a Material Inconsistency between the Other Information and the Auditor's Knowledge Obtained in the Audit (Ref: Para. 14(b))*

...

A31. The auditor's knowledge obtained in the audit includes the auditor's understanding of the entity and its environment, ~~the applicable financial reporting framework, and including~~ the entity's system of internal control, obtained in accordance with ISA 315 (Revised 2019).<sup>154</sup> ISA 315 (Revised 2019) sets out the auditor's required understanding, which includes such matters as obtaining an understanding of:

- (a) ~~The entity's organizational structure, ownership and governance, and its business model, including the extent to which the business model integrates the use of IT;~~
- (b) ~~The r~~Relevant industry, regulatory, and other external factors;
- (c) ~~The relevant measures used, internally and externally, to assess measurement and review of the entity's financial performance; and~~
- (b) ~~The nature of the entity;–~~
- (e) ~~The entity's selection and application of accounting policies;–~~

---

<sup>153</sup> ISA 315 (Revised 2019), paragraph 12(l)

<sup>154</sup> ~~ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment*, paragraphs 1911–2712~~

- (d) ~~The entity's objectives and strategies;~~

...

### **Responding When a Material Misstatement in the Financial Statements Exists or the Auditor's Understanding of the Entity and Its Environment Needs to Be Updated**

(Ref: Para. 20)

A51. In reading the other information, the auditor may become aware of new information that has implications for:

- The auditor's understanding of the entity and its environment, the financial reporting framework and the entity's system of internal control and, accordingly, may indicate the need to revise the auditor's risk assessment.<sup>155</sup>
- ...

---

<sup>155</sup> ISA 315 (Revised 2019), paragraphs 41-31 and A1-19-26 and 37



MALAYSIAN INSTITUTE  
OF ACCOUNTANTS

Dewan Akauntan, Unit 33-01, Level 33, Tower A, The Vertical, Avenue 3  
Bangsar South City, No.8, Jalan Kerinchi, 59200 Kuala Lumpur, Malaysia  
[phone] +603 2722 9000 [fax] +603 2722 9100  
[web] [www.mia.org.my](http://www.mia.org.my) [email] [technical@mia.org.my](mailto:technical@mia.org.my)