Agenda Item 1-B presents the Exposure Draft of ISA 315 (Revised) for reference purposes only. The final version of this proposed standard will be published with the Explanatory Memorandum in mid-July 2018.

PROPOSED INTERNATIONAL STANDARD ON AUDITING 315 (REVISED)
IDENTIFYING AND ASSESSING THE RISKS OF MATERIAL MISSTATEMENT

(Effective for audits of financial statements for periods beginning on or after December 15, 2020)

CONTENTS

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

Introduction

Scope of this ISA

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

Key Concepts in this ISA

2. ISA 200 deals with the overall objectives of the auditor in conducting an audit of the financial statements,[1] including to obtain sufficient appropriate audit evidence to reduce audit risk to an acceptably low level.[2] Audit risk is a function of the risks of material misstatement and detection risk. ISA 200 explains that the risks of material misstatement may exist at two levels:[3] the overall financial statement level; and the assertion level for classes of transactions, account balances and disclosures. ISA 200 further requires the auditor to exercise professional judgment in planning and performing an audit, and to plan and perform an audit with professional skepticism recognizing that circumstances may exist that cause the financial statements to be materially misstated.[4]

3. 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 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 controls.

4. The required understanding of the entity and the environment, the applicable financial reporting framework, and the system of internal control forms the basis for the auditor's identification of risks of material misstatement. The identification of risks of material misstatement at the assertion level is performed before consideration of any controls. The auditor does so based on a preliminary assessment of inherent risk that involves identifying those risks for which there is a reasonable possibility of material misstatement. In this ISA the assertions to which such risks of material misstatement relate are referred to as 'relevant assertions,' and the classes of transactions, account balances and disclosures to which the relevant assertions relate are referred to as 'significant classes of transactions, account balances and disclosures.'

5. For the identified risks of material misstatement at the assertion level, a separate assessment of inherent risk and control risk is required by this ISA. The auditor assesses the inherent risk by assessing the likelihood and magnitude of material misstatement, and by taking into account inherent risk factors. Inherent risk factors individually or in combination increase inherent risk to varying degrees. As explained in ISA 200, inherent risk is higher for some assertions and related classes of

---

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

2 ISA 200, paragraph 17

3 ISA 200, paragraphs 13(c) and 13(n)

4 ISA 200, paragraphs 15–16

transactions, account balances and disclosures than for others. The degree to which inherent risk varies, is referred to in this ISA as the 'spectrum of inherent risk.'

6. 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 (that is, control risk is assessed as less than maximum). The auditor's understanding of the system of internal control forms the basis for the auditor's intentions about whether to place reliance on the operating effectiveness of controls. That is, the auditor may identify specific controls that address the identified risks of material misstatement and for which the auditor intends to test operating effectiveness. If the auditor does not intend to test the operating effectiveness of controls related to certain identified risks of material misstatement,, the auditor's assessment of control risk cannot be reduced for the effective operation of controls with respect to the particular assertion (that is, control risk is assessed at maximum).

7. The auditor's assessment of the risks of material misstatement at the assertion level is based on the auditor's assessments of inherent risk and control risk at the assertion level. The auditor designs and performs further audit procedures whose nature, timing and extent are responsive to the assessed risks of material misstatement at the assertion level. The auditor also identifies and assesses the risks of material misstatement at the financial statement level in accordance with this ISA in order to design and implement overall responses to address such risks.

8. 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 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.

The iterative nature of the auditor's risk assessment process

9. The auditor's risk assessment process is iterative and dynamic. The auditor develops initial expectations about the potential risks of material misstatement and the potential significant classes of transactions, account balances and disclosures based on the auditor's understanding of the entity and its environment and the applicable financial reporting framework. The auditor's understanding of the system of the internal control, and in particular the information system component, provides further information to assist the auditor in developing those expectations.

10. After identifying the risks of material misstatement, the auditor determines the significant classes of transactions, account balances and disclosures. The auditor is also required to perform a stand-back to confirm that this identification is appropriate.

11. The auditor's process of assessing the identified risks of material misstatement at the assertion level also results in the auditor's determination of any significant risks and risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence.

12. This ISA requires 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, or if new information is obtained.

Scalability

13. ISA 200 states that the ISAs include considerations specific to smaller entities within the application and explanatory material.[5] This ISA is intended for audits of all entities, regardless of size or complexity. However, the application material of this ISA incorporates considerations specific to audits of smaller entities when such entities are also less complex. Accordingly, in this context, this ISA refers to 'smaller and less complex entities.' 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. Some of the considerations however may be useful in audits of larger and less complex entities.

Effective Date

14. This ISA is effective for audits of financial statements for periods beginning on or after December 15, 2020.

Objective

15. 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

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

    (a) Application controls – Controls of a preventative or detective nature that support the initiation, recording, processing and reporting of transactions or other information in the entity's information system, the objectives of which are to maintain the reliability of such transactions and other information. Such controls may rely on information, or other controls that maintain the integrity of information, or may rely on the operation of other controls.

    (b) 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 in responding to the risks of material misstatement. (Ref. Para: A1–A2).

    (c) 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.

    (d) Controls – Policies or procedures that are embedded within the components of the system of internal control to achieve the control objectives of management or those charged with governance. In this context:

        - 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.
        - Procedures are actions to implement policies. (Ref: Para. A3–A4)

[5] ISA 200, paragraphs 66 - 68

(e) General information technology (IT) controls – Controls related to the IT environment that support the effective functioning of application controls or the integrity of information by helping to maintain the continued operation, as designed, of the entity's information system. General IT controls include controls over the entity's IT processes. Also see the definition of *IT environment*

(f) Inherent Risk Factors – Characteristics of events or conditions that affect susceptibility to misstatement 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 fraud. (Ref: Para A5–A6)

(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:

- 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.
- The IT infrastructure is comprised of the network, operating systems, and databases and their related hardware and software.
- 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, which includes monitoring the IT environment. (Ref: Para: A7–A8)

(h) Relevant assertions – An assertion is relevant to a class of transactions, account balance or disclosure when the nature or circumstances of that item are such that there is a reasonable possibility of occurrence of a misstatement with respect to that assertion that is material, individually or in combination with other misstatements. There is such possibility when the likelihood of a material misstatement is more than remote. The determination of whether an assertion is a relevant assertion is made before consideration of controls. (Ref: Para. A9)

(i) 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.

(j) 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.

(k) Significant risk – An identified 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 one or a combination of the inherent risk factors affect the likelihood of a misstatement occurring or the magnitude of potential misstatement should that misstatement occur; or
- That is to be treated as a significant risk in accordance with the requirements of other ISAs.[6] (Ref: Para. A10)

[6] ISA 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*, paragraph 27 and ISA 550, *Related Parties*, paragraph 18

(l) 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: (Ref: Para. A11)

- Control environment.
- The entity's risk assessment process.
- The entity's process to monitor the system of internal control.
- The information system and communication.
- Control activities.

Requirements

Risk Assessment Procedures and Related Activities

17. The auditor shall design and perform risk assessment procedures to obtain an understanding of:

- The entity and its environment in accordance with paragraph 23(a);
- The applicable financial reporting framework in accordance with paragraph 23(b); and
- The entity's system of internal control in accordance with paragraphs 25–44

to obtain sufficient appropriate audit evidence as the basis for the identification and assessment of risks of material misstatement at the financial statement and assertion levels. Risk assessment procedures by themselves, however, do not provide sufficient appropriate audit evidence on which to base the audit opinion. (Ref: Para. A12–A16)

18. The risk assessment procedures shall include the following: (Ref: Para A17–A20)

(a) Inquiries of management, of appropriate individuals within the internal audit function (if the function exists), and of others within the entity who in the auditor's judgment may have information that is likely to assist in identifying risks of material misstatement due to fraud or error. (Ref: Para. A21–A29)

(b) Analytical procedures. (Ref: Para. A30–A34)

(c) Observation and inspection. (Ref: Para A35–A36)

19. The auditor, in identifying and assessing the risks of material misstatement, shall take into account information obtained from the auditor's acceptance or continuance of the client relationship or the audit engagement. (Ref: Para. A37)

20. If the engagement partner has performed other engagements for the entity, the engagement partner shall consider whether information obtained is relevant to identifying and assessing risks of material misstatement. (Ref: Para. A38)

21. Where 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–A40)

22. The engagement partner and other key engagement team members shall discuss the application of the applicable financial reporting framework in the context of the nature and circumstances of the entity and its environment, and the susceptibility of the entity's financial statements to material misstatement. The engagement partner shall determine which matters are to be communicated to engagement team members not involved in the discussion. (Ref: Para. A41–A46)

Obtaining an Understanding of the Entity and Its Environment and the Applicable Financial Reporting Framework (Ref: Para. A47–A48)

23. The auditor shall perform risk assessment procedures to obtain an understanding of the entity and its environment and the applicable financial reporting framework. In doing so, the auditor shall obtain an understanding of the following matters to provide an appropriate basis for understanding the classes of transactions, account balances and disclosures to be expected in the entity's financial statements:

    (a) The entity and its environment, including:

        (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 A49–A63)

        (ii) Relevant industry, regulatory and other external factors; and (Ref: Para. A64–A69)

        (iii) The relevant measures used, internally and externally, to assess the entity's financial performance. (Ref: Para. A70–A78)

    (b) The applicable financial reporting framework, including: (Ref: Para.A79–A82)

        (i) How it applies in the context of the nature and circumstances of the entity and its environment, including how events or conditions are subject to, or affected by, the inherent risk factors; and (Ref: Para.A83–A88)

        (ii) The entity's accounting policies and any changes thereto, including the reasons for any such changes.

24. The auditor shall evaluate whether the entity's accounting policies, and any changes thereto, are appropriate in the context of the nature and circumstances of the entity and its environment, and consistent with the applicable financial reporting framework.

Obtaining an Understanding of the Entity's System of Internal Control

25. The auditor shall perform risk assessment procedures to obtain an understanding of the entity's system of internal control relevant to financial reporting, including the entity's use of IT, by understanding each of the components of internal control. For this purpose, the auditor shall address the requirements set out in paragraphs 27 to 38 of this ISA. (Ref: Para. A89–A103)

26. The auditor shall identify controls relevant to the audit, and shall evaluate the design of such controls and determine whether the controls have been implemented in accordance with the requirements set out in paragraphs 39 to 42. (Ref. Para. A104)

Components of the Entity's System of Internal Control

Control Environment

27. The auditor shall obtain an understanding of the control environment relevant to financial reporting, including understanding how the entity: (Ref: Para. A105–A110)

    (a) Demonstrates a commitment to integrity and ethical values;

    (b) When those charged with governance are separate from management, demonstrates that those charged with governance are independent of management and exercise oversight of the entity's system of internal control;

    (c) Establishes, with the oversight of those charged with governance, structures, reporting lines, and appropriate authorities and responsibilities, in pursuit of its objectives;

    (d) Demonstrates a commitment to attract, develop, and retain competent individuals in alignment with its objectives; and

    (e) Holds individuals accountable for their responsibilities in the pursuit of the objectives of the system of internal control.

28. Based on the auditor's understanding of the control environment in accordance with paragraph 27, the auditor shall evaluate whether: (Ref: Para. A111–A114)

    (a) Management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior; and

    (b) The strengths in those areas of the entity's control environment addressed in paragraphs 27(a) to (e) collectively provide an appropriate foundation for the other components of the system of internal control, or whether those other components are undermined by control deficiencies in the control environment component.

The Entity's Risk Assessment Process (Ref: Para. A115–A116)

29. The auditor shall obtain an understanding of the entity's risk assessment process, including the extent to which it is formalized, by understanding: (Ref: Para. A117–119)

    (a) Whether, and if so, how, the entity's process:

        (i) Identifies business risks relevant to financial reporting objectives;

        (ii) Assesses the significance of those risks, including the likelihood of their occurrence; and

        (iii) Addresses those risks.

    (b) The results of the entity's process.

30. If the auditor identifies risks of material misstatement that management failed to identify, the auditor shall evaluate whether any such risks are of a kind that the auditor expects would have been identified by the entity's risk assessment process. If so, the auditor shall obtain an understanding of why the entity's risk assessment process failed to identify such risks of material misstatement, and consider the implications for the auditor's evaluation required by paragraph 31.

31. Based on the auditor's understanding of the entity's risk assessment process in accordance with paragraph 29, and if applicable, paragraph 30, the auditor shall: (Ref: Para. A120–A121)

(a) Evaluate whether the nature of the entity's risk assessment process, including its formality, is appropriate to the entity's circumstances considering the nature and size of the entity; and

(b) If not, determine whether the lack of an appropriate risk assessment process represents one or more control deficiencies.

The entity's process to monitor the system of internal control (Ref: Para. A122–A125)

32. The auditor shall obtain an understanding of the entity's process to monitor the system of internal control, including the extent to which it is formalized, by understanding how the entity's process: (Ref: Para. A126–A128)

(a) Monitors the effectiveness of controls; and

(b) Addresses the identification and remediation of control deficiencies, including those related to the entity's risk assessment process.

33. The auditor shall obtain an understanding of the sources of the information used in the entity's process to monitor the system of internal control, and the basis upon which management considers the information to be sufficiently reliable for the purpose. (Ref: Para. A129–A130)

34. If the entity has an internal audit function,[7] the auditor shall obtain an understanding of the nature of the internal audit function's responsibilities, its organizational status, and the activities performed, or to be performed. (Ref: Para. A131–A135)

The Information System and Communication

35. The auditor shall obtain an understanding of the information system relevant to financial reporting, including the related business processes, through understanding: (Ref: Para. A136–A141)

(a) How information relating to significant classes of transactions, account balances and disclosures flows through the entity's information system, whether manually or using IT, and whether obtained from within or outside of the general ledger and subsidiary ledgers. This understanding shall include how: (Ref: Para. A142–A143)

(i) Transactions 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 and conditions, other than transactions, is captured, processed and disclosed in the financial statements.

(b) The accounting records, specific accounts in the financial statements and other supporting records relating to the flows of information in paragraph 35(a);

(c) The financial reporting process used to prepare the entity's financial statements from the records described in paragraph 35(b), including as it relates to disclosures and to accounting estimates relating to significant classes of transactions, account balances and disclosures;

(d) The entity's IT environment relevant to (a) through (c) above. (Ref: Para. A144–A150 and Para. A180–A182)

[7] ISA 610 (Revised 2013), *Using the Work of Internal Auditors*, paragraph 14(a), defines the term "internal audit function" for purposes of the ISA.

36. The auditor shall evaluate the design of the information system controls relevant to financial reporting, by understanding how the matters in paragraph 35(a)–(d) are addressed by the entity, and implemented. (Ref: Para. A151–A157)

37. The auditor shall obtain an understanding of how the entity communicates financial reporting roles and responsibilities and significant matters relevant to financial reporting, including: (Ref: Para. A158–A159)

    (a) Communications between management and those charged with governance; and

    (b) External communications, such as those with regulatory authorities.

Control Activities

38. The auditor shall obtain an understanding of the control activities component by identifying the controls relevant to the audit in the control activities component in accordance with the requirements of paragraphs 39 through 41, and by evaluating their design and determining whether they have been implemented in accordance with paragraph 42. (Ref: Para. A160–A165)

Controls relevant to the audit

39. The auditor shall identify controls relevant to the audit, being those: (Ref: Para. A166–A167)

    (a) That address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence; (Ref: Para. A168)

    (b) That address risks that are identified as a significant risk; (Ref: Para. A169–A173)

    (c) Over journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments; (Ref: Para. A174–A175)

    (d) Controls for which the auditor plans to test the operating effectiveness in determining the nature, timing and extent of substantive testing; or (Ref: Para. A176–A178)

    (e) That, in the auditor's professional judgment, are appropriate to evaluate their design and determine whether they have been implemented to enable the auditor to: (Ref: Para. A179)

        (i) Identify and assess the risks of material misstatement at the assertion level; or

        (ii) Design further audit procedures responsive to assessed risks.

    Not all controls that are relevant to financial reporting are relevant to the audit. It is a matter of the auditor's professional judgment as to whether a control, individually or in combination with other controls, is identified as being relevant to the audit.

40. Based on the understanding obtained in accordance with paragraph 35(d), and the identification of the controls relevant to the audit in accordance with paragraph 39, the auditor shall identify the IT applications and the other aspects of the entity's IT environment that are relevant to the audit. In doing so, the auditor shall take into account whether the IT applications include or address: (Ref: Para. A180–A188)

    (a) Automated controls that management is relying on and that the auditor has determined to be relevant to the audit;

    (b) Maintenance of the integrity of information stored and processed in the information system that relates to significant classes of transactions, account balances or disclosures;

(c) System-generated reports on which the auditor intends to rely on without directly testing the inputs and outputs of such reports; or

(d) Controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.

41. For the IT applications and other aspects of the IT environment that are relevant to the audit, the auditor shall identify: (Ref: Para. A189–A193)

(a) The risks arising from the use of IT; and

(b) The general IT controls relevant to the audit.

42. For each control identified as relevant to the audit in accordance with paragraphs 39 and 41, the auditor shall: (Ref: Para. A194–A200)

(a) Evaluate 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

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

Control Deficiencies Within the System of Internal Control

43. The auditor shall, in accordance with ISA 265,[8] determine on the basis of the work performed in accordance with this ISA:

(a) Whether one or more control deficiencies within the system of internal control have been identified; and

(b) If so, whether the control deficiencies, individually or in combination, constitute significant control deficiencies.

44. The auditor shall consider the implications for the audit of one or more control deficiencies in the system of internal control, including for:

- The assessment of control risk for risks of material misstatement at the assertion level in accordance with paragraph 50; and
- Designing and implementing overall responses to address the assessed risks of material misstatement as required by ISA 330.[9]

Identifying and Assessing the Risks of Material Misstatement

45. The auditor shall identify the risks of material misstatement and determine whether they exist at: (Ref: Para. A201–A210)

(a) The financial statement level, by evaluating whether the identified risks relate more pervasively to the financial statements as a whole, including potentially affecting many assertions; or (Ref: Para. A207)

(b) The assertion level for classes of transactions, account balances, and disclosures, taking into account the inherent risk factors. (Ref. Para. A208)

---

[8] ISA 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*, paragraphs 7–8

[9] ISA 330, *The Auditor's Responses to Assessed Risks,* paragraph 5

46. The auditor shall determine significant classes of transactions, account balances and disclosures, and their relevant assertions, based on the identified risks of material misstatement. (Ref. Para. A211 – A214)

Assessing Risks of Material Misstatement at the Financial Statement Level

47. The auditor shall assess the identified risks of material misstatement at the financial statement level by: (Ref: Para. A215–A220)

    (a) Determining how, and the degree to which, such risks affect the assessment of risks of material misstatement at the assertion level (Ref: Para. A227), and

    (b) Evaluating the nature and extent of their pervasive effect on the financial statements to provide the basis for designing and implementing overall responses to the identified risk of material misstatement at the financial statement level in accordance with ISA 330.[10] (Ref: Para A216)

Assessing Risks of Material Misstatement at the Assertion Level

Assessing Inherent Risk

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

    (a) Identified events and conditions relating to significant classes of transactions, account balances and disclosures are subject to, or affected by, the inherent risk factors. (Ref: Para. A221–A228)

    (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. A216 and A227)

49. The auditor shall determine, based on the auditor's assessment of inherent risk, whether any of the assessed risks of material misstatement are significant risks. (Ref: Para. A229–A231)

Assessing Control Risk

50. For identified risks of material misstatement at the assertion level, the auditor shall assess control risk as follows: (Ref: Para. A232–A235)

    (a) When the auditor plans to test the operating effectiveness of controls in designing further audit procedures to be performed to respond to a risk of material misstatement at the assertion level, the auditor shall assess control risk at less than maximum. In doing so, the auditor shall take into account whether the design, implementation and expected operating effectiveness of such controls support the auditor's intended reliance thereon.

    (b) When the auditor does not plan to test the operating effectiveness of controls in designing further audit procedures to be performed to respond to a risk of material misstatement at the assertion level, the auditor shall assess control risk at the maximum.

[10] ISA 330, paragraph 5

Risks for Which Substantive Procedures Alone Cannot Provide Sufficient Appropriate Audit Evidence

51. The auditor shall determine, for any of the risks of material misstatement at the assertion level, whether substantive procedures alone cannot provide sufficient appropriate audit evidence (Ref: Para. A236–A239)

Classes of Transactions, Account Balances and Disclosures that are Not Significant, but which are Material

52. The auditor shall: (Ref: Para. A240–A242)

    (a) Identify the classes of transactions, account balances and disclosures that are quantitatively or qualitatively material, and that have not been identified as significant classes of transactions, account balances or disclosures in accordance with paragraph 46; and

    (b) Evaluate whether the auditor's conclusion that there are no relevant assertions (that is, no related risks of material misstatement) for these classes of transactions, account balances and disclosures remains appropriate.

Revision of Risk Assessment

53. The auditor's assessments of the risks of material misstatement at the financial statement level and assertion level may change during the course of the audit as additional audit evidence is obtained. In circumstances where the auditor obtains audit evidence from performing further audit procedures, or if new information is obtained, either of which is inconsistent with the audit evidence on which the auditor originally based the identification and assessments of the risks of material misstatement, the auditor shall revise the assessment and modify the planned overall responses or further audit procedures accordingly. (Ref: Para. A243)

Documentation

54. The auditor shall include in the audit documentation:[11] (Ref: Para. A244–A247)

    (a) The discussion among the engagement team, where required in accordance with paragraph 22, and the significant decisions reached;

    (b) Key aspects of the auditor's understanding obtained regarding the entity and its environment specified in paragraph 23 and of each of the components of the system of internal control specified in paragraphs 27, 29, 32 through 38; the sources of information from which the auditor's understanding was obtained; and the risk assessment procedures performed;

    (c) The controls identified to be relevant to the audit in accordance with the requirements in paragraphs 39 and 41.

    (d) The identified and assessed risks of material misstatement at the financial statement level and at the assertion level as required by paragraph 45 through 51, including significant risks, and the rationale for the significant judgments made in identifying and assessing the risks of material misstatement. (Ref: Para A245)

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

Application and Other Explanatory Material

Definitions

Assertions (Ref: Para. 16(b))

A1. Representations by management with respect to the recognition, measurement, presentation and disclosure of information in the financial statements of classes of transactions, account balances and disclosures differ from written representations provided to the auditor by management, as required by ISA 580,[12] to confirm certain matters or support other audit evidence.

A2. Assertions that the auditor may use in addressing the requirements of this ISA are further described in paragraph A204.

Controls (Ref: Para. 16(d))

A3. Policies are implemented through the actions of personnel within the entity, or through their restraint 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.

Inherent Risk Factors (Ref: Para. 16(f))

A5. Inherent risk factors may be qualitative or quantitative and affect the susceptibility to misstatement of financial statement items. Qualitative 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 inter-related 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 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

[12] ISA 580, *Written Representations*

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 best available knowledge to prepare the information using sufficiently precise and comprehensive observable data, to the extent available, and reasonable assumptions supported by the best 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 fraud*— 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 inherent incentives or pressures (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 for assertions about classes of transactions, account balances and disclosures are described in paragraphs A1 to A5 of ISA 240.

A6. Other inherent risk factors, that affect susceptibility to misstatement of an assertion about a class of transactions, account balance or disclosure include:

- The quantitative or qualitative significance of the class of transactions, account balance or disclosure, and of the items in relation to performance materiality;
- The composition of the class of transactions, account balance or disclosure, including whether the items are subject to differing risks;
- The volume of activity and homogeneity of the individual transactions processed through the class of transactions or account balance or class of transactions, or reflected in the disclosure; or

- The existence of related party transactions in the class of transaction or account balance, or that are relevant to the disclosure.

IT Environment (Ref: Para 16(g))

A7. IT applications may include data warehouses or report writers. A data warehouse is a central repository of integrated data from one or more disparate sources (such as multiple databases) from which reports may be generated or that may be used by the entity for other data analysis activities. A report-writer is an IT application that is used to extract data from one or more sources (such as a data warehouse, a database or an IT application) and present the data in a specified format.

A8. 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. The operating system is responsible for managing communications between hardware, IT applications, and other software used in the 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.

Relevant Assertions (Ref: Para. 16(h))

A9. There will be one or more risks of material misstatement that relate to a relevant assertion. A risk of material misstatement may relate to more than one assertion, in which case all the assertions to which such a risk relates would be relevant assertions

Significant Risk (Ref: Para. 16(k))

A10. Significance can be described as the relative importance of a matter, taken in context. The significance of a matter is judged by the auditor in the context in which the matter is being considered. The significance of a risk of material misstatement at the assertion level is considered in the context of the implications of the assessment of its inherent risk for the performance of the audit, including the nature, timing and extent of the auditor's further audit procedures and the persuasiveness of the audit evidence that will be required to reduce audit risk to an acceptable level. Significance can be considered in the context of how, and the degree to which, the susceptibility to misstatement is subject to, or affected by, the inherent risk factors, which affect the likelihood that a misstatement will occur, as well as the potential magnitude of the misstatement were that misstatement to occur.

System of Internal Control (Ref: Para. 16(l))

A11. 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 system of internal control is implemented by management, those charged with governance, and other personnel based on the structure of the entity. The system of internal control can be applied, based on the decisions of management, those charged with governance and 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.

Risk Assessment Procedures and Related Activities (Ref: Para. 17–22)

Risk Assessment Procedures (Ref: Para. 17)

A12. 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. As the auditor performs audit procedures, the audit evidence obtained may cause the auditor to update the understanding on which the risk assessment was based and the nature, timing or extent of other planned audit procedures in accordance with ISA 330. For example, information gathered in understanding the entity's system of internal control assists the auditor in assessing control risk at the assertion level, such that control risk may be assessed at less than maximum based on an expectation about the operating effectiveness of the control(s) and the planned testing of such control(s). Information gathered when testing the operation of the control(s) as part of performing further audit procedures may indicate that the control(s) are not effective, and as a result the auditor's original assessment is updated in accordance with paragraph 53.

A13. 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 the risks of material misstatement due to fraud.[13] In addition, the following ISAs provide further requirements and guidance on identifying and assessing risks of material misstatement in regard to specific matters or circumstances:

- ISA 540 (Revised)[14] in regard to accounting estimates;
- ISA 550[15] in regard to related party relationships and transactions;
- ISA 570 (Revised)[16] in regard to going concern; and
- ISA 600[17] in regard to group financial statements.

A14. The understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control also establishes a frame of reference within which the auditor plans the audit and exercises professional judgment throughout the audit, for example, when:

- Identifying and assessing risks of material misstatement of the financial statements (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));
- Determining materiality or performance materiality in accordance with ISA 320;[18]
- Considering the appropriateness of the selection and application of accounting policies, and the adequacy of financial statement disclosures;

---

13 ISA 240, paragraphs 12–24

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

15 ISA 550, *Related Parties*

16 ISA 570 (Revised), *Going Concern*

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

18 ISA 320, *Materiality in Planning and Performing an Audit*, paragraphs 10–11

- Developing expectations for use when performing analytical procedures in accordance with ISA 520;[19]
- Responding to the assessed risks of material misstatement, including designing and performing further audit procedures to obtain sufficient appropriate audit evidence in accordance with ISA 330;[20] and
- Evaluating the sufficiency and appropriateness of audit evidence obtained (e.g., relating to assumptions or management's oral and written representations).

A15. Information obtained by performing risk assessment procedures and related activities in accordance with paragraphs 17 to 22 of this ISA is audit evidence that supports the identification and assessment of the risks of material misstatement. In addition, the auditor may obtain some audit evidence about classes of transactions, account balances, or disclosures, and related assertions, and about the operating effectiveness of controls, even though such risk assessment procedures were not specifically planned as substantive procedures or as tests of controls. The auditor may also perform designed substantive procedures or tests of controls concurrently with risk assessment procedures because it is efficient to do so. For example, through the use of technology the auditor may perform procedures on large volumes of data, and audit evidence may be obtained that provides information that is useful for the identification and assessment of risks of material misstatement, as well as providing sufficient appropriate audit evidence to support the conclusion that the possibility of a material misstatement is remote.

A16. The auditor uses professional judgment to determine the nature and extent of the required understanding. The auditor's primary consideration is whether the understanding that has been obtained meets the objective stated in this ISA. The auditor's risk assessment procedures to obtain the overall understanding may be less extensive in audits of smaller and less complex entities. The depth of the overall understanding that is required by the auditor is less than that possessed by management in managing the entity.

Types of Risk Assessment Procedures and Sources of Information (Ref: Para. 18)

A17. ISA 500[21] explains the types of audit procedures that may be performed in obtaining audit evidence from risk assessment procedures and further audit procedures. The nature and timing of the audit procedures may be affected by the fact that some of the accounting data and other information may only be available in electronic form or only at certain points in time.[22]

A18. Some of the information used by the auditor when performing risk assessment procedures may be electronic data available from the entity's information system, for example the general ledger, sub-ledgers or other operational data. In performing risk assessment procedures, the auditor may use automated tools and techniques in performing the risk assessment procedures, including for analysis, recalculations, reperformance or reconciliations.

A19. Sources of information available to the auditor may include:

- Information obtained through interactions with management, those charged with governance, and other key entity personnel, such as internal auditors.

---

19 ISA 520, *Analytical Procedures*, paragraph 5

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

21 ISA 500, *Audit Evidence,* paragraphs A14–A17 and A21–A25.

22 ISA 500, paragraph A12

- Information obtained directly or indirectly from certain external parties such as regulators.
- Information obtained from the auditor's previous experience with the entity and from audit procedures performed in previous audits, updated as appropriate.
- Publicly available information about the entity, for example entity-issued press releases, and materials for analysts or investor group meetings, analysts' reports or information about trading activity.

These sources may provide potentially contradictory information, which may assist the auditor in exercising professional skepticism in identifying and assessing the risks of material misstatement. 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.[23]

A20. Although the auditor is required to perform all the risk assessment procedures described in paragraph 18 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 23–44), the auditor is not required to perform all of them for each aspect of that understanding. Other procedures may be performed where the information to be obtained therefrom may be helpful in identifying risks of material misstatement. Examples of such procedures may include making inquiries of the entity's external legal counsel or external supervisors, or of valuation experts that the entity has used.

Inquiries of Management, the Internal Audit Function and Others within the Entity (Ref: Para. 18(a))

A21. Much of the information obtained by the auditor's inquiries is obtained from management and those responsible for financial reporting. Information may also be obtained by the auditor through inquiries of the internal audit function, if the entity has such a function, and others within the entity.

A22. The auditor may also obtain information, or a different perspective in identifying risks of material misstatement, through inquiries of others within the entity and other employees with different levels of authority. For example:

- Inquiries directed towards those charged with governance may help the auditor understand the environment in which the financial statements are prepared. ISA 260 (Revised)[24] 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 involved in 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.

---

[23] ISA 500, paragraph 7

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

- Inquiries directed towards the risk management function (or those performing such roles) may provide information about operational and regulatory risks that may affect financial reporting.
- Inquiries directed towards information system personnel may provide information about system changes, system or control failures, or other information systems-related risks.

A23. As obtaining an understanding of the entity and its environment is a continual, dynamic process, the auditor's inquiries may occur throughout the audit engagement.

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

A25. 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 and the 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.[25] Inquiries of particular relevance may be about matters the internal audit function has raised with those charged with governance and the outcomes of the function's own risk assessment process.

A26. 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, 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.

A27. In addition, in accordance with ISA 240,[26] 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.

A28. 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.

---

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

[26] ISA 240, paragraph 19

Considerations specific to public sector entities

A29. 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 can assist the auditors in identifying the risk of material noncompliance with applicable laws and regulations and the risk of control deficiencies related to financial reporting.

Analytical Procedures (Ref: Para. 18(b))

A30. Analytical procedures performed as risk assessment procedures may identify aspects of the entity of which the auditor was unaware and may assist in identifying and assessing the risks of material misstatement. 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.

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

A32. Analytical procedures performed as risk assessment procedures may use data aggregated at a high level and accordingly the results of those analytical procedures may provide a broad initial indication about the likelihood of a material misstatement. For example, in the audit of many entities, including those with less complex business models and processes, and a less complex information system, the auditor may perform a simple comparison of information, such as the change in account balances from interim or monthly reporting with balances from prior periods, to obtain an indication of potentially higher risk areas.

A33. Analytical procedures can be performed using a number of tools or techniques, which may be automated. Applying automated analytical procedures to the data may be referred to as data analytics. For example, the auditor may use a spreadsheet to perform a comparison of actual recorded amounts to budgeted amounts, or may perform a more advanced procedure by extracting data from the entity's information system, and further analyzing this data using visualization techniques to identify more specific areas of possible misstatement.

A34. This ISA deals with the auditor's use of analytical procedures as risk assessment procedures. ISA 520 deals with the auditor's use of analytical procedures as substantive procedures ("substantive analytical procedures"). 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.

Observation and Inspection (Ref: Para. 18(c))

A35. Observation and inspection may support inquiries of management and others, and may also provide information about the entity and its environment. Examples of such risk assessment procedures 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; or regulatory or financial publications; or other external documents about the entity's financial performance (such as those referred to in paragraph A74).
- The behaviors and actions of management or those charged with governance (such as the observation of an audit committee meeting).

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 as documents related to mandatory performance reporting.

Information from the Acceptance or Continuance of the Client Relationship or the Audit Engagement (Ref: Para. 19)

A37. In accordance with ISA 220, the engagement partner is required to be satisfied that appropriate procedures regarding the acceptance and continuance of client relationships and audit engagements have been followed, and to determine that conclusions reached in this regard are appropriate.[27] Information obtained in the client and engagement acceptance or continuance process may be relevant to the identification and assessment of the risks of material misstatement. Examples may include:

- Information about the nature of the entity and its business risks.
- Information about the integrity and ethical values of management and those charged with governance, which may be relevant to the auditor's understanding of the control environment, and may also affect the auditor's identification and assessment of the risks of material misstatement at the financial statement level.
- The applicable financial reporting framework and information about its application to the nature and circumstances of the entity.

Information from Other Engagements Performed for the Entity (Ref: Para. 20)

A38. The engagement partner may have performed other engagements for the entity and may thereby have obtained knowledge relevant to the audit, including about the entity and its environment. Such engagements may include agreed-upon procedures engagements (e.g., agreed-upon procedures relating to an entity's debt covenant compliance) or other audit or assurance engagements (e.g., audits of special purpose financial statements or reviews of interim financial information).

Information Obtained in Prior Periods (Ref: Para. 21)

A39. 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:

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

- 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, which may assist the auditor in gaining a sufficient understanding of the entity to identify and assess risks of material misstatement.
- 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.

A40. The auditor is required to determine whether information obtained in prior periods remains relevant and reliable, if the auditor intends to use that information for the purposes of the current audit. This is because changes in the entity's system of internal control, for example, may affect the relevance and reliability of information obtained in the prior period. In evaluating whether such information remains relevant and reliable for the current audit, the auditor may consider whether changes have occurred that may affect the relevance or reliability of such information. For example, the auditor may make inquiries and perform other appropriate audit procedures, such as walk-throughs of relevant systems.

Discussion Among the Engagement Team (Ref: Para. 22)

A41. Paragraph 22 requires the engagement partner and other key engagement team members to discuss the application of the applicable financial reporting framework in the context of the nature and circumstances of the entity and its environment, and the susceptibility of the entity's financial statements to material misstatement. 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 A43 nonetheless may assist the auditor in identifying where there may be risks of material misstatement.

A42. The discussion among the engagement team about 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 the inherent risk factors may affect the 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.[28]

A43. As part of the discussion among the engagement team required by paragraph 22, 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. Examples of 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.

A44. In addition to the intended benefits of the engagement team discussion included in paragraph A42, the engagement team may also have an opportunity to exercise professional skepticism while performing risk assessment procedures, such as through identifying and discussing contradictory information obtained in performing those procedures, as well as in considering whether there are indicators of possible management bias (both intentional and unintentional). 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, which may in turn drive the consideration of those engagement team members who are appropriately skilled to be involved in the performance of audit procedures related to those areas.

A45. It is not always necessary or practical for the discussion to include all members in a single discussion (as, for example, in a multi-location audit), nor is it necessary for all of the members of the engagement team to be informed of all of 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, while taking into account of the extent of communication considered necessary throughout the engagement team. A communications plan, agreed by the engagement partner, may be useful.

[28] ISA 240, paragraph 15

Considerations Specific to Public Sector Entities

A46. As part of the discussion among the engagement team, as required by paragraph 22, 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 and the Applicable Financial Reporting Framework (Ref: Para. 23–24)

A47. The auditor's understanding of the entity and its environment, and the applicable financial reporting framework, establishes a frame of reference within which the auditor identifies and assesses risks of material misstatement, and plans and performs audit procedures. Specifically, the auditor applies professional judgment in determining whether the understanding required by paragraph 23 is sufficient to provide an appropriate basis for the auditor to understand the classes of transactions, account balances and disclosures to be expected in the entity's financial statements. This understanding assists the auditor in identifying areas in the financial statements where material misstatements may be more likely to arise and assists the auditor in exercising professional skepticism throughout the audit. The nature and extent of the understanding required will likely depend on the nature, size and complexity of the entity.

The Entity and Its Environment (Ref: Para 23(a))

A48. In obtaining an understanding of the entity and its environment, the auditor may be able to enhance the understanding by using automated tools and techniques. For example, the auditor may use automated 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).

The Entity's Organizational Structure, Ownership and Governance, and Business Model (Ref: Para. 23(a)(i))

The entity's organizational structure and ownership

A49. 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. For example, the entity may be a single entity or the entity's structure may include subsidiaries, divisions or other components in multiple locations. Further, the legal structure may be different from the operating structure. Complex structures often introduce factors that may give rise to increased susceptibility to risks of material misstatement. Such issues may include whether goodwill, joint ventures, investments, or special-purpose entities are accounted for appropriately and whether adequate disclosure of such issues in the financial statements have 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.[29]

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

- The distinction between the owners, those charged with governance and management. In some entities, particularly smaller and less complex entities, owners of the entity may be involved in managing the entity, or those charged with governance may be involved in managing the entity.[30]
- The entity's IT environment. For example, an entity's IT environment may be relatively simple because it consists only of commercial software for which the entity does not have access to the underlying source code to which no changes have been made. Alternatively, an entity may have grown through extensive merger and acquisition activity and have multiple legacy IT systems in diverse businesses that are not well integrated resulting in a complex IT environment.

Considerations specific to public sector entities

A50. In obtaining an understanding of the entity's organizational structure and ownership, auditors of public sector entities may consider the relevance of ownership of a public sector entity (i.e., 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 initiated outside of the entity as a result of political processes and therefore management may not have control over decisions that are made). Matters related to the understanding of the organizational structure, governance and business model of a public sector entity may 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 mandate and strategic direction. For example, the 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. 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

A51. Responsibilities of management and those charged with governance are broader than responsibilities for the oversight of the system of internal control, but are generally prerequisites for an effective system of internal control. The responsibilities of those charged with governance in relation to the control environment are further discussed in Appendix 3. Deficient governance processes may limit an entity's ability to provide appropriate oversight of its system of internal control, which may increase the entity's susceptibility to risks of material misstatement. 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.

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

- The responsibilities of those charged with governance for oversight of financial reporting, including approval of the financial statements.

The Entity's Business Model

A52. 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 are relevant in the context of the audit. Furthermore, this may assist the auditor in identifying risks of material misstatement. For example, incentives and pressures on management may result in intentional or unintentional management bias, which may affect the reasonableness of significant assumptions and expectations of management or those charged with governance thereby increasing the susceptibility to risks of material misstatement. (See also paragraph A59).

A53. 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, such as public benefits, for its stakeholders.

A54. 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.

A55. 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.

A56. 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. Not all aspects of the business model are relevant for the auditor's understanding, but those aspects that give rise to business risks, which are relevant to the identification and assessment of risks of material misstatement, are likely to be more relevant for the auditor's understanding.

A57. Appendix 1 provides examples of matters that may be considered when obtaining an understanding of the activities of the entity, as well as other matters that may be considered when auditing financial statements of special purpose entities.

Considerations specific to public sector entities

A58. 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' to promote value in the public interest. 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.

Business risks in the context of the entity's business model

A59. 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. Business risks are broader than the risks of material misstatement of the financial statements, although business risks includes the latter. The auditor does not have a responsibility to identify or assess all business risks because not all business risks give rise to risks of material misstatement. Business risk may arise from, among other matters, 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.

A60. 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 indicate risks of material misstatement are indicated in Appendix 2.

A61. 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 (a potential related business risk might be, for example, that the entity does not have the personnel or expertise to deal with the changes in the industry).
- New products and services (a potential related business risk might be, for example, that there is increased product liability).

- Expansion of the business (a potential related business risk might be, for example, that the demand has not been accurately estimated).
- New accounting requirements (a potential related business risk might be, for example, incomplete or improper implementation, or increased costs).
- Regulatory requirements (a potential related business risk might be, for example, that there is increased legal exposure).
- Current and prospective financing requirements (a potential related business risk might be, for example, the loss of financing due to the entity's inability to meet requirements).
- Use of IT (a potential related business risk might be, for example, that the entity is implementing a new IT system that will affect both operations and financial reporting).
- The effects of implementing a strategy, particularly any effects that will lead to new accounting requirements (a potential related business risk might be, for example, incomplete or improper implementation).

A62. 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 29–31 and paragraphs A115–A121.

Considerations Specific to Public Sector Entities

A63. 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.

Relevant Industry, Regulatory and Other External Factors (Ref: Para. 23(a)(ii))

Industry factors

A64. Relevant industry factors include industry conditions such as the competitive environment, supplier and customer relationships, and technological developments. Examples of 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.

A65. The industry in which the entity operates may give rise to specific risks of material misstatement arising from the nature of the business or the degree of regulation. For example, 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.[31]

Regulatory Factors

A66. Relevant regulatory factors include the regulatory environment. The regulatory environment encompasses, among other matters, the applicable financial reporting framework and the legal and

[31] ISA 220, paragraph 14

political environment and any changes thereto. Examples of matters the auditor may consider include:

- Regulatory framework for a regulated industry, for example, medical or retirement funds, including requirements for 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.

A67. 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.[32]

Considerations specific to public sector entities

A68. 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

A69. Examples of 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.

Relevant Measures Used to Assess the Entity's Financial Performance (Ref: Para. 23(a)(iii))

A70. Management and others ordinarily measure and review those matters they regard as important. The procedures undertaken to measure the relevant performance of the entity 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.

A71. Performance measures, whether used externally or internally, may create pressures on the entity. These pressures, in turn, may motivate management to take action to improve the business performance or to intentionally misstate the financial statements. Accordingly, an understanding of the entity's performance measures assists the auditor in considering whether pressures to achieve performance targets may result in management actions that increase the susceptibility to misstatement due to management bias or fraud. For example, the auditor may identify incentives or pressures that may increase the risk of management override of controls. See ISA 240 for requirements and guidance in relation to the risks of fraud.

A72. 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 A122–A135), though their purposes may overlap:

---

[32] ISA 250 (Revised), *Consideration of Laws and Regulations in an Audit of Financial Statements*, paragraph 13

- 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.

A73. Examples of internally-generated information used by management for measuring and reviewing financial performance, and which the auditor may consider, 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.

A74. External parties may also review and analyze the entity's financial performance, in particular for entities where financial information is publicly available. For example, publicly available financial information may be issued by:

- Analysts or credit agencies.
- Revenue authorities.
- Regulators.
- Trade unions.
- Providers of finance.

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

A75. Internal measures may highlight unexpected results or trends requiring management to determine their cause and take corrective action (including, in some cases, the detection and correction of misstatements on a timely basis). Performance measures may also indicate to the auditor the likelihood with which risks of misstatement of related financial statement information exist. 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.

A76. Performance measures and targets, whether imposed internally or externally, particularly if combined with other factors such as performance-based bonus or incentive remuneration, may indicate an increased susceptibility to misstatement due to management bias or fraud in the preparation of the financial statements.

A77. Inquiry of management may reveal that it relies on certain key indicators for evaluating financial performance and taking appropriate 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.

Considerations specific to public sector entities

A78. 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. 23(b))

A79. Examples of 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 share-based payments).
- 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.

A80. Obtaining an understanding of the entity and its environment assists the auditor in considering where changes in the entity's financial reporting (e.g., from prior periods) may be expected. For example, if the entity has had a significant business combination during the period, the auditor would likely expect changes in classes of transactions, account balances and disclosures associated with that business combination. Alternatively, if there were no significant changes in the financial reporting framework during the period the auditor's understanding may help confirm that the understanding obtained in the prior period remains applicable.

A81. Disclosures in the financial statements of smaller and less complex entities may be simpler and less detailed (e.g., 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, the applicable financial reporting framework as it applies to the entity, and its related system of internal control.

Considerations specific to public sector entities

A82. 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 (such as the International Public Sector Accounting Standards), a cash-basis of accounting, or a hybrid. The financial reporting applied by a public sector entity further impacts the ability to assess the accountability for all assets and liabilities of the entity, as well as the entity's system of internal control.

How Events or Conditions are Subject To, or Affected By, the Inherent Risk Factors

A83. The auditor is required to consider events or conditions in understanding how the applicable financial reporting framework applies in the context of the nature and circumstances of the entity. In doing so, the auditor identifies how events or conditions are subject to, or affected by, the inherent risk factors, which may assist the auditor in understanding which classes of transactions, account balances and disclosures may be affected. Understanding whether, and the relative degree to which the inherent risk factors affect the events and conditions may assist the auditor in identifying and assessing the risks of material misstatement at the assertion level. Appendix 2 provides examples of events and conditions that may indicate susceptibility to risks of material misstatement, categorized by inherent risk factor.

A84. The extent to which a class of transactions, account balance or disclosure is subject to, or affected by, complexity or subjectivity, is often closely related to the extent to which it is subject to change or uncertainty. Further, when a class of transactions, account balance or disclosure is subject to, or affected by, 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 or fraud. Accordingly, 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 the inherent risk factors.

A85. Events or conditions that may be affected by, or subject to, the susceptibility of misstatement due to management bias or fraud may be indicative of increased risks of material misstatement due to fraud. 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.

A86. 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. For example, when there are many potential data sources, with different characteristics, and the processing of that data involves many interrelated steps, the data may be inherently more difficult to identify, capture, access, understand or process.

A87. 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, models and assumptions may reflect unintentional or intentional management bias.

A88. Where there are increased opportunities for intentional management bias or fraud (e.g., owner-managed entities where there is an increased opportunity for management override of controls), the auditor may identify an increased susceptibility to misstatement due to management bias or fraud.

Obtaining an Understanding of the Entity's System of Internal Control (Ref: Para. 25–26)

A89. Obtaining an understanding of the components of the entity's system of internal control:

- Assists the auditor in identifying and assessing the risks of material misstatement at the financial statement level and the assertion level; and
- Provides a basis for the auditor's determination of the extent to which the auditor plans to rely on the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures in accordance with ISA 330.

A90. The auditor is required to perform risk assessment procedures to obtain an understanding of each component of internal control relevant to financial reporting. Paragraphs 27–38 address the matters the auditor is required to understand in relation to the components of the system of internal control. The nature, timing, and extent of risk assessment procedures that the auditor performs to obtain this understanding are matters of the auditor's professional judgment and are based on the auditor's determination as to what will provide sufficient and appropriate audit evidence for the auditor's identification and assessment of risks of material misstatement. Accordingly, the nature, timing and extent of procedures to understand the entity's system of internal control will vary from entity to entity, and may depend on matters such as:

- The size and complexity of the entity, including its IT environment.
- Previous experience with the entity.
- The nature of each component[33] of the entity's system of internal control.
- The nature and form of the entity's documentation, including as it relates to specific controls.

A91. 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.

A92. 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.

System of Internal Control Relevant to Financial Reporting

A93. The entity's system of internal control is designed, implemented and maintained to address identified business risks that threaten the achievement of any of the entity's objectives that concern:

- The reliability of the entity's financial reporting;
- The effectiveness and efficiency of its operations; and
- Its compliance with applicable laws and regulations.

[33] See paragraph 102

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

A94. The entity's system of internal control relevant to financial reporting will include aspects of the system of internal control 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. For example, controls over compliance with laws and regulations may be relevant to financial reporting when such controls are relevant to the entity's preparation of contingency disclosures in the financial statements. In particular, the auditor is required by paragraph 35 to understand how the entity initiates transactions and captures information relevant to financial reporting as part of the auditor's understanding of the information system. Such information may include information from the entity's systems and controls designed to address compliance and operations objectives. 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.

A95. For the purposes of this ISA, the system of internal control relevant to financial reporting means the system of internal control relevant to the preparation of the financial statements in accordance with the requirements of the applicable financial reporting framework.

Considerations Specific to Public Sector Entities

A96. 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.

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

A97. An entity's system of internal control contains manual elements and automated elements. An entity's mix of manual and automated elements in the entity's system of internal control varies with the nature and complexity of the entity's use of IT. 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. An entity's use of IT affects the manner in which the information relevant to financial reporting is processed, stored and communicated, and therefore affects the manner in which the system of internal control relevant to financial reporting is designed and implemented. Each component of the system of internal control may involve some extent of automation. The auditor's understanding of the system of internal control relevant to financial reporting involves understanding the entity's use of IT for each component.

A98. 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, by control parameters that are automated.
- Controls where the specific ways to perform the control can be adequately designed and automated.

Components of the Entity's System of Internal Control

A99. The components of the entity's system of internal control for the purpose of this ISA do 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.

A100. The entity's system of internal control relevant to financial reporting addresses the prevention, detection and correction of misstatements in the entity's financial statements; however, the manner in which the individual components operate in this respect differs. The control environment provides the overall foundation for the operation of 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. Therefore these components support the controls within the other components of the entity's system of internal control. Due to the manner in which the controls within these components are designed to operate, they are typically not precise enough to prevent, or detect and correct, misstatements at the assertion level and instead may have an indirect effect on the likelihood that a misstatement will be detected or prevented on a timely basis. These controls may be referred to as "indirect controls."

A101. In contrast, the information system and communication component, as well as the control activities component, typically include controls that are designed to prevent, or to detect and correct, misstatements at the assertion level for the classes of transactions, account balances and disclosures in the entity's financial statements. Such controls may be referred to as "direct controls."

A102. The nature of each of the components of the entity's system of internal control may also affect the auditor's identification and assessment of the risks of material misstatement as follows:

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

A103. Notwithstanding the types of controls that are typically within each component of the entity's system of internal control, direct or indirect controls may exist in any of the components. In particular, the control activities component includes general IT controls, which may include 'indirect controls.' For example, controls that address the continued functioning of automated controls over the processing of transactions, such as controls over the integrity of information in the entity's information system, may also include 'direct controls.'

Controls Relevant to the Audit (Ref: Para. 26)

A104. The auditor identifies controls relevant to the audit in accordance with paragraphs 39 through 41. Controls relevant to the audit are likely to include mainly controls that address potential risks of misstatement at the assertion level (i.e., controls in the control activities component). However, controls relevant to the audit may also include controls in other components of the system of internal control, i.e., the control environment, the risk assessment process and the process to monitor controls components that address the risks of material misstatement at the assertion level. The auditor evaluates the design of each control relevant to the audit and determines whether it has been implemented in accordance with paragraph 42.

Understanding the Components of the Entity's System of Internal Control (Ref: Para. 27–38)

Control Environment (Ref: Para. 27)

A105. 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.

A106. The control environment relating to smaller and less complex entities is likely to vary from larger or more complex entities. For example, the organizational structure may be simpler and include a small number of employees involved in roles related to financial reporting. Further, those charged with governance in smaller and 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 inapplicable or less relevant. For example, 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.

A107. In addition, audit evidence for elements of the control environment in smaller and less complex entities may not be available in documentary form, in particular where communication between management and other personnel may be informal, but is still effective. For example, such entities may not have a written code of conduct but, instead, develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication and by management example. Consequently, the attitudes, awareness and actions of management or the owner-manager are of particular importance to the auditor's understanding of a smaller and less complex entity's control environment.

Understanding the Control Environment

A108. Audit evidence for the auditor's understanding of the control environment may be obtained through a combination of inquiries and other risk assessment procedures (i.e., corroborating inquiries through observation or inspection of documents). The nature, timing and extent of the auditor's procedures to obtain the understanding of the control environment may vary to the extent necessary, to provide an appropriate basis for the required evaluation in paragraph 28. For example, 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 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.

A109. The auditor may also consider how management has responded to the findings and recommendations of the internal audit function regarding identified control deficiencies relevant to the audit, including whether and how such responses have been implemented, and whether they have been subsequently evaluated by the internal audit function.

A110. The auditor's consideration of the entity's use of IT as it relates to the control environment may include such matters as:

- Whether governance over IT is commensurate with the nature and size 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)).

Evaluating the Control Environment (Ref: Para. 28)

A111. The control environment in itself does not prevent, or detect and correct, a material misstatement. It may, however, influence the auditor's evaluation of the effectiveness of other controls (for example, the monitoring of controls and the operation of specific controls in the control activities component) and thereby, the auditor's identification and assessment of the risks of material misstatement. As further explained in paragraph A218–A219, control deficiencies in the control environment may lead to risks of material misstatement at the financial statement level, which may have implications for the audit, including, as explained in ISA 330, an influence on the nature, timing and extent of the auditor's further procedures.[34]

A112. Some elements of an entity's control environment have a pervasive effect on assessing the risks of material misstatement. 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.

A113. Some entities may be dominated by a single individual who may exercise a great deal of discretion. The actions and attitudes of that individual may have a pervasive effect on the culture of the entity, which in turn may have a pervasive effect on the control environment. Such an effect may be positive or negative. For example, direct involvement by this single individual may be key to enabling the entity to meet its growth and other objectives, and can also contribute significantly to an effective

[34] ISA 330, paragraphs A2–A3

system of internal control. On the other hand, such concentration of knowledge and authority can also lead to an increased susceptibility to misstatement through management override of controls.

A114. Active involvement by those charged with governance, who are also independent, may influence the philosophy and operating style of senior management. However, other elements may be more limited in their effect. For example, although human resource policies and practices directed toward hiring competent financial, accounting, and IT personnel may reduce the risk of errors in processing financial information, they may not mitigate a strong bias by top management to overstate earnings. Overall, although a control environment that provides an appropriate foundation for the system of internal control may help reduce the risk of fraud, an appropriate control environment is not necessarily an effective deterrent to fraud.

The Entity's Risk Assessment Process (Ref: Para. 29–31)

A115. 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.

A116. The extent to which an entity's risk assessment process is formalized may vary. Some entities, including smaller and less complex entities, and particularly owner-managed entities, may not have established a structured risk assessment process, or the risk assessment process may not be documented or performed on regular basis. Irrespective whether the risk assessment process is formally established or not, the auditor may still obtain the understanding required by paragraph 29 about how the entity identifies risks relevant to financial reporting and how these risks are addressed through observation and inquiry.

Understanding the Entity's Risk Assessment Process (Ref: Para. 29)

A117. In order to understand how management and those charged with governance have identified business risks relevant to financial reporting objectives, and have decided about actions to address those risks, matters the auditor may consider include how management or, as appropriate, those charged with governance have:

- Specified objectives with sufficient clarity to enable the identification and assessment of the risks relating to the objectives;
- Identified the risks to achieving the entity's objectives and analyzed the risks as a basis for determining how the risks should be managed;
- Considered the potential for fraud when considering the risks to achieving the entity's objectives; and
- Identified and evaluated changes that could significantly affect the entity's system of internal control.

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

A118. The nature, timing and extent of the auditor's risk assessment procedures to obtain the understanding of the entity's risk assessment process may vary to the extent necessary, to provide an appropriate basis for the required evaluation in paragraph 31.

A119. Understanding the risks arising from the entity's use of IT identified by the entity, as well as how these risks have been addressed, is an important input to the auditor's identification of risks arising from

the use of IT in accordance with paragraph 41. It may also help the auditor understand the nature and extent of automated processes, and the data, used in controls that may be relevant to the audit.

Evaluating the Appropriateness of the Entity's Risk Assessment Process (Ref: Para. 31)

A120. Whether the entity's risk assessment process is appropriate to the circumstances of the entity, including its nature, size, and complexity, is a matter of the auditor's professional judgment. For example, in some smaller and 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 risks that may affect how the entity applies the requirements of the applicable financial reporting framework related to the entity's ability to continue as a going concern).

A121. When the auditor determines, in accordance with paragraph 31(b), that a control deficiency exists related to the entity's risk assessment process, the auditor is required to determine, in accordance with paragraph 43, whether any such deficiency constitutes a significant control deficiency. Whether the absence of an appropriate risk assessment process represents a significant control deficiency is a matter of the auditor's professional judgment. Circumstances that may indicate a significant control deficiency exists include matters such as:

- The absence of a risk assessment process when such a process would ordinarily be expected to have been established; or
- Evidence of an ineffective risk assessment process, which may be the case when the process has failed to identify a risk of material misstatement when it would be expected the risk assessment process would have identified the risk.

The Entity's Process to Monitor the System of Internal Control (Ref: Para. 32–34)

A122. The entity's process to monitor the system of internal control is a continuous process to evaluate the effectiveness of the system of internal control and to take necessary remedial actions on a timely basis. The entity's process to monitor the system of internal controls 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 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.

A123. In smaller and less complex entities, and in particular owner-manager entities, the entity's process to monitor the system of internal control is often accomplished by management's or the owner-manager's direct involvement in operations, and there may not be any other monitoring activities. For example, this is the case when significant variances from expectations and inaccuracies in financial data are identified through the owner-manager's direct involvement. The owner-manager's actions and follow-up may also be how remedial actions are implemented. In such cases, the auditor's understanding of the process to monitor the system of internal control may be accomplished through inquiry of the owner-manager and employees about these activities, and may also involve inspection or observation of related communications or other evidence of remedial actions.

A124. For entities where there is no distinct process for monitoring the system of internal control, it may be difficult to distinguish between controls in the control activities component and activities related to monitoring. For example, a supervisory review may not be considered a monitoring activity by the entity, but the review may have a role in monitoring the effectiveness of underlying controls. For such

entities, 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.

A125. Controls in the entity's process to monitor the system of internal control are likely to consist of primarily indirect controls. However, monitoring activities, such as management or supervisory reviews, may be precise enough to address risks of material misstatement at the assertion level (i.e., direct controls). Such controls may also include certain activities performed by the internal audit function. The auditor may determine certain direct controls to be controls relevant to the audit in accordance with paragraph 39–41.

Understanding the Entity's Process to Monitor the System of Internal Control (Ref: Para. 32)

A126. In order to understand how the entity monitors its system of internal control, matters that may be relevant for the auditor to consider 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.

A127. The entity's process to monitor the system of internal control includes monitoring underlying controls that involve the use of IT, and may include, for example:

- Controls to monitor complex IT environments that:
  - Evaluate the continuing design effectiveness of underlying controls and modify them, as appropriate, for changes in conditions; or
  - Evaluate the operating effectiveness of underlying controls.
- Controls that monitor the permissions applied in automated application 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.

A128. Controls within the entity's process to monitor the 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.

Sources of Information (Ref: Para. 33)

A129. Much of the information used in monitoring may be produced by the entity's information system. If management assumes that information used for monitoring is accurate without having a basis for that assumption, errors that may exist in the information could potentially lead management to incorrect conclusions from its monitoring activities. Accordingly, an understanding of:

- The sources of the information related to the entity's monitoring activities; and

- The basis upon which management considers the information to be sufficiently reliable for the purpose of the monitoring activities

is required to provide a basis for the auditor's understanding of the entity's process to monitor the system of internal control.

A130. 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.

The Entity's Internal Audit Function (Ref: Para. 34)

A131. If the entity has an internal audit function, the auditor's understanding of the entity's process to monitor the system of internal control involves obtaining an understanding of the role that the internal audit function plays in that process. The auditor's inquiries of appropriate individuals within the internal audit function in accordance with paragraph 18(a) of this ISA 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 in paragraph 18(a) of this ISA, may also provide information that is directly relevant to the auditor's identification and assessment of the risks of material misstatement.

A132. 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 size of the entity and the nature of its operations, and has a direct reporting relationship to those charged with governance.

A133. 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.

A134. 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.

A135. 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[35] discusses the importance of the auditor planning and performing the audit with professional skepticism, including being alert to information that brings into question the reliability of documents and responses to inquiries to be used as audit evidence.

[35] ISA 200, paragraph 15

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.

The Information System and Communication

The Information System Relevant to Financial Reporting (Ref: Para. 35)

A136. The information system relevant to financial reporting consists of the policies or procedures, and records, designed and established to:

- Initiate, record, process, and report 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 financial reporting 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.

A137. 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. 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 relevant to financial reporting in a manner that is appropriate to the entity's circumstances.

A138. The entity's information system relevant to financial reporting 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.

A139. The information system, and related business processes relevant to financial reporting in smaller and less complex entities is likely to be less sophisticated than in larger entities and involve a less complex IT environment, but the role of the information system is just as important. Regardless of the size or

nature of the entity, the information system includes relevant aspects of that system relating to information disclosed in the financial statements that is obtained from within or outside of the general and subsidiary ledgers. Smaller and less complex entities with direct management involvement may not need extensive descriptions of accounting procedures, sophisticated accounting records, or written policies. Understanding the entity's information system relevant to financial reporting may therefore require less effort in an audit of smaller and less complex entity, and may be more dependent on inquiry than on review of documentation. The need to obtain an understanding, however, remains important to identify risks of material misstatement.

A140. The auditor's understanding of the information system relevant to financial reporting required by paragraph 35 includes understanding the flows of information relating to the entity's significant classes of transactions, account balances, and disclosures in the financial statements. The auditor's understanding of the information system relevant to financial reporting is not required to include an understanding of the flows of information related to classes of transactions, account balances or disclosures that are not significant classes of transactions, account balances or disclosures.

A141. Risk identification and assessment is an iterative process. The auditor's expectations formed in paragraph 23 about the classes of transactions, account balances and disclosures may assist the auditor in determining the significant classes of transactions, account balances and disclosures in accordance with paragraph 46, which are those that need to be understood when obtaining an understanding of the information system in accordance with paragraph 35. For example, the auditor may have an expectation that certain significant classes of transactions related to revenue exist, but in obtaining the understanding about the flows of information in the information system, the auditor may identify additional classes of transactions related to revenue that may be significant.

Information Obtained from Outside of the General and Subsidiary Ledgers

A142. Financial statements may contain information that is obtained from outside of the general and subsidiary ledgers. Examples of such information may include:

- Information obtained from lease agreements disclosed in the financial statements, such as renewal options or future lease payments.
- 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.[36]

A143. Certain amounts or disclosures in the entity's financial statements (such as disclosures about credit risk, liquidity risk, and market risk) may be based on information obtained from the entity's risk management system. However, the auditor is not required to understand all aspects of the risk management system, and uses professional judgment in determining the necessary understanding.

Understanding the Entity's Use of Information Technology in the Information System (Ref: Para. 35(d))

A144. The auditor is required to understand the IT environment relevant to 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. The nature and significance of these risks vary based on whether, and the extent to which, the entity relies on IT, including automated controls, to support the processes in its information system and to maintain the completeness and accuracy of the underlying data and information. The entity may implement general IT controls in response to these risks. General IT controls may be relevant to the audit and may need to be taken into account in the auditor's assessment of control risk at the assertion level.

A145. Examples of risks arising from the use of IT include:

- Inappropriate reliance on IT applications that are inaccurately processing data, processing inaccurate data, or both.
- Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or 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.

A146. The auditor may take an approach to obtaining the understanding the IT environment that involves identifying 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 through the entity's information system.

A147. In obtaining the understanding of the IT environment, the auditor may also obtain a high-level understanding of the IT processes and the personnel involved in maintaining the IT environment (e.g., the number and skill level of the IT support resources that manage security and changes to the environment), which assists the auditor in understanding the complexity of the IT environment. This understanding may include identifying significant changes in the IT environment, which may be

[36] See paragraphs 19–20 of ISA 570 (Revised), *Going Concern*

revealed through significant changes in the flows of transactions or information through the entity's information system.

A148. Obtaining the auditor's understanding of the IT environment in accordance with paragraph 35(d), and the auditor's identification of IT applications and other aspects of the IT environment relevant to the audit in accordance with paragraph 40, may involve an iterative process or may be performed concurrently. Matters that may be relevant to the auditor's understanding of the IT environment, or the determination of the aspects that are relevant to the audit, include matters such as:

- The extent of automated procedures for processing, and the complexity of those procedures, including, whether there is highly automated, paperless processing.
- The extent of the entity's reliance on system-generated reports in the processing of information.
- How data is input (i.e., manual input, customer or vendor input, or file load).
- How IT facilitates communication between applications, databases or other aspects of the IT environment, internally and externally, as appropriate, through system interfaces.
- The volume and complexity of data in digital form being processed by the system, including whether accounting records or other information are stored in digital form.
- Matters related to the individual aspects of the IT environment, for example:
    - The type of application (e.g., a commercial application with little or no customization, or a highly-customized or highly-integrated application that may have been purchased and customized, or developed in-house).
    - The complexity of the nature of the IT applications and the underlying IT infrastructure.
    - 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 security risks, particularly when there are web-based transactions or transactions involving external interfaces.
    - 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)
    - Whether there is third-party hosting or outsourcing of IT.
    - Whether the entity is using emerging technologies that affect its financial reporting.
- 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.
- Whether program changes have been made to the manner in which information is processed, and the extent of such changes during the period

A149. Obtaining an understanding of the entity's IT environment may be more easily accomplished for a smaller and 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 smaller and 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; and
- The nature and extent of modifications that have been made to 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.

A150. 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 financial reporting IT applications. In such circumstances, certain IT applications used in the entity's business operations may be relevant to financial reporting. 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 third-party service providers to manage certain aspects of, or IT processes within, its IT environment.

Evaluating the Design of the Information System Controls Relevant to Financial Reporting (Ref: Para. 36)

A151. The information system relevant to financial reporting comprises the entity's financial reporting processes, and the entity's personnel, IT and other resources, deployed in applying those processes. The objective of those processes is to capture, store and process data from internal and external sources, and to produce the entity's accounting records and the information that the entity needs to include in its financial statements. The objective of those processes is also to comply with the requirements and principles in the applicable financial reporting framework, and in other applicable laws or regulations. Paragraphs 10–12 of Appendix 3 sets out further matters for consideration relating to the information system.)

A152. The design of the information system is established in the policies and procedures that define the nature, timing and extent of the entity's financial reporting processes, and how the entity's personnel, IT and other resources are deployed in applying them. Such controls are referred to in this ISA as information system controls relevant to financial reporting. Such policies and procedures may be formally documented, for example in a financial reporting manual, or may be less formally established through communication by management.

A153. The auditor's understanding of the information system may be obtained in various ways. The auditor's risk assessment procedures to obtain such understanding may include, for example, a combination of:

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

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

A154. The audit evidence obtained by these risk assessment procedures is used by the auditor to evaluate the design of the information system controls relevant to the financial reporting and determine whether they have been implemented.In evaluating the design of the entity's information system controls relevant to financial reporting, the auditor considers whether such controls would meet their financial reporting objectives, if implemented as designed and operating effectively.

A155. The auditor may also use automated techniques by obtaining direct access to, or a digital download from, the databases in the entity's information system that store the accounting records of transactions. By using 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 additional risks of material misstatement related to non-standard procedures.

A156. Regardless of the techniques used to evaluate the design of the information system and determine whether it has been implemented, the auditor's understanding of the sources of data, and the IT applications involved in processing that data, may also assist the auditor in understanding the IT environment.

A157. The entity also establishes controls that are designed to support the operating effectiveness of the controls within the information system. For purposes of the ISAs, controls over the information system are treated as controls in the control activities component and may be identified as controls relevant to the audit. The objectives of such controls may include, for example, maintaining the integrity or security of the data captured, stored or processed, and of the accounting records and information produced by the information system. The auditor is required to evaluate the design of those controls and determine whether they have been implemented, in accordance with paragraph 42. These procedures may be performed together with the procedures performed to evaluate the design of the information system controls relevant to financial reporting. For example, the auditor may perform a walk-through of a transaction to confirm the flow of transactions relevant to the transaction and at the same time, evaluate the design and implementation of controls relevant to the audit that relate to that class of transactions, such as those related to approvals or reconciliations.

Communication (Ref: Para. 37)

A158. 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 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. Communication may take such forms as policy manuals and financial reporting manuals, particularly in larger entities.

A159. Communication may be less structured (e.g., formal manuals may not be used) and easier to achieve in a smaller and less complex entity than in a larger entity due to fewer levels of responsibility and management's greater visibility and availability. Regardless of the size of the entity, open communication channels help ensure that exceptions are reported and acted on.

Control Activities (Ref: Para. 38)

A160. Controls in the control activities component include those controls over the flows of information within the information system relating to significant classes of transactions, account balances and disclosures and the financial reporting process used to prepare the financial statements. Such controls consist of application controls and general IT controls, both of which could be manual or automated. 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. 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.

A161. Controls in smaller and less complex entities are likely to be similar to those in larger entities, but the formality with which they operate may vary. Further, in smaller and less complex entities, more controls may be directly applied by management. For example, management's sole authority for granting credit to customers and approving significant purchases can provide strong control over important account balances and transactions.

A162. Some individual controls may consist of both automated and manual aspects, such as controls that may use information produced by IT (e.g., an exception report) that is subject to manual procedures (e.g., review and follow-up). For many entities, most controls may be automated controls or involve a combination of automated and manual aspects because of the extent of use of IT applications for financial reporting purposes. In some cases, authorizations, approvals and the preparation of reconciliations may involve the use of technology enabled workflow or use of supporting records in digital form.

A163. 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 application controls.

A164. It may be less practicable to establish segregation of duties in smaller and 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.[37]

A165. Controls in the control activities component may 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.

Controls Relevant to the Audit (Ref: Para. 39–41)

Determining controls relevant to the audit (Ref: Para. 39)

A166. Controls relevant to the audit are primarily direct controls and are primarily controls in the control activities component because such controls typically are controls over the entity's information system

[37] ISA 240, paragraph A27

and address risks of material misstatement at the assertion level. However, there may 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 components. Controls are required to be relevant to the audit when such controls meet one or more of the criteria included in paragraph 39. However, when multiple controls each achieve the same objective, it is unnecessary to identify each of the control related to such objective.

A167. Controls relevant to the audit are required to include 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 relevant to the audit may vary based on the nature of the entity and the auditor's planned approach to further audit procedures. For example, in an audit of a smaller and less complex entity, the entity's information system may not be complex and the auditor may not be required to, or plan to, rely on the operating effectiveness of any 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 controls relevant to the audit other than the entity's controls over journal entries.

Controls that address risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence (Ref: Para. 39(a))

A168. The auditor determines whether there are any risks of material misstatement at the assertion level for which it is not possible or practicable to obtain sufficient appropriate audit evidence through substantive procedures alone as described in paragraph 51. The auditor is required, in accordance with ISA 330,[38] to design and perform tests of relevant controls that address such risks of material misstatement when substantive procedures alone cannot provide sufficient appropriate audit evidence at the assertion level. As a result, when such controls exist that address these risks, they are relevant to the audit.

Controls that address significant risks (Ref: Para. 39(b))

A169. The auditor determines whether any assessed risks of material misstatement at the assertion level are significant risks in accordance with paragraph 49. Significant risks are those that exist close to the upper end of the spectrum of inherent risk and therefore are those risks of material misstatement that require the most persuasive audit evidence in accordance with ISA 330.[39] Paragraph 39 requires that the auditor identify controls that address significant risks to be controls relevant to the audit. The risk assessment procedures performed to understand these controls in accordance with paragraph 42 contribute to the audit evidence related to the significant risk.

A170. Regardless of whether the auditor intends to test the operating effectiveness of controls that address significant risks, the understanding obtained about management's approach to addressing those risks may inform the design and performance of substantive procedures responsive to significant risks as required by ISA 330.[40] Although risks relating to significant non-routine or judgmental matters are often less likely to be subject to routine controls, management may have other responses intended to deal with such risks. Accordingly, the auditor's understanding of whether the entity has

---

[38] ISA 330, paragraph 8

[39] ISA 330, paragraph 7(b)

[40] ISA 330, paragraph 21

designed and implemented controls for significant risks arising from non-routine or judgmental matters includes whether and how management responds to the risks. Such responses might include:

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

A171. For example, where there are one-off events such as the receipt of notice of a significant lawsuit, consideration of the entity's response may include such matters as whether it has been referred to appropriate experts (such as internal or external legal counsel), whether an assessment has been made of the potential effect, and how it is proposed that the circumstances are to be disclosed in the financial statements.

A172. ISA 240[41] requires the auditor to identify the controls that address risks of material misstatement due to fraud as controls relevant to the audit and 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. In identifying the controls relevant to the audit 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.

A173. In some cases, management may not have appropriately responded to significant risks by implementing controls over these significant risks. Failure by management to implement such controls is an indicator of a significant control deficiency.[42]

Controls over journal entries (Ref: Para. 39(c))

A174. An entity's information system typically includes the use of standard journal entries that are required on a recurring basis to record transactions. Examples might be journal entries to record sales, purchases, and cash disbursements in the general or a subsidiary ledger, or to record accounting estimates that are periodically made by management, such as changes in the accounting estimate of uncollectible accounts receivable.

A175. An entity's financial reporting process also includes the use of non-standard journal entries to record non-recurring, unusual transactions or adjustments. Examples of such entries include consolidation adjustments, entries for a business combination or disposal, or non-recurring estimates such as the impairment of an asset. 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. For example, applying automated techniques to analyze an entire population of journal entries within a general ledger may assist in understanding the nature and extent of journal entries made, which account balances are subject to standard or non-standard journal entries, and which entity personnel made or authorized the journal entries. These techniques can be accompanied by inquiries of management or inspection of supporting documentation for journal entries to identify the controls the entity has implemented over journal entries.

---

41 ISA 240, paragraphs 27 and A32.

42 ISA 265, paragraph A7

Testing of operating effectiveness of controls (Ref: Para. 39(d))

A176. When the auditor determines that a risk(s) for which substantive procedures alone cannot provide sufficient appropriate audit evidence exists, the auditor is required to, in accordance with ISA 330,[43] design and perform tests of relevant controls. Further, when the auditor voluntarily intends to take into account the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures, such controls are required to be identified as relevant to the audit because ISA 330[44] requires the auditor to design and perform tests of those controls. For example, the auditor may plan to test controls over routine classes of transactions because such testing may be more effective or efficient for large volumes of homogenous transactions.

A177. The auditor's intentions 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.

A178. The auditor may plan to test the operating effectiveness of controls over the completeness and accuracy of information produced by the entity when the auditor intends to take into account the operating effectiveness of those controls in designing and performing further audit procedures to determine the reliability of that information for its use as audit evidence. The auditor may also plan to test the operating effectiveness of controls relating to operations and compliance objectives when they relate to data the auditor evaluates or uses in applying audit procedures.

Other controls relevant to the audit (Ref: Para. 39(e))

A179. The extent to which other controls are identified as relevant to the audit is a matter of the auditor's professional judgment. The auditor's judgment about whether it is appropriate to devote additional attention to evaluating the design of controls and determining whether they have been implemented in order to provide a basis for the design and performance of further audit procedures is influenced by:

- The auditor's knowledge about the presence or absence of controls obtained from the understanding of the components of the system of internal control. For example, when an engagement is new or the entity has made significant changes to its information system, the auditor may determine that more information about the entity's controls is needed to provide a basis for the design of the auditor's further audit procedures, including to assist the auditor in deciding whether to test the operating effectiveness of such controls; and
- The identification of risks of material misstatement and the related assessments of inherent risk at the assertion level because ISA 330 requires more persuasive audit evidence the higher the auditor's assessment of risk.[45] For risks that are assessed as higher, but are not significant risks, the auditor may identify controls over those risks to be relevant to the audit. Similar to controls over significant risks, the auditor's evaluation of the design of these controls and determination of whether they have been implemented contributes to the audit evidence related to the higher risk. This understanding of controls may also assist the auditor in designing further audit procedures responsive to the risk.

---

[43] ISA 330, paragraph 8

[44] ISA 330, paragraph 8(a)

[45] ISA 330, paragraph 7(b)

IT Applications and Other Aspects of the IT Environment Relevant to the Audit (Ref: Para 35(d) and 40)

A180. An entity may be using and relying upon IT to accurately process and maintain the integrity of information in the entity's information system relevant to financial reporting. In obtaining the understanding of the IT environment in accordance with paragraph 35(d), the auditor may have obtained information about the nature and number of the IT applications and the complexity of the IT processes in the entity's IT environment. Obtaining a high-level understanding of the extent to which the entity's IT processes include the implementation of general IT controls may assist the auditor in identifying whether there are IT applications on which management is relying for the purposes of financial reporting and that therefore may be IT applications relevant to the audit. In addition, the auditor is required to take into account the matters included in paragraph 39 because these matters may further assist the auditor in identifying those IT applications for which the entity's general IT controls may be relevant to the audit.

A181. In smaller and less complex entities that use commercial software and that do not have access to the source code to make any program changes, the entity may not have any IT processes other than, for example, to process updates to the software received from the vendor. Also, in smaller and less complex entities, management may not be relying on the IT applications, and the controls within them, to maintain the integrity of information. For example, management may instead be relying on reconciliations of information about transactions processed by the IT application to hard copy records or external documents (e.g., reconciliation of cash sales to deposits reported on a bank statement). When an entity uses an IT application that is reputable, widely-used and considered reliable, is unable to change its programming, and maintains hard-copy accounting records, the auditor may determine that there are no IT applications relevant to the audit. In such a case, the auditor is also likely to be able to obtain audit evidence about the completeness and accuracy of the information produced by the entity used as audit evidence through substantive testing without the need to test controls over its production.

A182. In larger entities, the entity may be relying on IT to a greater extent and the IT environment may involve multiple IT applications and the IT processes to manage the IT environment may be complex. When an entity has greater complexity in its IT environment, determining the IT applications and other aspects of the IT environment that are relevant to the audit is likely to require the involvement of team members with specialized skills in IT.

Matters taken into account in identifying IT applications relevant to the audit

A183. Automated controls that may be determined to be relevant to the audit in accordance with paragraph 40 may include, for example, automated calculations or input, processing and output controls, such as a three-way match of a purchase order, shipping document, and vendor invoice. 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.

A184. In considering whether the IT applications in which automated controls exist and reports are generated are relevant to the audit, 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. For system-generated reports to be used as audit evidence, 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 relevant to the audit.

A185. 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 relevant to the audit. 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 relevant to the audit.

A186. 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 application 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 application 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 relevant to the audit.

A187. 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 relevant to the audit 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 relevant to the audit.

Identifying other aspects of the IT environment that are relevant to the audit

A188. The other aspects of the IT environment that may be relevant to the audit include the network, operating system and databases, and in certain circumstances interfaces between IT applications. When there are no IT applications relevant to the audit, other aspects of the IT environment are also not relevant. When there are IT applications relevant to the audit, the other aspects of the IT environment that are relevant to the audit varies based on the extent to which such aspects support and interact with the IT applications determined to be relevant to the audit. The database(s) that stores the data processed by an IT application relevant to the audit is also relevant to the audit. Similarly, because an IT application's ability to operate is often dependent on the operating system, the operating system is typically relevant to the audit. The network may be relevant to the audit, for example, when an IT application interacts with vendors or external parties through the internet.

Risks Arising from the Use of IT and General IT Controls Relevant to the Audit (Ref: Para. 41)

A189. The extent and nature of the risks arising from the use of IT vary depending on the nature and characteristics of the IT applications and other aspects of the IT environment relevant to the audit. Specific IT risks may result when the entity uses third-party hosting for relevant aspects of its IT environment. It is more likely that there will be more IT 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. Examples of risks arising from the use of IT are included in paragraph A145.

A190. General IT controls are implemented to address risks arising from the use of IT. Accordingly, the auditor uses the understanding obtained about the IT applications and other aspects of the IT environment that are relevant to the audit and the related risks arising from the use of IT in determining the general IT controls relevant to the audit. In doing so, the auditor may take an approach of understanding the general IT controls that the entity has established over its IT processes for management of access, program change and IT operations for each IT application or other aspect of the IT environment that is relevant to the audit. 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.

A191. In identifying the risks arising from the use of IT, the auditor may also consider the nature of the IT application or other aspect of the IT environment and the reasons for it being determined to be relevant to the audit. For some IT applications or other aspects of the IT environment, the risks identified may relate primarily to unauthorized access or unauthorized program changes. In the case of databases or data warehouses, the auditor may be focused on the risk of inappropriate changes to the data through direct database access and the ability to directly manipulate information.

A192. In general, a greater number of general IT controls related to IT applications and databases are likely to be relevant to the audit than for other aspects of the IT environment. This is because these aspects are the most closely concerned with the processing and storage of information and most subject to automated controls used 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.

A193. Identifying the risks arising from the use of IT and the general IT controls relevant to the audit is likely to require the involvement of team members with specialized skills in IT, other than for the simplest of IT environments. Such involvement is likely to be essential, and may need to be extensive, for complex IT environments. Appendix 4 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.

Evaluating the Design, and Determining Implementation of, Controls Relevant to the Audit (Ref: Para 42)

A194. Evaluating the design of a control involves considering 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). Implementation of a control means that the control exists and that the entity is using it. There is little point in assessing the implementation of a control that is not designed effectively, and so the design of a control is considered first. An improperly designed control may represent a significant control deficiency.

A195. In making risk assessments, the auditor may identify the controls that are likely to prevent, or detect and correct, material misstatement in specific assertions. Generally, it is useful to obtain an understanding of controls and relate them to risks of material misstatement in the context of processes and, when applicable, IT applications in which they exist. The relationship to IT applications assists with relating the general IT controls relevant to the audit to the controls that they support. In many cases, an individual control may not in itself adequately address a risk of material

misstatement. Often, only multiple controls, together with other components of the system of internal control, will be sufficient to address a risk of material misstatement.

A196. Conversely, some controls may have a specific effect on an individual risk of material misstatement at the assertion level embodied in a particular significant class of transactions or account balance. For example, the controls that an entity 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.

A197. Controls that support other controls are indirect controls. The more indirect the relationship, the less effective that control may be in preventing, or detecting and correcting, misstatements related to the risk of material misstatement. For 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 reducing those risks than controls more directly related thereto, such as matching shipping documents with billing documents. Similarly, a general IT control alone is typically not sufficient to address a risk of material misstatement at the assertion level.

A198. Risk assessment procedures to obtain audit evidence about the design and implementation of controls relevant to the audit 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.

A199. Evaluating the design and determining the implementation of controls relevant to the audit is not sufficient to test their operating effectiveness, unless there is some automation that provides for the consistent operation of the controls. For example, 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. However, the auditor may evaluate the design and determine whether the control has been implemented concurrently with the testing of its operating effectiveness, when, for example, there is some automation that provides for consistent operation of the control and the relevant risks arising from the use of IT have been addressed (e.g., when general IT controls are operating effectively). Tests of the operating effectiveness of controls, including tests of indirect controls, are further described in ISA 330.[46]

A200. Notwithstanding that the risk assessment procedures to obtain audit evidence about the design and implementation of controls relevant to the audit are not sufficient to test the operating effectiveness of controls (and thus assess control risk below the maximum), these procedures provide information important to the auditor's identification and assessment of the risks of material misstatement, and to the design of further audit procedures. In addition to contributing toward the auditor's understanding of the components of the entity's system of internal control, the results of these risk assessment procedures may:

- Influence the auditor's plans to test the operating effectiveness of the controls. When a control is not designed or implemented effectively, there is no benefit in testing it. Conversely, the auditor may conclude that a control, which is effectively designed and implemented, may be

[46] ISA 330, *paragraphs 8–11*

appropriate to test in order to take its operating effectiveness into account in designing substantive procedures. 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.

- Provide the auditor with a greater understanding of the risks of material misstatement, including the identification of additional risks of material misstatement. This understanding is used in designing the nature, timing and extent of substantive audit procedures that are responsive to the risks of material misstatement, including when the auditor does not plan to test the operating effectiveness of the controls. For example, the results of these procedures may inform the auditor's consideration of possible deviations in a population when designing audit samples.
- 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.

Identifying and Assessing the Risks of Material Misstatement

A201. Information gathered by performing risk assessment procedures, including the audit evidence obtained in evaluating the design of controls relevant to the audit and determining whether they have been implemented, is used as audit evidence to support the risk assessment. The risk assessment determines the nature, timing and extent of further audit procedures to be performed in accordance with ISA 330. In identifying and assessing the risks of material misstatement in the financial statements, the auditor exercises professional skepticism in accordance with ISA 200.[47]

A202. The auditor's understanding required by paragraphs 23 to 25, and the identification and assessment of the risks of material misstatement, is an iterative process. For example, the auditor may form initial expectations about the significant classes of transactions, account balances and disclosures based on the understanding of the entity and its environment and the applicable financial reporting framework obtained in accordance with paragraph 23. These expectations may be confirmed or updated as the auditor performs further risk assessment procedures to address the requirements in paragraphs 24 and 25, in particular relating to the auditor's understanding of the entity's information system. Specifically, the auditor may identify additional risks of material misstatement related to the classes of transactions, account balances or disclosures that were expected to be significant, thus confirming their significance. The auditor may also identify risks of material misstatement at the assertion level that are related to classes of transactions, account balances or disclosures not previously considered significant and which may therefore give rise to the identification of additional significant classes of transactions, account balances, or disclosures. (Ref: Para. 45(b) and 46)

The Use of Assertions

A203. In identifying and assessing the risks of material misstatement, the auditor may use the assertions as described in paragraph A204(a)–(b) below or may express them differently provided all aspects described below have been covered. For example, 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.

---

[47] ISA 200, paragraph 15

A204. Assertions used by the auditor in considering the different types of potential misstatements that may occur may fall into the following categories:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A205. The assertions described in paragraph A204(a)–(b) above, adapted as appropriate, may also be used by the auditor in considering the different types of misstatements that may occur in disclosures not directly related to recorded classes of transactions, events, or account balances. As an example of such a disclosure, the entity may be required 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

A206. When making assertions about the financial statements of public sector entities, in addition to those assertions set out in paragraph A204(a)–(b), management may often assert that transactions and events have been carried out in accordance with law, regulation or other authority. Such assertions may fall within the scope of the financial statement audit.

Identifying Risks of Material Misstatement (Ref: Para. 45)

A207. The required understanding of the entity and the environment, the applicable financial reporting framework, and the system of internal control forms the basis for the auditor's identification of risks of material misstatement. 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. Rather, they represent circumstances that may pervasively increase the risks of material misstatement at the assertion level.

A208. Risks of material misstatements that do not relate pervasively to the financial statements are risks of material misstatement at the assertion level. The identification of risks of material misstatement at the assertion level is performed before consideration of any controls. The auditor does so based on a preliminary assessment of inherent risk that involves identifying those risks for which there is a reasonable possibility of material misstatement. The assertions to which such risks of material misstatement relate are relevant assertions, and the classes of transactions, account balances and disclosures to which the relevant assertions relate are significant classes of transactions, account balances and disclosures.

A209. While obtaining the understanding as required by paragraph 23, the auditor takes into account the inherent risk factors. Appendix 2 sets out examples, in the context of the inherent risk factors, of events and conditions that may indicate susceptibility to misstatement that may be material.

Considerations Specific to Public Sector Entities

A210. 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.

Significant Classes of Transactions, Account Balances and Disclosures, and their Relevant Assertions (Ref: Para. 46)

A211. The auditor determines the significant classes of transactions, account balances and disclosures by considering whether there are one or more risks of material misstatement related to the assertions for classes of transactions, account balances and disclosures expected in the financial statements (i.e., whether there is a reasonable possibility of being subject to a misstatement that is material, individually or in combination with other misstatements). When there is a remote possibility of a material misstatement with respect to an assertion, there are no identified risks of material misstatement and the assertion is not relevant. In determining the relevant assertions, the auditor considers the information gathered from the auditor's risk assessment procedures about the identified risks of material misstatement and the assertions that they may affect.

A212. In determining significant classes of transactions, account balances and disclosures from the identified risks of material misstatement, understanding how the inherent risk factors affect the classes of transactions, account balances and disclosures enables the auditor to consider which related assertions may be subject to risks of material misstatement (see paragraph A83).

A213. The auditor may also use automated techniques to confirm whether all significant classes of transactions and account balances have been identified by, for example, analyzing an entire population of transactions to identify 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 actually was comprised of numerous offsetting transactions and journal entries occurring during the period thus indicating that the account balance or class of transactions may be significant (e.g., a "loan processing suspense" account in a financial institution entity).

Identifying Significant Disclosures

A214. Significant disclosures include both quantitative and qualitative disclosures for which there is one or more relevant assertions. Examples of significant disclosures that have qualitative aspects 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 Financial Statement Level (Ref: Para. 47)

A215. Because risks of material misstatement at the financial statement level have a pervasive effect on the financial statements, it may not be possible to identify the specific assertions that are more susceptible to the risk (e.g., risk of management override of controls). In other cases, a number of assertions may be identified as susceptible to the risk, and which may therefore affect the auditor's risk identification and assessment of risks of material misstatement at the assertion level.

A216. The evaluation of whether risks identified relate pervasively to the financial statements as required by paragraph 45(a) supports the auditor's ability to perform the assessment of the risks of material misstatement at the financial statement level as required by paragraph 47. The determination of the effect of the risks of material misstatement at the financial statement level on the risks of material misstatement at the assertion level as required by paragraph 47(a) is taken into account in the auditor's assessment of inherent risk at the assertion level in accordance with paragraph 48(b).

A217. Risks of material misstatement due to fraud may be particularly relevant to the auditor's consideration of the risks of material misstatement at the financial statement level. For example, the risk of management override of controls may pervasively affect the risks of material misstatement at the assertion level, although the auditor may consider particular assertions to have a greater potential for misstatement based on greater susceptibility to management bias or fraud.

A218. 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, including the outcome of the evaluations required by paragraphs 28 and 31(b) and any control deficiencies identified in accordance with paragraph 43. 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.

A219. The auditor's understanding of the control environment and other components of the system of internal control may raise doubts about the auditability of an entity's financial statements, such that it may affect the auditor's opinion or be cause for withdrawal from the engagement. For example:

- Concerns about the integrity of the entity's management may be so serious as to cause the auditor to conclude that the risk of management misrepresentation in the financial statements is such that an audit cannot be conducted.
- Concerns about the condition and reliability of an entity's records may cause the auditor to conclude that it is unlikely that sufficient appropriate audit evidence will be available to support an unmodified opinion on the financial statements.

A220. ISA 705 (Revised)[48] 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.

Assessing Risks of Material Misstatement at the Assertion Level

Assessing Inherent Risk (Ref: Para. 48)

Assessing the Likelihood and Magnitude of the Risks of Material Misstatement at the Assertion Level (Ref: Para: 48(a))

A221. The degree to which events or conditions relating to significant classes of transactions, account balances and disclosures are subject to, or affected by, the inherent risk factors affects the degree to which such events and conditions are susceptible to misstatement. The 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 disclosures is susceptible to material misstatement, the higher the inherent risk assessment is likely to be.

A222. The relative degrees of the likelihood and magnitude of a possible misstatement determine where on the spectrum of inherent risk the risk of misstatement is assessed. The higher the combination of likelihood and magnitude, the higher the inherent risk; the lower the combination of likelihood and magnitude, the lower the inherent risk. When considering the potential magnitude of the misstatement, the quantitative and qualitative aspects of the potential misstatement may be relevant. A higher inherent risk assessment may also arise from different combinations of likelihood and magnitude, for example a higher risk assessment could result from a lower likelihood but a very high magnitude. Determining the combination of the likelihood and potential magnitude of a possible misstatement is a matter of the auditor's professional judgment. Significant risks, which are identified in accordance with paragraph 49, are those close to the upper end of the spectrum of inherent risk.

---

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

A223. Misstatements in assertions about classes of transactions, account balances or disclosures may be judged to be material due to size, nature or circumstances.

A224. The assessment of inherent risks for individual risks of material misstatement in relation to audits of smaller and less complex entities may be such that a greater proportion of such risks are assessed close to the lower end of the spectrum of inherent risk.

A225. In order to develop appropriate strategies for responding to risks of material misstatement, the auditor may designate risks of material misstatement within relative categories along the spectrum of inherent risk, based on their assessment of inherent risk. These relative categories may be described in different ways, for example audit methodologies may use numerical categorizations (e.g., on a scale of one to ten), or the relative placement on the spectrum of inherent risk may be described (e.g., high, medium, low). 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 responsive to the assessment of inherent risk and the reasons for that assessment.

A226. In assessing the identified risks of material misstatement at the assertion level, the auditor may conclude that some risks of material misstatement relate more pervasively to the financial statements as a whole and potentially affect many assertions, in which case the auditor may update the identification of risks of material misstatement at the financial statement level.

A227. In circumstances in which risks of material misstatement are identified as financial statement level risks due to their pervasive effect on a number of assertions and that effect is identifiable with specific assertions, the auditor takes into account the evaluation required by paragraph 47(b), including those assertions identified that are affected by those risks when assessing the inherent risk for risks of material misstatement at the assertion level. (Ref: Para. 48(b))

Considerations specific to public sector entities

A228. In exercising professional judgment as to the assessment of the risk of material misstatement, public sector auditors may consider the complexity of the regulations and directives, and the risks of non-compliance with authorities.

Significant Risks (Ref: Para. 49)

A229. In determining significant risks, the auditor may first identify those assessed inherent risks that have been assessed close to the upper end of the spectrum of inherent risk. The determination of which of the assessed inherent risks 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 (see paragraph A230). Routine, non-complex transactions that are subject to systematic processing are less likely to give rise to significant risks because these are likely to give rise to risks of material misstatement at the assertion level that are assessed as close to the lower end on the spectrum of inherent risk. However, risks of material misstatement that may be assessed as having higher inherent risk and may therefore be assessed as significant risks, may arise from matters such as the following:

- Transactions for which there are multiple acceptable accounting treatments such that subjectivity is involved.
- Accounting estimates that have high estimation uncertainty or complex models.
- Complexity in data collection and processing to support account balances.

- Account balances or quantitative disclosures that involve complex calculations
- Accounting principles that may be subject to differing interpretation.
- Changes in the entity's business that involve changes in accounting, for example, mergers and acquisitions.

A230. Significant risks include those risks of material misstatement that are treated as significant in accordance with the requirements of other ISAs. ISA 240 provides further requirements and guidance in relation to the identification and assessment of the risks of material misstatement due to fraud.[49]

Implications for the audit

A231. ISA 330 describes the consequences for further audit procedures of identifying a risk as significant. When a risk is assessed as a significant risk, the implications for the audit include the design and implementation of an appropriate response to address the assessed risk, which may include for example the use of more experienced engagement team members, including those with specialized skills, to perform audit procedures or audit work may involve the use of experts. In addition, the ISAs set out required responses, including:

- Controls that address significant risks are required to be identified as relevant to the audit in accordance with paragraph 39.
- 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.[50]
- ISA 330 requires the auditor to obtain more persuasive audit evidence the higher the auditor's assessment of risk.[51]
- ISA 260 (Revised) requires communicating with those charged with governance about the significant risks identified by the auditor.[52]
- 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.[53]
- Review of audit documentation by the engagement partner on or before the date of the auditor's report which allows significant matters, including significant risks, to be resolved on a timely basis to the engagement partner's satisfaction.[54]
- 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.[55]

---

49 ISA 240, paragraphs 25–27

50 ISA 330, paragraphs 15 and 21

51 ISA 330, paragraph 7(b)

52 ISA 260 (Revised), paragraph 15

53 ISA 701, *Communicating Key Audit Matters in the Independent Auditor's Report*, paragraph 9

54 ISA 220, paragraphs 17 and A18

55 ISA 600, paragraphs 30 and 31

The nature, timing and extent of the involvement of individuals with specialized skills and knowledge may vary throughout the audit.

Assessing Control Risk (Ref: Para. 50)

A232. The auditor's intention to test the operating effectiveness of controls provides the basis for the auditor's assessment of control risk. In assessing control risk, the auditor takes into account the expectation about the operating effectiveness of the controls (based on the auditor's evaluation of the design effectiveness and implementation of the controls set out in paragraph 42).

A233. 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. For example, if control risk is assessed as maximum, the auditor contemplates no expectation of the operating effectiveness of controls. If control risk is assessed at less than maximum, the auditor contemplates an expectation of the operating effectiveness of controls.

A234. If a risk of material misstatement is addressed by one or more controls, the auditor takes into account whether one, or a combination of controls, will address the assessment of inherent risk.

A235. The assessment of control risk takes into account the expected results from the auditor's planned tests of the operating effectiveness of controls relevant to the audit, including general IT controls. For controls relevant to the audit as determined in accordance with paragraph 39, and for which the auditor intends to test the operating effectiveness, the auditor may identify related general IT controls as relevant to the audit in accordance with paragraph 41. For example, 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 application control to address the risks arising from the use of IT, and to provide a basis for the auditor's expectation that the application control operated effectively throughout the period. When the auditor expects general IT controls that have been determined to be relevant to the audit to be ineffective, this determination may affect the auditor's assessment of control risk at the assertion level depending on whether the auditor is able to perform other tests to address those 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.[56]

Risks for Which Substantive Procedures Alone Cannot Provide Sufficient Appropriate Audit Evidence (Ref: Para. 51)

A236. Risks of material misstatement may relate directly to the recording of routine classes of transactions or account balances, and the preparation of reliable financial statements. Such risks may include risks of inaccurate or incomplete processing for routine and significant classes of transactions such as an entity's revenue, purchases, and cash receipts or cash payments.

A237. Where such 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. For example, the auditor may consider this to be the case in circumstances where a significant amount of an entity's information is initiated, recorded, processed, or reported only in

[56] ISA 330, paragraphs A29–A31

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.

A238. ISA 540 (Revised) provides further guidance related to accounting estimates about risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence.[57]

A239. Paragraph 39 requires the identification of controls that address risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence to be relevant to the audit because the auditor is required, in accordance with ISA 330,[58] to design and perform tests of such controls.

Classes of Transactions, Account Balances and Disclosures that are Not Significant, but are Material (Ref: Para. 52)

A240. As explained in ISA 320,[59] 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 reporting needs of users of the financial statements.[60] Classes of transactions, account balances or disclosures are quantitatively or qualitatively material if omitting, misstating or obscuring information about them could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements as a whole.

A241. There may be classes of transactions, account balances or disclosures that are quantitatively or qualitatively material but have not been determined to be significant classes of transactions, account balances or disclosures (i.e., there are no relevant assertions identified). For example, the entity may have a disclosure about executive compensation for which the auditor has not identified a risk of material misstatement. However, the auditor may determine that this disclosure is material based on the consideration in paragraph A240.

A242. Audit procedures to address classes of transactions, account balances or disclosures that are quantitatively or qualitatively material but are not determined to be significant are addressed in ISA 330.[61] When a class of transactions, account balance or disclosure is determined to be significant as required by paragraph 46, the class of transactions, account balance or disclosure, is also treated as a material class of transactions, account balance or disclosure for the purposes of paragraph 18 of ISA 330.

Revision of Risk Assessment (Ref: Para. 53)

A243. During the audit, information may come to the auditor's attention that differs significantly from the information on which the risk assessment was based. For example, the risk assessment may be

---

57 ISA 540 (Revised), paragraphs A87–A89

58 ISA 330, paragraph 8

59 ISA 320, paragraph A1

60 ISA 320, paragraph 4

61 ISA 330, paragraph 18

based on an expectation that certain controls are operating effectively. In performing tests of those controls, the auditor may obtain audit evidence that they were not operating effectively at relevant times during the audit. Similarly, in performing substantive procedures the auditor may detect misstatements in amounts or frequency greater than is consistent with the auditor's risk assessments. In such circumstances, the risk assessment may not appropriately reflect the true circumstances of the entity and the further planned audit procedures may not be effective in detecting material misstatements. Paragraphs 16 and 17 of ISA 330 provide further guidance about evaluating the operating effectiveness of controls.

Documentation (Ref: Para. 54)

A244. The manner in which the requirements of paragraph 54 are documented is for the auditor to determine using professional judgment. For example, in audits of smaller and less complex entities the documentation may be incorporated in the auditor's documentation of the overall strategy and audit plan.[62] 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 procedures.[63] 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.

A245. More detailed documentation may be required where the auditor applies a higher level of professional judgment, for example when exercising professional judgment to support the rationale for difficult judgments made. 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.

A246. For the audits of smaller and less complex entities, the form and extent of documentation may be simple in form and relatively brief. It is not necessary to document the entirety of the auditor's understanding of the entity and matters related to it. Key elements of understanding documented by the auditor may include those on which the auditor based the assessment of the risks of material misstatement.

A247. For recurring audits, certain documentation may be carried forward, updated as necessary to reflect changes in the entity's business or processes.

---

62 ISA 300, *Planning an Audit of Financial Statements*, paragraphs 7 and 9

63 ISA 330, paragraph 28

Appendix 1

(Ref: Para. 23(a)(i), A57)

Considerations for Understanding the Entity and its Business Model

The appendix provides further matters that the auditor may consider in understanding the entity and its business model.

Activities of the Entity

1. 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 partnerships, joint ventures and special-purpose entities.

   (c) Financing and financing activities such as:

   - 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 (local, foreign, business reputation and experience) and related parties.
- Use of derivative financial instruments.

Nature of Special-Purpose Entities

2. 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.[64]

3. 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.

[64] ISA 550, paragraph A7

Appendix 2

(Ref: Para. A60, A83, A209)

Events and Conditions That May Indicate Susceptibility to Risks of Material Misstatement

In obtaining the understanding of the entity and its environment and the applicable financial reporting framework in accordance with paragraph 23, the auditor considers whether and, if so, how events and conditions are subject to by, or affected by, the inherent risk factors.

The following are examples of events and conditions that may indicate the existence of risks of material misstatement in the financial statements, either 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 the 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.

Inherent Risk Factors at the Assertion Level

***Complexity**:*

Regulatory:

- Operations that are subject to a high degree of complex regulation.

Business model:

- The existence of complex alliances and joint ventures.

Applicable financial reporting framework:

- Accounting measurements that involve complex processes.

Transactions:

- Use of off balance sheet finance, special-purpose entities, and other complex financing arrangements.

***Subjectivity*:**

Applicable financial reporting framework:

- A wide range of possible measurement criteria of an accounting estimate. For example, management's recognition of depreciation or construction income and expenses.
- Management's selection of a valuation technique or model for a non-current asset, such as investment properties.

***Change*:**

Economic conditions:

- Operations in regions that are economically unstable, for example, countries with significant currency devaluation or highly inflationary economies.

Markets:

- Operations exposed to volatile markets, for example, futures trading.

Customer loss:

- Going concern and liquidity issues including loss of significant customers.

Industry model:

- Changes in the industry in which the entity operates.

Business model:

- Changes in the supply chain.
- Developing or offering new products or services, or moving into new lines of business.

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.

***Uncertainty*:**

Reporting:

- Events or transactions that involve significant measurement uncertainty, including accounting estimates, and related disclosures.
- Pending litigation and contingent liabilities, for example, sales warranties, financial guarantees and environmental remediation.

***Susceptibility to misstatement due to management bias or fraud*:**

Reporting:

- Opportunities for management and employees to engage in fraudulent financial reporting, including omission, or obscuring, of significant information in disclosures.

Transactions:

- Significant transactions with related parties.

- Significant amount of non-routine or non-systematic transactions including intercompany transactions and large revenue transactions at period end.
- Transactions that are recorded based on management's intent, for example, debt refinancing, assets to be sold and classification of marketable securities.

Other Inherent Risk Factors

- Constraints on the availability of capital and credit.
- Inconsistencies between the entity's IT strategy and its business strategies.
- Investigations into the entity's operations or financial results by regulatory or government bodies.

***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, especially those not addressed by management.
- Past misstatements, history of errors or a significant amount of adjustments at period end.

Appendix 3

(Ref: Para. 16(f), 27–38, A51, A92, A105–A165)

Understanding the Entity's System of Internal Control

1. 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 16(f), 27–38, A51, A92 and A105–A165, as they relate to a financial statement audit.

Components of the System of Internal Control

Control Environment

2. The control environment encompasses the following elements:

   (a) *How the entity demonstrates a 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) *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 significantly by those charged with governance. Considerations 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 has established, with oversight from those charged with governance, structures, reporting lines, and appropriate authorities and responsibilities in pursuit of its objectives.* This includes 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 resource 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.

The appropriateness of an entity's organizational and governance structure depends, in part, on its size and the nature of its activities.

(d) *How the entity demonstrates a commitment to attract, develop, and retain 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 internal control responsibilities in pursuit of its objectives.* This may be accomplished through, for example:

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

Entity's Risk Assessment Process

3. 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 respond to and 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.

4. 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 accept a risk because of cost or other considerations. Risks can arise or change due to circumstances such as the following:

- *Changes in operating environment*. Changes in the regulatory, 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 system of internal control.
- *New or revamped information systems*. 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 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 (including cyber security risks);
    - Risks to the entity business strategy that arise if the entity's IT strategy does not effectively supporting 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

5. An important management responsibility is to establish and maintain the entity's system of internal control on an ongoing basis. Management's process to monitor the system of internal control includes considering whether controls are operating as intended and that they are modified as appropriate for changes in conditions. The entity's process to monitor the 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.

6. When distinguishing between a monitoring activity and a control in the control activities component, the underlying details of the activity are considered, especially where the activity involves some level of supervisory review. As also explained in the application material, 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 in the control activities component or a monitoring activity. For example, the intent of a monthly completeness control in the control activities component would be to detect and correct errors, where a monitoring activity would ask why errors are occurring and assign management the responsibility of fixing the process to prevent future errors. In simple terms, a control in the control activities component responds to a specific risk, whereas a monitoring activity assesses whether controls within each of the five components of the system of internal control are operating as intended.

7. 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 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 system of internal control from external auditors.

Use of internal audit

8. 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 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.

9. 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 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 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.

The Information System and Communication

10. The information system relevant to financial reporting encompasses policies, procedures and records that:

    - Identify and record all valid transactions.
    - Describe on a timely basis the transactions in sufficient detail to permit proper classification of transactions for financial reporting.
    - Measure the value of transactions in a manner that permits recording their proper monetary value in the financial statements.

- Determine the time period in which transactions occurred to permit recording of transactions in the proper accounting period.
- Present properly the transactions and related disclosures in the financial statements.
- Capture, process and disclose information about events and conditions other than transactions.

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

12. 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.

Control Activities

13. Controls in the control activities component consist of application controls and general IT controls, both of which may be manual or automated in nature, and 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 where 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 and, 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 perform 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, of 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 he or she could, for example, create a fictitious sale that could go undetected. Similarly, salespersons should not have the ability to modify product price files or commission rates.

  Sometimes segregation is not practical, cost effective, or feasible. For example, smaller and less complex entities may lack sufficient resources to achieve ideal segregation, and the cost of hiring additional staff may be prohibitive. In these situations, management institutes 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.

14. Certain controls in the control activities component 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.

Benefits of IT

15. 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 applications, databases, and operating systems.

Limitations of internal control

16. 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 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 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.

17. Additionally, controls can be circumvented by the collusion of two or more people or inappropriate management override of internal control. For example, management may enter into side agreements with customers that alter the terms and conditions of the entity's standard sales 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.

18. 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. A193)

Considerations for Understanding General IT Controls

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

1. The nature of the general IT controls (GITCs) 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 are also 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 be exist by IT process include:

   (a) Process to manage access:

   - *Authentication*

     Controls that ensure a user accessing the IT application or other aspect of the IT environment is using their 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.