KAEG-I [INTL VERSION 2024]: ISA 315 (Revised 2019) Identifying and Assessing the Risks of Material Misstatement

Contents

KAEG-I [INTL VERSION]: ISA 315 (Revised 2019) Identifying and Assessing the Risks of Material Misstatement [ISA | KAEGISA315]

Understanding the Entity and Its Environment, and the Applicable Financial Reporting Framework

International Standards on Auditing: ISA 315.19-20

ISA Application and Other Explanatory Material: ISA 315.A48-A89

How do we comply with the standards?

Control environment

International Standards on Auditing: ISA 315.21

ISA Application and Other Explanatory Material: ISA 315.A96-A108

How do we comply with the standards?

The entity's risk assessment process

International Standards on Auditing: ISA 315.22-23

ISA Application and Other Explanatory Material: ISA 315.A96-A98 | ISA 315.A109-A113

How do we comply with the standards?

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

International Standards on Auditing: ISA 315.24

ISA Application and Other Explanatory Material: ISA 315.A96-A98 | ISA 315.A114-A122

How do we comply with the standards?

The information system and communication

International Standards on Auditing: ISA 315.25

ISA Application and Other Explanatory Material: ISA 315.A123-A146

How do we comply with the standards?

Control Activities

International Standards on Auditing: ISA 315.26

ISA Application and Other Explanatory Material: ISA 315.A123-A130 | ISA 315.A147-A181

How do we comply with the standards?

Evaluating the Audit Evidence Obtained from the Risk Assessment Procedures

International Standards on Auditing: ISA 315.35

ISA Application and Other Explanatory Material: ISA 315.A230-A232

How do we comply with the standards?

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

International Standards on Auditing: ISA 315.36

ISA Application and Other Explanatory Material: ISA 315.A233-A235

How do we comply with the standards?

Revision of Risk Assessment

International Standards on Auditing: ISA 315.37

ISA Application and Other Explanatory Material: ISA 315.A236

How do we comply with the standards?

Documentation

International Standards on Auditing: ISA 315.38

ISA Application and Other Explanatory Material: ISA 315.A237-A241

How do we comply with the standards?

Considerations for Understanding the Entity and its Business Model

International Standards on Auditing: ISA 315.Appendix 1

How do we comply with the standards?

Understanding Inherent Risk Factors

International Standards on Auditing: ISA 315.Appendix 2

How do we comply with the standards?

Understanding the Entity's System of Internal Control

International Standards on Auditing: ISA 315.Appendix 3

How do we comply with the standards?

ISA 315 (Revised 2019) Identifying and Assessing the Risks of Material Misstatement

View the Full Chapter for this Standard

ISA 315 (Revised 2019) *Identifying and Assessing the Risks of Material Misstatement*

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

Introduction, Objective and Definitions

International Standards on Auditing: ISA 315.01-12

Introduction

Scope of this ISA

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

Key Concepts in this ISA

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

_____

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

2 ISA 200, paragraph 17

3 ISA 200, paragraph 13(c)

4 ISA 200, paragraph A36

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

_____

5 ISA 200, paragraphs 15-16

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

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

5. ISA 200 explains that risks of material misstatement are assessed at the assertion level in order to determine the nature, timing and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence.[6] For the identified risks of material misstatement at the assertion level, a separate assessment of inherent risk and control risk is required by this ISA. As explained in ISA 200,

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

---

6 ISA 200, paragraph A43a and ISA 330, The Auditor's Responses to Assessed Risks, paragraph 6

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

---

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

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

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

---

8 ISA 330, paragraph 5

9 ISA 330, paragraph 6

Scalability

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

---

10 ISA 200, paragraph A65a

Effective Date

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

Objective

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

Definitions

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

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

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

(c) *Controls* - Policies or procedures that an entity establishes to achieve the control objectives of management or those charged with governance. In this context: (Ref: Para. A2-A5)

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

(ii) Procedures are actions to implement policies.

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

(e) *Information processing controls* - Controls relating to the processing of information in IT applications or manual information processes in the entity's information system that directly address risks to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information). (Ref: Para. A6)

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) Control environment;

(ii) The entity's risk assessment process;

(iii) The entity's process to monitor the system of internal control;

(iv) The information system and communication; and

(v) Control activities.

---

11 ISA 240, paragraphs A24.A27

12 ISA 240, paragraph 27 and ISA 550, Related Parties, paragraph 18

ISA Application and Other Explanatory Material: ISA 315.A1-A10

Application and Other Explanatory Material

Definitions (Ref: Para. 12)

Assertions (Ref: Para. 12(a))

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

---

14 ISA 580, Written Representations

Controls (Ref: Para. 12(c))

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A10. Significance can be described as the relative importance of a matter, and is judged by the auditor in the context in which the matter is being considered. For inherent risk, significance may be considered in the context of how, and the degree to which, inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur.

Risk Assessment Procedures and Related Activities

International Standards on Auditing: ISA 315.13-18

Requirements

Risk Assessment Procedures and Related Activities

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

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

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

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

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

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

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

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

Information from Other Sources

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

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

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

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

Engagement Team Discussion

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

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

ISA Application and Other Explanatory Material: ISA 315.A11-A47

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

A11. The risks of material misstatement to be identified and assessed include both those due to fraud and those due to error, and both are covered by this ISA. However, the significance of fraud is such that further requirements and guidance are included in ISA 240 in relation to risk assessment procedures and related activities to obtain information that is used to identify and assess the risks of material misstatement due to fraud.[15] In addition, the following ISAs provide further requirements and guidance on identifying and assessing risks of material misstatement regarding specific matters or circumstances:

- ISA 540 (Revised)[16] in regard to accounting estimates;
- ISA 550[22] in regard to related party relationships and transactions;

- ISA 570 (Revised)[17] in regard to going concern; and
- ISA 600 (Revised)[18] in regard to group financial statements.

---

15 ISA 240, paragraphs 12-27

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

17 ISA 570 (Revised), Going Concern

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

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

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

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

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

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

Sources of Audit Evidence (Ref: Para. 13)

A15. Designing and performing risk assessment procedures to obtain audit evidence in an unbiased manner may involve obtaining evidence from multiple sources within and outside the entity. However, the auditor is not required to perform an exhaustive search to identify all possible sources of audit evidence.

In addition to information from other sources[19], sources of information for risk assessment procedures may include:

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

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

19 See paragraphs A37 and A38.

20 ISA 500, Audit Evidence, paragraph 7

Scalability (Ref: Para. 13)

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

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

Examples:

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

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

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

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

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

21 ISA 500, paragraphs A14-A17 and A21-A25

22 ISA 500, paragraph A12

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

Automated Tools and Techniques (Ref: Para. 14)

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

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

Why Inquiries Are Made of Management and Others Within the Entity

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

A23. Inquiries of management and those responsible for financial reporting and of other appropriate individuals within the entity and other employees with different levels of authority may offer the auditor varying perspectives when identifying and assessing risks of material misstatement.

Examples:

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

- Inquiries directed towards IT personnel may provide information about system changes, system or control failures, or other IT-related risks.

---

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

Considerations Specific to Public Sector Entities

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

Inquiries of the Internal Audit Function

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

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

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

Considerations specific to public sector entities

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

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

Why Analytical Procedures Are Performed as a Risk Assessment Procedure

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

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

Types of Analytical Procedures

A29. Analytical procedures performed as risk assessment procedures may:

- Include both financial and non-financial information, for example, the relationship between sales and square footage of selling space or volume of goods sold (non-financial).

- Use data aggregated at a high level. Accordingly, the results of those analytical procedures may provide a broad initial indication about the likelihood of a material misstatement.

Example:

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

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

_____

24 ISA 520, Analytical Procedures

Automated tools and techniques

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

Example:

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

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

Why Observation and Inspection Are Performed as Risk Assessment Procedures

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

Scalability

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

Examples:

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

Observation and Inspection as Risk Assessment Procedures

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

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

Automated tools and techniques

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

Considerations Specific to Public Sector Entities

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

Information from Other Sources (Ref: Para. 15)

Why the Auditor Considers Information from Other Sources

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

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

Other Relevant Sources

A38. Other relevant sources of information include:

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

---

25 ISA 220, Quality Management for an Audit of Financial Statements, paragraph 22 - 24

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

Why information from previous audits is important to the current audit

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

Nature of the Information from Previous Audits

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

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

A41. The auditor is required to determine whether information obtained from the auditor's previous experience with the entity and from audit procedures performed in previous audits remains relevant and reliable, if the auditor intends to use that information for the purposes of the current audit. If the nature or circumstances of the entity have changed, or new information has been obtained, the information from prior periods may no longer be relevant or reliable for the current audit. To determine whether changes have occurred that may affect the relevance or reliability of such information, the auditor may make inquiries and perform other appropriate audit procedures, such as walk-throughs of relevant systems. If the information is not reliable, the auditor may consider performing additional procedures that are appropriate in the circumstances.

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

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

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

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

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

---

26 ISA 240, paragraph 16

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

Scalability

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

A45. When an engagement is carried out by a large engagement team, such as for an audit of group financial statements, it is not always necessary or practical for the discussion to include all members

in a single discussion (for example, in a multi-location audit), nor is it necessary for all the members of the engagement team to be informed of all the decisions reached in the discussion. The engagement partner may discuss matters with key members of the engagement team including, if considered appropriate, those with specific skills or knowledge, and those responsible for the work to be performed at components, while delegating discussion with others, taking into account the extent of communication considered necessary throughout the engagement team. A communications plan, agreed by the engagement partner, may be useful.

Discussion of Disclosures in the Applicable Financial Reporting Framework

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

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

Considerations Specific to Public Sector Entities

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

How do we comply with the Standards?

[ISA | KAEGHDWC]

1 Design and perform risk assessment procedures

[ISA | 341]

What do we do?

Design and perform procedures to identify and assess risks of material misstatements.

Why do we do this?

Our risk assessment aims to identify risks of misstatement (RM) and assess those that are risks of material misstatement (RMMs) so we can design and execute responses.

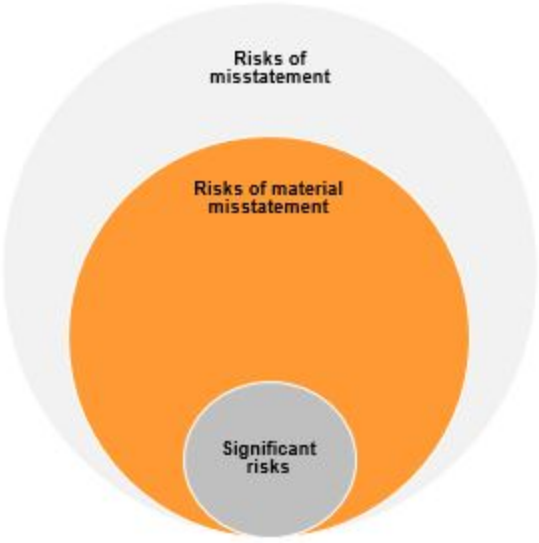
Risk assessment is essential to an audit. The appropriateness and sufficiency of our audit response - e.g. tests of controls, substantive procedures - depend on our ability to identify and assess the relevant RMMs. If we don't, we can't design and perform audit procedures that will address these risks.

Execute the Audit

What is a risk of material misstatement? [ISA | 341.1300]

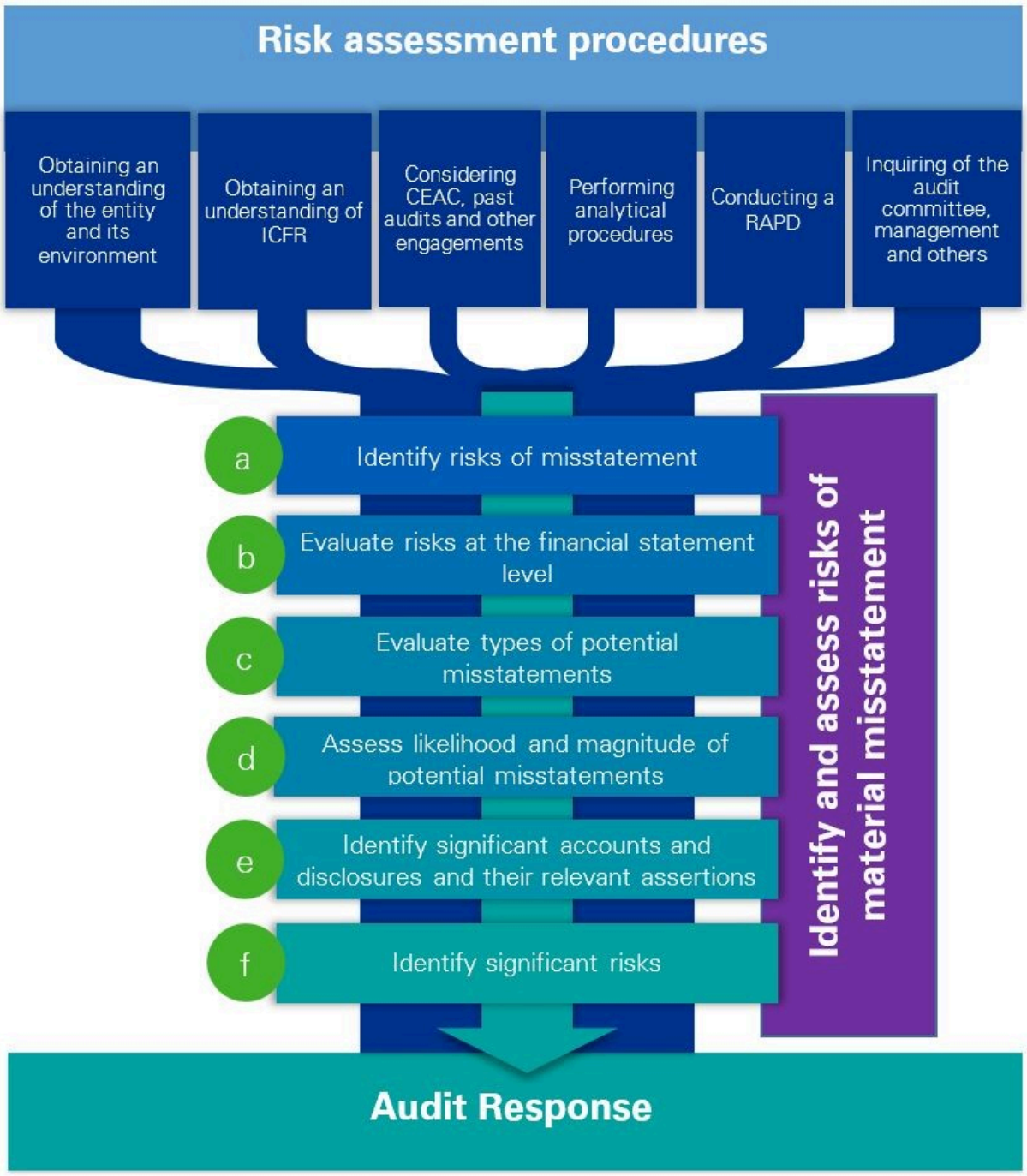
A risk of material misstatement (RMM) is a risk that could result in a *material* misstatement to the financial statements.

In practice, RMMs represent a subset of the total population of risks of misstatement. They are more broadly defined as those risks with a 'reasonable possibility' of resulting in misstatements, individually or in combination with others, that are material to the financial statements. 'Reasonable possibility' means a more than remote possibility, and is therefore a low threshold. We assess both risks due to error and risks due to fraud.



What risk assessment procedures do we design and perform? [ISA | 341.1500]

Our risk assessment procedures are outlined in the visual below. We design and perform our risk assessment procedures with a specific purpose in mind: to collect information to identify and assess risks of material misstatement and to enable us to design appropriate audit procedures in response to the identified risks. These risks will then drive our audit responses.



Our risk assessment procedures also include observation and inspection. For example, observing or inspecting the entity's operations, premises and facilities, documents and reports such as meeting minutes, business plans etc.

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

Why do we obtain audit evidence in an unbiased manner? [ISA | 341.6692]

Obtaining audit evidence in an unbiased manner is important as it may assist us in identifying potentially contradictory information, which may assist us in exercising professional skepticism in identifying and assessing the risks of material misstatement.

See 'Apply professional skepticism' for more information related to professional skepticism.

What incremental risk assessment procedures do we perform over accounting estimates? [ISA | 341.8433]

When assessing risk related to accounting estimates, we perform the incremental procedures at Perform risk assessment procedures related to accounting estimates.

1.1.1 Determine the nature of inquiries about RMMs [ISA | 558]

What do we do?

Determine the nature of the inquiries about risks of material misstatement using our knowledge of the entity and its environment, as well as information from other risk assessment procedures and our understanding of internal controls

Why do we do this?

Our knowledge of the entity and information from other risk assessment procedures may indicate the existence of risks of material misstatement (RMMs).

We therefore use this knowledge to determine the nature of our inquiries with those charged with governance, management, the internal audit function (where it exists) and others about RMMs that may exist.

Execute the Audit

How do we determine the nature of our inquiries about RMMs? [ISA | 558.1300]

We determine the nature of our inquiries about RMMs by:

- drawing on our knowledge of the entity and its environment, and information from other risk assessment procedures; and
- tailoring our questions to the individual of whom we are inquiring.

Our knowledge from other risk assessment procedures can help us specifically tailor our inquiries to learn additional information about topics that are relevant to the audit and the identification and assessment of RMMs.

How may we tailor our questions? [ISA | 558.11548]

To get the best results, we tailor our questions to the subject of our inquiry.

Our goal is to ask questions about topics relevant to the individual and their role at the entity, and to obtain information relevant to identifying and assessing RMMs.

When planning our questions, we remember that not every inquiry needs to be an invasive interrogation.

For example, suppose we're inquiring of the Financial Controller. We may ask questions that focus on the accounting for specific transactions.

But when we inquire of those charged with governance, we may ask questions that focus on the overall entity.

Alternatively, when thinking about risks in revenue accounts, we may want to make specific inquiries of:

- the VP of Sales, about sales arrangements with multiple elements or complex terms; but
- the Chief Operations Officer, about technological feasibility, and research and development costs.

What inquiries do we make? [ISA | 558.1400]

At minimum, we make those inquires in the 'Inquiries agenda'. Some inquiries of specific parties are presumed mandatory — including management, those charged with governance, those within the internal audit function and others. These inquiries are summarized in the 'Inquiries agenda https://alex.kpmg.com/AROWeb/document/lfc/GO_KCW_Links_required_inquiries_documents'.

However, we use our knowledge of the entity and its environment, as well as information from our other risk assessment procedures, to determine the nature of our inquiries.

Example

What inquiries may we make about RMMs? [ISA | 558.11549]

The table below sets out examples of inquiries we may make, responses we may receive, and how we might evaluate those responses.

Inquiry of	Question asked	Response received	RMM(s) identified in relation to...
Audit Committee Chair	How do you comply with laws and regulations, and have you received any violation notices?	We received a notice that we violated an environmental remediation law.	An unrecorded liability for environmental remediation for the period of non-compliance
Chief Executive Officer	What have been the significant changes in the business or environment?	We recently finished testing a new product that will be released this year.	Revenue recognition for the new product and how the entity capitalizes and amortizes product development costs

Chief Financial Officer	How do you budget or forecast financial performance?	We recently reviewed our budgeting process and found that management has compiled fairly aggressive forecasts.	Estimates that are based on the entity's forecasts and projected financial information
General Counsel	What litigation, claims, or assessments is the entity involved with?	Recently, there's been an increase in inquiry claims about sales of defective machinery.	The entity's returns allowance and/or its accrual for liabilities arising from these claims
Chief Information or Technology Officer	Have there been any significant changes in your IT systems?	We recently implemented a new general ledger IT system.	The entity's implementation and use of the new general ledger IT system

1.1.C Core and Less Complex | Inquire of management and others about RMMs [ISA | 7737]

What do we do?

Inquire of management, the internal audit function and others about risks of material misstatement

Why do we do this?

We inquire of individuals we deem likely to have information and perspectives relevant to our risk assessment. In making these inquiries, we seek to:

- better understand their personal views;
- identify and assess additional risks we may not have considered yet; and
- confirm our understanding of the risks we've already identified.

Execute the audit

Core and Less Complex | Who do we inquire of? [ISA | 7737.6233]

We inquire of individuals whom we reasonably expect to have information that could lead us to identify and assess a risk of material misstatement (RMM). These include:

- key members of management;
- members of internal audit (if an internal audit function exists); and
- individuals in other positions who could have insight and information about RMMs, we may, for example, inquire of those charged with governance

Suppose we're seeking information on a home repair project.

We would likely ask others with previous experience, or perhaps someone who works in home improvement. Asking a doctor, despite holding them in high esteem, is unlikely to help (unless they, too, have experience in home repairs).

Similarly, during risk assessment, if we're looking for information on the entity's plans for implementing accounting policies, asking the Vice President of Operations may not be as effective as inquiring of the Chief Accounting Officer.

This isn't to say that we limit our inquiries to only those individuals in the accounting department. Individuals throughout the entity may have different views and information that can help us identify and assess RMMs.

It doesn't hurt to inquire of someone who ultimately has no useful information, but it *can* hurt if we omit someone who could provide helpful information.

So as a general rule of thumb: when in doubt, inquire.

Core and Less Complex | Who are 'those charged with governance' for a private entity? [ISA | 7737.6234]

A private entity may or may not have an audit committee, board of directors or equivalent body. In that case, if we choose to inquire of those charged with governance we inquire of the person(s) who oversee the entity's accounting and financial reporting processes and audits of the entity's financial statements. Those charged with governance could include management personnel — e.g. executive members of a governance board — or an owner-manager.

When do we make our inquiries? [ISA | 7737.1500]

We make our inquiries:

- early enough in the audit to help us identify and assess RMMs; and
- as necessary throughout the audit.

Our aim is to gather information for our risk assessment — so making our inquiries too late in the audit will be ineffective, and the information may not help us plan the audit.

However, risk assessment is an iterative process — so making these inquiries is not a 'check the box' exercise that we complete and then file away.

We may find it appropriate to make additional inquiries, or to probe into a matter we inquired about previously. For example, if we become aware of a new material claim against the entity, we'll likely inquire about it again — even though we've already discussed litigations, claims and assessments.

Further, we try to make all our inquiries of a specific individual at once. So we think about other inquiries that other standards ask us to make, or which are relevant to include — e.g. fraud, related party transactions, significant transactions etc.

For example, when meeting with the CEO, we may take the opportunity to inquire about several matters at once — rather than hold a series of meetings. However, it may be necessary to inquire again when we obtain new or conflicting information.

Who makes the inquiries? [ISA | 7737.1600]

Inquiries are made by an engagement team member with the appropriate level of knowledge, experience and stature for both:

- the matter(s) we are inquiring about; and
- the person of whom we are inquiring.

> For example, we wouldn't ask a first-year associate to inquire of the audit committee chair or owner-manager. Similarly, if there is a going concern risk, then a more senior team member — e.g. the engagement partner — is likely the best person to inquire.

To the extent possible, we make inquiries in person - observing nonverbal communication can help us evaluate the inquiree's response.

1.1.E Enhanced | Inquire of those charged with governance, management and others about RMMs [ISA | 557]

What do we do?

Inquire of those charged with governance, management, the internal audit function and others about risks of material misstatement

Why do we do this?

We inquire of individuals we deem likely to have information and perspectives relevant to our risk assessment. In making these inquiries, we seek to:

- better understand their personal views;
- identify and assess additional risks we may not have considered yet; and
- confirm our understanding of the risks we've already identified.

Execute the Audit

Enhanced | Who do we inquire of? [ISA | 557.1300]

We inquire of individuals whom we reasonably expect to have information that could lead us to identify and assess a risk of material misstatement (RMM). These include:

- those charged with governance;
- key members of management;
- members of internal audit (if an internal audit function exists); and
- individuals in other positions who could have insight and information about RMMs.

> Suppose we're seeking information on a home repair project.
>
> We would likely ask others with previous experience, or perhaps someone who works in home improvement. Asking a doctor, despite holding them in high esteem, is unlikely to help (unless they, too, have experience in home repairs).

Similarly, during risk assessment, if we're looking for information on the entity's plans for implementing accounting policies, asking the Vice President of Operations may not be as effective as inquiring of the Chief Accounting Officer.

This isn't to say that we limit our inquiries to only those individuals in the accounting department. Individuals throughout the entity may have different views and information that can help us identify and assess RMMs.

It doesn't hurt to inquire of someone who ultimately has no useful information, but it *can* hurt if we omit someone who could provide helpful information.

So as a general rule of thumb: when in doubt, inquire.

Enhanced | Who are 'those charged with governance' for a public entity versus a private entity? [ISA | 557.1400]

Many public entities have an audit committee or equivalent body, established by and among the board of directors. When we audit a public entity, 'those charged with governance' will often mean the audit committee or equivalent (or its chair).

A private entity may or may not have an audit committee, board of directors or equivalent body. In that case, we inquire of the person(s) who oversee the entity's accounting and financial reporting processes and audits of the entity's financial statements. Those charged with governance could include management personnel — e.g. executive members of a governance board — or an owner-manager.

When do we make our inquiries? [ISA | 557.1500]

We make our inquiries:

- early enough in the audit to help us identify and assess RMMs; and
- as necessary throughout the audit.

Our aim is to gather information for our risk assessment — so making our inquiries too late in the audit will be ineffective, and the information may not help us plan the audit.

However, risk assessment is an iterative process — so making these inquiries is not a 'check the box' exercise that we complete and then file away.

We may find it appropriate to make additional inquiries, or to probe into a matter we inquired about previously. For example, if we become aware of a new material claim against the entity, we'll likely inquire about it again — even though we've already discussed litigations, claims and assessments.

Further, we try to make all our inquiries of a specific individual at once. So we think about other inquiries that other standards ask us to make, or which are relevant to include — e.g. fraud, related party transactions, significant transactions etc.

For example, when meeting with the CEO, we may take the opportunity to inquire about several matters at once — rather than hold a series of meetings. However, it may be necessary to inquire again when we obtain new or conflicting information.

Who makes the inquiries? [ISA | 557.1600]

Inquiries are made by an engagement team member with the appropriate level of knowledge, experience and stature for both:

- the matter(s) we are inquiring about; and
- the person of whom we are inquiring.

> For example, we wouldn't ask a first-year associate to inquire of the audit committee chair or owner-manager. Similarly, if there is a going concern risk, then a more senior team member — e.g. the engagement partner — is likely the best person to inquire.

To the extent possible, we make inquiries in person - observing nonverbal communication can help us evaluate the inquiree's response.

1.2 Perform analytical procedures [ISA | 547]

What do we do?

Perform analytical procedures

Why do we do this?

Analytical procedures allow us to examine relationships that exist among both financial and non-financial data.

We perform these procedures during risk assessment to help us understand the entity's business and significant transactions that have occurred.

They also help us identify areas that might represent risks of material misstatement (RMMs) relevant to the audit.

Execute the Audit

What do we consider when we perform analytical procedures? [ISA | 547.11465]

We consider the below. Details of each is outlined in the respective activities:

- Perform analytical procedures, including those related to revenue;
- Use the PA capability when electronic data is available;
- Evaluate the Account Analysis results when AA capability is used;
- Consider the analytical procedures applied during interim review engagements;
- Use our understanding of the entity to develop expectations about plausible relationships; and
- Consider unusual or unexpected results in identifying and assessing RMMs.

1.2.1 Perform analytical procedures, including those related to revenue [ISA | 548]

What do we do?

Perform analytical procedures, including analytical procedures related to revenue

Why do we do this?

Performing analytical procedures allows us to analyze unusual or unexpected trends, relationships and changes that:

- have happened since the prior period end; and
- may give rise to potential risks of material misstatement (RMMs) whether due to fraud or error.

Performing analytical procedures as part of our risk assessment may also identify aspects of the entity we were unaware of. This analysis draws on our existing knowledge about the entity and its environment, and helps us:

- better understand the entity; and
- identify areas that might represent specific RMMs relevant to the audit, such as:
  - the existence of unusual transactions and events; and
  - amounts, ratios and trends that warrant investigation.

We refer to the analytical procedures we perform during risk assessment as 'planning analytical procedures'.

To help identify fraud risks, we also include specific analytical procedures over revenue. We therefore analyze unusual or unexpected relationships between revenue and other accounts.

Execute the Audit

How do we perform planning analytical procedures? [ISA | 548.1300]

Performing analytical procedures during risk assessment involves the following.

- Enhancing our understanding of the client's business and the significant transactions and events that have occurred since the prior year end.
- Identifying areas that might represent specific risks relevant to the audit, including the existence of unusual transactions and events, and amounts, ratios, and trends that warrant investigation.
- Using our understanding of the entity to develop expectations about relationships that we expect to exist among certain financial and non-financial data.

  For example, there may be a relationship between headcount and payroll expense, so if we learn that the workforce decreased, we may expect payroll expense to decrease.

- Comparing our expectations with the actual amounts recorded in the financial statements (and with non-financial data, if relevant).
- Identifying areas in which the amounts are different from our expectations, and inquiring of management to understand the reason for the difference.

Our goal is not to simply compare the amounts and identify changes — i.e. perform a 'flux' analysis. Relationships among data can be understood and analyzed in many ways, including:

- comparing the movement of specific financial statement accounts with our expectations;
- drawing on our overall understanding of the entity and its industry; and
- drawing on past experience.

These relationships can be based on simple comparisons of recorded amounts, but may also be expressed as financial ratios that we can compare.

In addition, when we analyze income statement amounts, it may be helpful to estimate the full-period results by:

- annualizing the period-to-date results, adjusting for seasonality if needed; or
- using a combination of actual and forecasted results.

Do we perform planning analytical procedures with a specific level of precision? [ISA | 548.11490]

We do not compare our expectation of plausible relationships among recorded amounts with a specific level of precision, and we do not set an acceptable difference. In this respect, planning analytical procedures differ from those we perform to obtain substantive audit evidence (also known as 'substantive analytical procedures' or 'SAPs').

When performing planning analytical procedures, our analysis may be as simple as forming a general expectation about the direction and/or basic level of an expected change - e.g. expecting that when sales increase, accounts receivable should increase.

> For example, we may develop a broader expectation of how much revenue might change in the current period — e.g. 2-4% increase from the prior period — based on industry statistics or information available about an entity's competitors.
>
> Or we may expect the current-period days' sales outstanding (DSO) to remain consistent with historical DSO — and any deviations from that expectation may lead us to inquire further of management to understand the change. Ultimately, we may identify or assess an RMM differently if it is not consistent with historical DSO.

What are some of the common planning analytical procedures that we may perform? [ISA | 548.1400]

In performing planning analytical procedures, comparisons may help us identify results that do not align with our expectations. Common comparisons include:

- the balance sheet at the most recent, available period end with that of the prior period end;
- the income statement, cash flow statement and statement of comprehensive income for the most recent, available period (including period-to-date results), with those of the prior corresponding period;
- key financial ratios for the most recent, available period with those of the prior period; and/or
- budgeted information for the most recent, available period with actual amounts.

As part of our planning analytical procedures, we may use

- the Planning Analytics capability to automate certain types of comparisons and other types of analysis to help us perform planning analytical procedures; and
- the Account Analysis capability to help us identify the existence of unusual or unexpected relationships between accounts that might indicate the existence of potential risks of material misstatement.

Why do we perform analytical procedures specific to revenue? [ISA | 548.1500]

Revenue recognition is a presumed fraud risk, so we perform revenue-specific analytical procedures to identify unusual or unexpected relationships involving revenue accounts that are relevant to our audit and our risk assessment.

Financial statement users often consider revenues in total, but revenue is also a component of many key financial ratios, such as gross margin and profit margin. And revenue is often disaggregated and tracked by operating segment, such as line of business or even product line. Given its importance, revenue is also an account that may be more susceptible to fraud.

What are some of the common revenue-specific analytical procedures that we may perform? [ISA | 548.1600]

Our revenue-specific analytical procedures may include:

- specific analysis of revenue by product line, division or location;
- analysis of key ratios, such as DSO, gross margin or inventory turnover; and
- examining and analyzing revenue trends over several historical periods - e.g. monthly or quarterly.

In addition, revenue-related metrics reported by the entity, including non-GAAP metrics, may be useful in our risk assessment.

We may also use Account Analysis as part of our planning analytical procedures related to revenue.

How can we use D&A routines to enhance our analytical procedures? [ISA | 548.8076]

We may use data and analytics (D&A) routines to support our understanding of the entity and our identification and assessment of RMMs.

When relevant data is available in electronic format, we may use the Planning Analytics capability. Additionally, when relevant data is available in electronic format and certain conditions are met, we may also use the Account Analysis capability as part of our planning analytical procedures.

Before using a D&A routine in the audit we ask ourselves some basic questions:

- what is the purpose for using it?
- what is the nature of the data it uses?
- what is the nature of the audit evidence it is expected to provide?

Answering these questions helps us to understand how a D&A routine fits into our audit approach (see question 'How may we use D&A routines to obtain audit evidence or supplement our judgment?'). If we are unsure how to answer these questions, we risk using a routine which is not fit for the purpose, failing to appropriately consider the reliability of the data used, or placing inappropriate reliance on the results.

What is the Account Analysis capability? [ISA | 548.1610]

Account Analysis capability (AA capability) is a risk assessment tool that performs an automated analysis of an entity's journal entries, comparing them with pre-determined expectations and determining whether those entries reflect "expected", "unexpected" or other types of account combinations.

The AA capability offers several visualizations of the analysis performed, including the "Visual Ledger" that provides a graphical representation of the journal entries flow for selected accounts and processes.

AA capability results assist us in obtaining an understanding of the entity's accounting processes and recording of transactions, while identifying and assessing potential risks of material misstatement and enabling the determination of an audit approach specifically responsive to such risks.

What is an account combination? [ISA | 548.11491]

The AA capability analysis is based on the consideration of simple "one debit/one credit" account pairings - e.g. debit to Trade Receivables / credit to Revenue.

Some journal entries are already in the "one debit/one credit" format and can be directly evaluated by the capability. For journal entries with multiple line items, the AA capability uses a pre-defined set of rules to break down such entries into a number of 'one debit/one credit' account pairings, where possible.

For example, the entity may record the following journal entry:

Debit (Dr) Trade receivables	120	
Credit (Cr) Revenue		100
Credit (Cr) Sales tax, payable or receivable		20

When this journal entry is processed by the AA capability, it is broken down into the following 'one debit/one credit' pairings:

Pairing 1		
Debit (Dr) Trade receivables	100	
Credit (Cr) Revenue		100
Pairing 2		
Debit (Dr) Trade receivables	20	
Credit (Cr) Sales tax, payable or receivable		20

We refer to these 'one debit/one credit' account pairings as 'account combinations'.

What are primary/secondary accounts and primary/secondary account combinations? [ISA | 548.11492]

The AA capability allows us to select the specific accounts that we want to analyze. When we do so, only journal entries that contain the selected accounts are analyzed. However, since journal entries may contain multiple line items, once these entries are processed, we may obtain results for account combinations that do not include the accounts we specifically selected.

For example, we use the AA capability only on Revenue and all journal entries including Revenue are processed. These include the following journal entry:

Debit (Dr) Trade receivables	120	
Credit (Cr) Revenue		100
Credit (Cr) Sales tax, payable or receivable		20

When this journal entry is processed by the AA capability, it is broken down into the following 'one debit/one credit' pairings:

Account combination 1		
Debit (Dr) Trade receivables	100	
Credit (Cr) Revenue		100
Account combination 2		
Debit (Dr) Trade receivables	20	
Credit (Cr) Sales tax, payable or receivable		20

Even though account combination 2 does not include the Revenue account, it is also displayed as part of the Account Analysis results.

For the purpose of the AA capability:

- the accounts we select to analyze are primary accounts (e.g. Revenue in the example above) and any account combinations which involve those primary accounts are primary account combinations (e.g., account combination 1 in the example above).
- the other accounts displayed in the AA capability results are secondary accounts (e.g. Trade receivables and Sales tax, payable or receivable in the example above) and any account combinations which only involve secondary accounts are secondary account combinations (e.g. account combination 2 in the example above).

What are pre-determined expectations? [ISA | 548.11493]

For the purpose of the AA capability analysis, each possible account combination is assigned a "pre-determined expectation" with results of "expected" or "unexpected". These pre-determined expectations are based on general assumptions on how transactions are recorded, considering the specific industry and financial reporting framework.

For example, we expect a basic sales transaction to originate as a 'debit to Trade Receivables / credit to Revenue' account combination. Accordingly, this account combination is pre-determined as "expected" by the AA capability.

We can modify pre-determined expectations so that these represent a more accurate description of an entity's specific circumstances based on our understanding of the entity's process (see activity 'Confirm the pre-determined expectations').

When may we use the Account Analysis capability? [ISA | 548.1620]

We may use the Account Analysis capability (AA capability) as part of our planning analytical procedures when relevant data is available in electronic format and certain conditions for use of the capability are met.

Relevant data for the use of the AA capability include:

- General Ledger accounts,
- General ledger account balances (prior period ending account balances, current period opening balances, and current period ending balances), and,
- Journal Entries for the current period.

Determining whether "certain conditions for use of the AA capability are met" refers to:

- How an entity's accounting system records transactions in the General Ledger and whether the analysis performed by the AA capability will result in meaningful output,
- Whether pre-determined expectations related to the industry and financial reporting framework relevant to the entity are available in the AA capability, so that the analysis is performed using such expectations. When unavailable, we may still consider whether we can effectively modify existing pre-determined expectations to make them more accurate for the entity's specific circumstances, without requiring excessive customization.

Examples of where conditions for use of the AA capability may not be met:

- entities that use large batch journal entries to record a variety of transaction types in a single journal entry (e.g. transactions related to revenue, inventory purchases and other procurement and expenses activity may all be recorded daily in one single large batch entry)
- entities that make extensive use of 'suspense accounts' to record revenue and other relevant transactions temporarily before they are allocated to the primary general ledger accounts

We may determine the accounts to analyze through the AA capability by using our knowledge of the entity/industry and thinking about:

- the type of analysis performed by the AA capability and the nature of the entity's journal entries,
- the nature and characteristics of the account and the specific circumstances of the entity and its suitability to such type of analysis, and
- other planning analytical procedures that we may perform over the account.

Examples of scenarios that may support the use of the AA capability include:

- for accounts with a high volume of transactions where there is a history of misstatements arising from incorrect postings of journal entries, the AA capability could help us identify the existence of similar journal entries during the current period
- in situations where an entity has adopted a new accounting treatment/standard that impacts certain accounts, the AA capability may help confirm our understanding of how such transactions are recorded in the general ledger
- where a fraud risk may be present that would arise from specific entries through a specific account, the AA capability over that account may help us gather additional information related to that risk
- where an entity has experienced significant turnover in the accounting department, the AA capability being applied to the complete population of accounts may help us identify specific accounts that could be impacted as a result of this pervasive financial statement level risk.

If we use the AA capability over interim data, we apply professional judgment in determining an appropriate response to the identified risks, which may include using the AA capability at a later stage in the audit over period end data.

What is the Planning Analytics capability? [ISA | 548.12800]

The Planning Analytics capability (PA capability) is a risk assessment tool that automates certain analyses over an entity's data to help us perform planning analytical procedures.

The PA capability offers several analyses, such as:

- a comparison of prior year balances to current year balances, for both the statement of financial position and statement of profit or loss (e.g., balance sheet and income statement); this analysis is provided at the financial statement caption level, with drill down functionality to the general ledger level;
- a visualization of the monetary amount and number of journal entry postings to selected accounts by period, such as day, month or quarter – for example, the total amount of credit and debits entries posted to Revenue by month.

When may we use the Planning Analytics capability? [ISA | 548.12801]

When relevant data is available in electronic format, we may use the Planning Analytics capability (PA capability) as part of the planning analytical procedures performed to identify and assess RMMs. Relevant data for the use of the PA capability include:

- General Ledger accounts
- General Ledger account balances (current and prior period), and
- Journal Entries for the current period.

What is our responsibility regarding the relevance and reliability of data used in a D&A routine? [ISA | 548.1630]

Our responsibility over the relevance and reliability of the data used in a D&A routine is based on the same guidance that we follow when we use data in other audit procedures. We determine the nature and extent of effort to evaluate the relevance and reliability of the information used by thinking about how we intend to use the D&A routine in our audit. See question 'How is information used in a D&A

routine?' and activity 'Evaluate the relevance and reliability of information used in our audit' for further information.

Examples

How might the information from our planning analytical procedures affect the identification of RMMs? [ISA | 548.1700]

The table below sets out examples of information we may gather from our planning analytical procedures, and how that might help us identify and assess RMMs.

What our planning analytical procedures identified	How that might help us identify and assess RMMs
An increase in other accrued liabilities as compared to the prior period	The entity may have accrued for a probable loss. We may identify an RMM related to the accounting for new litigation or other loss contingency.
A decrease in revenue and gross margin for a particular product as compared to the prior period	The entity may have lost a significant customer. We may identify an RMM related to the accounting for related intangibles, such as trademarks or customer relationships.
An increase in transportation expense as compared to the prior period	The entity may have: • entered a new transportation agreement; • changed its methodology to accrue for transportation expense; or • failed to accrue for transportation expense in the prior period. We may identify an RMM related to the accounting for transportation costs.
An increase in IT expense as compared to the prior period	The entity may have expensed costs that are capital in nature. We may identify an RMM related to the accounting for software developed for internal use.

A significant increase in the relationship between sales and square footage of selling pace compared to the prior period	The entity may have recognized revenue in the wrong period. We may identify an RMM related to revenue recognition.
An unexpected account combination crediting revenue, as identified by the Account Analysis capability.	The entity may not have accurately recorded revenue. We may identify an RMM related to revenue recognition.

What D&A routines might we use to identify and assess RMMs for further analysis? [ISA | 548.8078]

Depending on the granularity of the analysis performed and the data used, D&A routines may provide us with detailed information that is relevant to support our risk assessment.

The table below sets out examples of analyses we may perform and the data we may use, and the RMMs we may identify.

Example of analysis performed and the data used	RMMs we may identify based on the analysis performed
The D&A routine is designed to provide detailed information about...	**We may identify an RMM related to:**
Cash by financial institution and country location	• The disclosure of concentrations of cash in a particular financial institution or country • The accounting and disclosure of the tax liability for the repatriation of cash from overseas
Long-term investments by investee and month incurred, as compared to the prior period	• The accounting and disclosure for a recent investment in a limited liability company • The accounting and disclosure for an equity method investee where the entity has acquired additional interest
Capital expenditures by project, type and month incurred	• The accounting for capitalized interest • The accounting for internal time

Revenue by product and month recognized, including amount accrued, as compared to the previous period	• The recoverability of certain intangibles — e.g. customer relationships and/ or trademarks — due to a significant decrease in revenue from an existing product line that may otherwise have been masked by a significant increase in revenue following the introduction of a new product line • The estimate to accrue for a new product line

1.2.2 Evaluate the Account Analysis results when AA capability is used [ISA | 4576]

What do we do?

IF Account Analysis is used THEN we evaluate its results according to the Account Analysis results evaluation approach

Why do we do this?

When we use the Account Analysis capability, we evaluate its results by using a specific Account Analysis results evaluation approach. The approach provides a phased analysis of the results to facilitate our identification and assessment of potential risks of material misstatement, and our determination of an audit approach that is specifically responsive to such risks.

Execute the Audit

What are the results from the Account Analysis capability? [ISA | 4576.1300]

After analyzing journal entries for the period, the Account Analysis capability (AA capability) uses the pre-determined expectations to determine whether those entries reflect "expected", "unexpected" or other account combinations.

Through this analysis, the AA capability facilitates our identification and assessment of potential risks of material misstatement and provides us with additional insight into the entity's business processes and how transactions are recorded by the entity. The following table identifies the different types of account combination classifications that may result from the AA capability, and the expected nature and extent of analysis over such results:

Account combination classification	Description	Expected nature and extent of analysis over Account Analysis results

'Expected' (color-coded in the tool as "green cells")	Account combinations that are expected to occur under the applicable financial reporting framework for the respective industry.	Prior to using the AA capability, we review the pre-determined expectations to confirm that the expected account combinations are appropriate for the entity. The expected account combinations may support our understanding of the entity's accounting processes in recording transactions through the general ledger. For further information about how we review the pre-determined expectations, see activity 'Confirm the pre-determined expectations'.
'Unexpected' (color-coded in the tool as "red cells")	Account combinations that are not expected to occur under the applicable financial reporting framework for the respective industry could be due to: • Entity's accounting treatments that differ from those considered in the pre-determined expectations, • Previously unknown process activities at the entity, or • Misstatements.	The analysis, understanding and audit response to an 'unexpected' account combination vary depending on the underlying cause. For further information about how we address unexpected account combinations, see activities: • 'Confirm the pre-determined expectations'; • 'Determine consequential unexpected account combinations'; and • 'Analyze consequential unexpected account combinations'.
'Unique' (color-coded in the tool as "grey cells")	Account combinations involving accounts for which no pre-determined expectations have been defined, such as: • accounts with increased complexity (e.g. Derivatives) and/or	We use our understanding of the entity, including our assessment of fraud risk factors, and apply professional judgment in determining whether to perform any specific analysis of 'unique' account combinations.

	• accounts where the extent of possible account combination relationships is too broad to provide meaningful results (e.g. Intercompany receivables and payables)	
'Same account' (color-coded in the tool as "black cells")	Account combinations resulting from debits and credits to the same account.	We use our understanding of the entity, including our assessment of fraud risk factors, and apply professional judgment in determining whether to perform any further analysis of 'same account' account combinations.
'Unbifurcated' (color-coded in the tool as "purple cells")	Journal entries or components of journal entries that could not be further disaggregated into account combinations are identified as 'unbifurcated'. For every account, all debits and all credits to the account resulting from unbifurcated journal entries are summarized and displayed separately in a credit and a debit cell and labeled as 'unbifurcated'.	Unbifurcated entries are not associated with any pre-determined expectations regarding the level of risk in the underlying entries. We apply our understanding of the entity and our professional judgment in determining whether to perform any specific analysis of unbifurcated journal entries.

How do we address the Account Analysis capability results? [ISA | 4576.1400]

We address the results of the Account Analysis capability (AA capability) by following the Account Analysis results evaluation approach. This is a phased approach that includes a logical sequence of activities to facilitate our:

- understanding the entity's accounting processes and recording of transactions,
- identifying and assessing potential risks of material misstatement, and
- determining an audit approach that is specifically responsive to such risks.

What are the phases in the Account Analysis results evaluation approach? [ISA | 4576.1500]

The Account Analysis results evaluation approach includes the following three sequential phases:

1.2.2.1 Confirm the pre-determined expectations [ISA | 4577]

What do we do?

Confirm the applicability of the pre-determined expectations used in the Account Analysis capability to the entity's specific circumstances in Phase I of the Account Analysis results evaluation approach

Why do we do this?

The Account Analysis capability determines whether the processed journal entries reflect "expected", "unexpected" or other account combinations. This determination is based on pre-determined expectations about how transactions are recorded, generally relevant to the entity's industry and financial reporting framework. Phase I of the Account Analysis results evaluation approach allows us to confirm that the pre-determined expectations are applicable to the specific entity's circumstances, and to modify the related account combinations classifications — i.e. expected or unexpected as appropriate.

Execute the Audit

How do we confirm the pre-determined expectations? [ISA | 4577.1300]

To confirm the pre-determined expectations, we:

- Understand what the pre-determined expectations are.
- Based on our understanding of the entity's processes, identify differences between how the entity accounts for transactions and the pre-determined expectations.
- Determine how those differences affect the related pre-determined account combinations classifications — i.e. "expected" or "unexpected" and modify such classifications as appropriate.

When is it appropriate to modify the pre-determined classifications?

The purpose of a classification modification is for the AA capability results to represent a more accurate alignment to an entity's specific circumstances.

- We modify pre-determined classifications when we identify pre-determined expectations that do not apply to the entity's specific circumstances.

  For example, the pre-determined expectation for our entity's industry and financial reporting framework assumes that all recognized revenue generates trade receivables. However, under one of the entity's specific business operations, revenue is recognized only through cash sales.

In these circumstances, we modify 'debit to Cash and cash equivalents / credit to Revenue' to "expected".

- When modifying a pre-determined classification for an account combination, we also consider modifying any other 'related' account combination classifications as appropriate.

  Referring to the previous example, when we modify 'debit to Cash and cash equivalents / credit to Revenue' to "expected", at the same time we modify the 'related' account combination 'debit to Trade receivables / credit to Revenue' to "unexpected" for this particular business operation.

- When the entity's accounting treatment relative to certain transactions is not appropriate under the relevant accounting framework, we do not modify the pre-determined classification.

  For example, if the entity capitalizes advertising costs in inventory when this is not considered appropriate under the relevant financial reporting framework, the corresponding pre-determined "unexpected" account combination (debit to Inventory / credit to Advertising and marketing expenses) should NOT be modified to "expected".

What are some differences between the entity's business and accounting processes and the account analysis pre-determined expectations? [ISA | 4577.1400]

- Differences may exist regarding pre-determined expectations as to how transactions are recorded for the respective industry as compared to how these are actually recorded by the entity.

  For example, pre-determined expectations assume that inventories are recorded through the balance sheet and 'debit to Inventory / credit to Trade Payables' is the "expected" account combination to record purchases of inventory. However, the entity may record purchases of Inventory throughout the year by 'debiting Cost of Sales / crediting Trade Payables' and adjust the related inventory account against Cost of Sales based on periodic inventory counts.

- Differences may exist due to transactions that pre-determined expectations assume as atypical for the industry's business operations which are, in fact, typical for the particular entity.

  For example, pre-determined expectations for the entity's industry may assume that recognized revenue generates a trade receivable; accordingly, the account combination 'debit to Cash and cash equivalents / credit to Revenue' is pre-determined as "unexpected". However, the entity may instead have cash sales and the referred account combination is in fact "expected" for the entity.

- Pre-determined expectations focus mainly on transactions resulting from 'routine' processes — e.g. sales, purchases, payroll, etc.; as a result, transactions from 'non-routine' processes are "unexpected" by default.

  For example, transactions regarding convertible bonds are not specifically considered in pre-determined expectations. As a result, the account combination 'debit to Loans and borrowing / credit to Share capital' is "unexpected". Where the entity transacts with convertible bonds on a recurring basis, the referred account combination is in fact "expected".

1.2.2.2 Determine consequential unexpected account combinations [ISA | 4578]

What do we do?

Determine consequential unexpected account combinations for further analysis in Phase II of the Account Analysis results evaluation approach.

Why do we do this?

When using the Account Analysis capability and evaluating its results, we focus our analysis on unexpected account combinations that may result in risks of material misstatement. Accordingly, we determine which of those unexpected account combinations are consequential for the purpose of our audit.

Execute the Audit

How do we determine which unexpected account combinations are consequential? [ISA | 4578.1300]

When determining whether unexpected account combinations are consequential individually or in the aggregate, we consider both relevant quantitative and qualitative factors, including:

- unexpected account combinations with amounts above AMPT are ordinarily considered consequential
- unexpected account combinations whose characteristics may be considered as indicative of a fraud risk (see chapter on fraud (ISA 240, AU-C 240, AS 2401), bias and/or ineffective controls, maybe determined to be consequential, even when their monetary amount is quantitatively inconsequential.

> For example, there is an unexpected account combination that shows a total amount below AMPT, which we may initially consider to be inconsequential. However, let's assume we have identified a fraud risk related to revenue recognition and that the unexpected account combination includes a credit to Revenue. In this instance, we may instead consider this unexpected account combination as consequential, given its connection to a fraud risk, and subject it to further analysis.

When there is uncertainty about whether an unexpected account combination is inconsequential or not, the account combination is considered consequential.

For unexpected account combinations that are inconsequential, we do not perform further analysis for the purpose of the Account Analysis capability.

How do we determine whether an unexpected "secondary account combination" is quantitatively consequential?

Secondary account combinations do not represent a population resulting from a complete processing of all journal entries for the analyzed period, accordingly, the quantitative assessment is not possible solely from the results of this analysis. The evaluation of unexpected secondary account combinations may involve the use of additional information to assist in the quantification assessment — e.g. we may use the Journal Entry Analysis capability to assess the existence of additional entries involving the same accounts as those involved in the secondary account combinations.

Absent additional information to allow for the quantification assessment of unexpected secondary account combinations, these are treated as consequential and subject to further analysis.

1.2.2.3 Analyze consequential unexpected account combinations [ISA | 4579]

What do we do?

Analyze consequential unexpected account combinations in Phase III of the Account Analysis results evaluation approach.

Why do we do this?

When using the Account Analysis capability and evaluating its results, we obtain an understanding of the nature and cause of these account combinations after we determine which unexpected account combinations are consequential. This understanding facilitates our identification and assessment of potential risks of material misstatement and our determination of an audit approach that is specifically responsive to those risks.

Execute the Audit

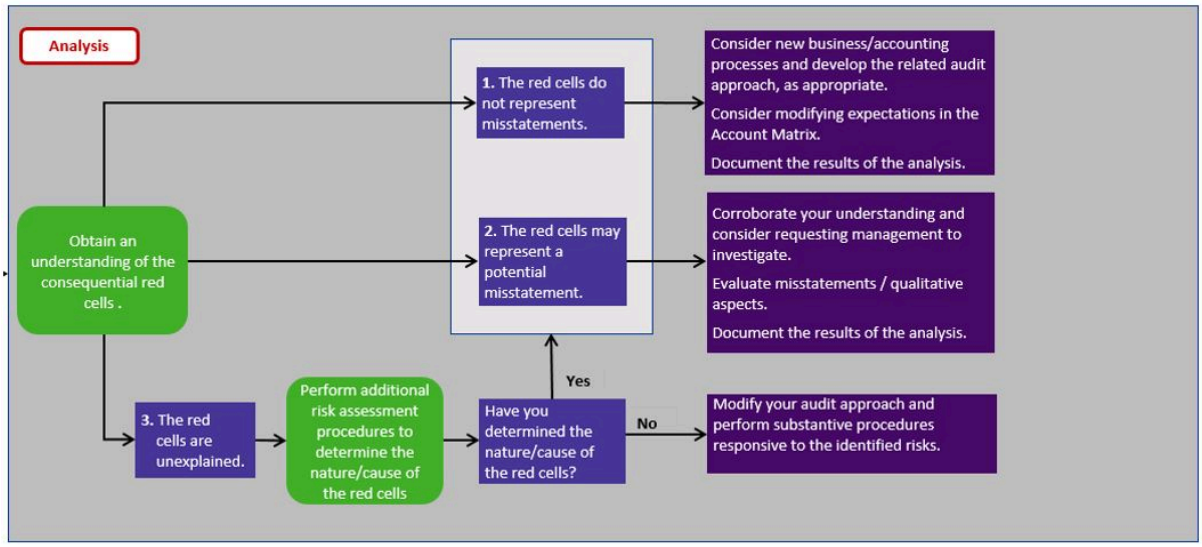
How do we obtain an understanding of the nature and cause of consequential unexpected account combinations? [ISA | 4579.1300]

In obtaining our understanding of an unexpected account combination, we consider relevant aspects of the original journal entries resulting in such account combinations and use a combination of risk assessment procedures that include inquiry, observation and inspection, as appropriate. Inquiry alone may not be sufficient to achieve our understanding.

Based on the evidence obtained from this analysis and our knowledge of the entity, we determine whether an unexpected account combination:

- does not represent a misstatement,
- may represent a potential misstatement, or
- remains unexplained.

The flowchart below illustrates the activities we perform and our responses when analyzing consequential unexpected account combinations:



What do we do when an unexpected account combination does not represent a misstatement?

When an unexpected account does not represent a misstatement, it may be due to either:

Potential cause	How we respond
A business/accounting process previously unknown	• Update our understanding of the process activities and consider whether there are new RMMs to identify and assess as part of our audit plan. • Modify related pre-determined expectations to adapt those to the specific entity's business/accounting process that were previously unknown (see activity 'Confirm the pre-determined expectations').
Other causes, for example: • An inappropriate mapping of the entity's general ledger accounts to the accounts used by the Account Analysis capability (AA capability) • A non-recurring transaction we do not normally expect in the entity/industry, but may be determined appropriate in the circumstances	• Modify mapping accordingly and reprocess Account Analysis when the cause is inappropriate mapping • Consider whether it is appropriate to modify expectations • Think about qualitative aspects, if any • Consider whether it is appropriate to modify expectations • Think about qualitative aspects, if any

What do we do when an unexpected account combination is likely to represent a misstatement?

When an unexpected account combination is likely to represent a misstatement, we:

- Identify relevant RMMs, as appropriate
- Consider corroborating our understanding by performing additional inspection of supporting evidence over the journal entries leading to the unexpected account combination
- Consider requesting that management investigate and make necessary adjustments
- Evaluate the misstatement(s)
- Consider including the originating journal entries in the relevant population of 'high-risk' journal entries and test them accordingly when the characteristics of the unexpected account combination are associated to high-risk criteria. See activity 'Identify and select journal entries and other adjustments for testing'.

What do we do when an unexpected account combination remains unexplained?

There may be instances where our initial analysis may not be conclusive and the unexpected account combination remains unexplained. In these circumstances, we perform additional risk assessment procedures to determine the nature and cause of the unexpected account combination.

After performing the additional risk assessment procedures, we may be able to determine the nature and cause of the unexpected account combination. This will allow us to determine whether an unexpected account combination may represent a potential misstatement or not, and follow the additional steps, as applicable.

If after performing the additional risk assessment procedures, we are not able to determine the nature and cause of the unexpected account combination, we identify relevant RMMs, as appropriate, and respond to the identified risks by modifying the audit approach and planning substantive procedures over the transactions leading to the unexpected account combination.

When do we perform substantive procedures responding to unexpected account combinations?

We may perform substantive procedures responding to unexpected account combinations:

- at the time the AA capability is used and the combination is identified, or
- later in the audit when we perform other planned procedures over the related RMMs.

For example:

- The Account Analysis results include the following unexplained unexpected account combination: 'Debit to PPE - Credit to Advertising and marketing expenses'.
- As part of the audit procedures responding to RMMs related to Existence and Accuracy of PPE, we planned to perform a substantive test of PPE additions and we now decide to specifically include the transactions captured in the unexpected account combination in the items to be tested.
- After performing the planned procedure, we determine whether the items and amounts in the unexpected account combination have been appropriately addressed.

What substantive procedures may we perform to test the journal entries that led to the unexpected account combinations?

Substantive procedures performed to test the journal entries that led to the unexpected account combinations may include:

- Obtaining appropriate supporting evidence as to the validity of the transactions.
- Comparing to the prior period and assessing whether it remains appropriate, when the item is a recurring journal entry.
- Assessing whether the journal entry:
  - Reflects the underlying events and transactions
  - Has been recorded in the correct accounting period at appropriate amounts
  - Has been recorded to the correct general ledger accounts (or has been included in the appropriate financial statement captions)
  - Is consistent with the entity's accounting policies.
- Identifying and addressing any qualitative considerations, if applicable (e.g., indication of potential control failure, potential fraud risk). If the characteristics of the unexpected account combinations are associated to high-risk criteria, we include the related journal entries in the relevant population of 'high-risk' journal entries and test them accordingly. See activity 'Identify and select journal entries and other adjustments for testing'.
- Consider requesting management to specifically investigate the journal entries resulting in the unexpected account combinations.

What do we think about when analyzing an unexpected "secondary account combination"?

"Secondary account combinations" do not represent a population resulting from a complete processing of all journal entries for the analyzed period. As part of the analysis over an unexpected secondary account combination, we evaluate the risk of other journal entries resulting in the same account combination and respond accordingly. This may be achieved by performing additional analysis, including:

- using the Journal Entry Analysis capability to identify and analyze additional journal entries involving the same accounts in the secondary account combination (see activity 'Use the JEA capability when electronic data is available');
- performing other risk assessment procedures, as appropriate to the specific entity and engagement circumstances — e.g. other types of planning analytical procedures; or
- where we believe Account Analysis is able to provide relevant and/or meaningful information on the specific accounts involved in the unexplained secondary account combination, selecting those accounts to be analyzed through the AA capability.

What may we consider when analyzing the nature and cause of the unexpected account combinations?

[ISA | 4579.1400]

Relevant aspect to consider	Examples and other considerations
Nature of the account involved in an unexpected account combination	For example, unexpected account combinations involving: • accounts with a history of misstatements in the prior year(s)

	• accounts related to potential fraud risks — e.g. Revenue, Cash.
Risk of potential misstatement resulting from an unexpected account combination	For example, consider if the unexpected account combination may: • potentially overstate Income — i.e. unexpected credits to Income accounts • potentially overstate Assets — i.e. unexpected debits to Asset accounts • potentially understate Expenses — i.e. unexpected credits to Expense accounts • potentially understate Liabilities — i.e. unexpected debits to Liability accounts.
Characteristics of journal entries resulting in an unexpected account combination	• For example, and depending on the data imported from the entity's system: - Posting period — e.g. unexpected account combinations resulting from journal entries posted at period end - Entry type — i.e. automated/manual - JE line items — e.g. unexpected account combinations resulting from journal entries with > XX line items - Underlying entity's general ledger accounts - User name — e.g. unexpected account combinations resulting from journal entries recorded by a specific user. • The characteristics of the original journal entries resulting in unexpected account combinations is also relevant in determining the appropriate extent of the investigation: - Where the original journal entries show identifiable common patterns — e.g. resulting from an automated batch entry processed at each month-end for the same amount, it may be sufficient to test one or a limited number of such journal entries in order to obtain understanding over all of them. - Otherwise, where the original journal entries have different characteristics — e.g. manual and automated entries recorded on non-recurring dates and for different amounts we may consider testing individually, each different type of journal entry. • Where patterns identified for the original entries resulting in unexpected account combinations include indicators of potential management bias or fraud, the extent of our investigation is increased and we include the related journal

	entries in the relevant population of 'high-risk' journal entries and test them as appropriate.

1.2.3 Consider the analytical procedures applied during interim review engagements [ISA | 549]

What do we do?

IF we performed an interim review, THEN take into account the analytical procedures applied in that review when designing and applying analytical procedures as risk assessment procedures

Why do we do this?

We perform many of the more common planning analytical procedures as part of our interim reviews.

These analytics can help us identify items that appear to be unusual and that indicate a potential RMM. We use our interim findings when we plan our risk assessment procedures, and supplement them with additional procedures as necessary.

Execute the Audit

How do our interim review analytical procedures differ from those performed for risk assessment? [ISA | 549.1300]

Our interim review analytical procedures and our planning analytical procedures are quite similar. They both involve comparisons of recorded amounts - or ratios developed from recorded amounts - to expectations that we develop.

However, the objectives of our analyses during an interim review (identifying items that may reflect material misstatements) may be different from those of our planning analytical procedures (identifying areas that might represent specific RMMs relevant to the audit).

Can we simply use our interim review analytical procedures for risk assessment? [ISA | 549.1400]

The analytical procedures from our interim review may be sufficient for risk assessment, depending on the timing of those procedures and the specific analyses we perform.

Because of the differences in objectives of our analyses, if interim review analytical procedures are not performed with risk assessment in mind, we may need to perform additional planning analytical procedures to meet the objective for risk assessment.

In addition, our interim review analytical procedures may be performed too late in the year to be helpful during risk assessment, e.g. interim review on half-year numbers when risk assessment was done earlier in the year.

What if we learn new information during a subsequent interim review? [ISA | 549.1500]

Similar to other information, we consider what we learn and whether it contradicts or corroborates our original risk assessment.

This includes information we learn during interim reviews we perform after our risk assessment procedures.

Example

How might the results of analytical procedures performed during our interim reviews impact our risk assessment? [ISA | 549.1600]

The table below sets out examples of information we may gather from our interim reviews, and how that might help us identify and assess RMMs.

What our review of analytical procedures identified	How that might help us identify and assess RMMs
An increase in debt or equity balances	The entity may have issued new debt during the period, or entered into an equity transaction. We may identify an RMM related to the accounting for new debt or equity instruments.
Significant swings in revenue between quarters	We may identify that revenue is recognized based on subjective criteria, and increases in periods in which a bonus is calculated. We may identify an RMM that revenue is not being recognized appropriately, or a fraud risk related to revenue recognition.
An increase in professional fees in a quarter	The entity may not have accrued costs for the outcome of litigation, or it might be connected to a tax investigation. We may identify an RMM related to the valuation of uncertain tax position liabilities.

1.2.4 Use our understanding of the entity to develop expectations about plausible relationships

[ISA | 550]

What do we do?

Use our understanding of the entity to develop expectations about plausible relationships among the data to be used in the analytical procedure

Why do we do this?

Relationships can exist between financial data and other financial data, and between financial and non-financial data.

Where plausible relationships exist, we expect them to continue to exist, unless something disturbs the relationship. This allows us to develop an expectation.

If, when we compare our expectations to recorded amounts, we get unusual or unexpected results, this can yield information that's relevant when we identify and assess the risks of material misstatement (RMMs).

Execute the Audit

What data might we use in our analytical procedures? [ISA | 550.1300]

We may use both financial and non-financial data when we perform analytical procedures. For example, we may use financial data from the entity's financial statements, and we may also use non-financial data such as the locations in which it operates, number of employees, etc.

How do we identify relevant data to consider in our analytical procedures? [ISA | 550.1400]

We consider our understanding of the entity and the results of our other risk assessment procedures to identify relevant data we can use in our analytical procedures.

We may have access to a significant amount of data, but not all of it will be relevant or have a plausible relationship that will help us perform our analytical procedures. So we focus on data where relationships are likely to exist. In many cases, the measures that have the biggest impact on the entity are the same measures analyzed by the entity and its stakeholders.

For example, by performing our risk assessment procedures we understand performance measures including those which are:

- followed by management, analysts and other third parties; and
- used in compensation arrangements and through covenants included in debt arrangements.

These performance measures are likely to point us to relevant data we can use in our analytical procedures.

> For example, after observing a retail entity's earnings calls and having read several analysts' reports, the engagement team learned that the entity's investors and analysts are focused on the same store sales.
>
> Consequently, the team identified sales and the number of stores as relevant data to be used in their analytical procedures.

What is a 'plausible relationship'? [ISA | 550.1500]

A plausible relationship is an expected relationship between financial data and other financial data, or financial data and non-financial data.

We base an expected relationship on our understanding of the entity, the industry or past experience. These relationships can be expressed in various ways, including for example:

- simple comparisons of recorded amounts;
- financial ratios that we can compare; or

- predetermined expectations around account combinations used in the Account Analysis capability.

For example, we normally expect a relationship between sales and accounts receivable, whereby accounts receivable increase as sales increase. Similarly, we expect a revenue transaction to generate a debit to accounts receivable and a credit to revenue. And in a brick and mortar retail environment, we may expect a relationship between sales and retail square feet.

Where these plausible relationships exist, we expect them to continue to exist, unless something happens to disturb the relationship. This means that if the types of sales-generating activities remain the same, we might expect accounts receivable to increase as sales increase. Conversely, we might expect accounts receivable to decrease as sales decrease.

How do we develop our expectations of plausible relationships? [ISA | 550.1600]

We develop our expectations of plausible relationships by using our understanding of the entity, including any information we may have learned from our other risk assessment procedures — e.g. changes that have happened in the business.

> For example, we may compare sales from the current and prior periods, and develop a general expectation for the accounts receivable balance.
>
> If, however, our risk assessment procedures revealed that the entity was making significantly more cash sales than in the past, we would likely adjust our expectation of the relationship between sales and accounts receivable accordingly.

What do we do with our expectations of plausible relationships? [ISA | 550.1700]

We compare our expectations of plausible relationships with relationships derived from the entity's recorded amounts.

We consider whether our expectations align with the relationships from the entity's recorded amounts, or if they produce unusual or unexpected results.

Plausible relationships are expected to exist and continue unless something disturbs the relationship. Therefore, a relationship based on recorded amounts that does not match our expectation might suggest an RMM or unusual event that may warrant investigation.

> Consider an entity that has historically generated most of its sales through wholesale distribution channels. If that entity begins to sell its products through retail stores, it may generate significantly more cash sales than in the past.
>
> This change may disturb the relationship between sales and accounts receivable, because the entity will now have more sales without corresponding accounts receivables (since the sale was made for cash).

How do we determine the relevance and reliability of the data we use? [ISA | 550.1800]

How do we determine relevance? [ISA | 550.11503]

We determine the relevance of the data we use to develop plausible relationships based on our understanding of the entity and the financial statement data that is key to the entity's operations.

'Relevance' connects back to the nature of our analytical procedures, and whether the data helps us understand a plausible relationship that exists. We do not use data unless it's relevant to our procedure.

How do we determine reliability? [ISA | 550.11504]

We determine the reliability of the data through inquiry with management, or through other procedures to consider the source of the information.

Inquiry of management may sometimes be sufficient - e.g. it may help us confirm that the data we are using came directly from the entity's general ledger system, which has general IT controls in place.

For other data, we may perform additional procedures to determine its source and establish its reliability before we use it, such as observing management generating the data. For additional guidance, refer to the following guidance in the Audit Evidence chapter - 'Determine the appropriate audit procedures to address the reliability of the information'.

What level of evidence do we use to determine relevance and reliability in a risk assessment procedure? [ISA | 550.11505]

The evidence we use to determine the relevance and reliability of the data in a risk assessment procedure may be less than what we use when testing a control or performing a substantive procedure (including a substantive analytical procedure).

Example

What plausible relationships might exist between data? [ISA | 550.2000]

The table below sets out examples of plausible relationships that may be relevant to our analytical procedures.

Example of plausible relationship	Type of relationship
Sales and accounts receivable: • as sales increase, we expect accounts receivable to increase • as sales decrease, we expect accounts receivable to decrease	General relationship between accounts
Accounts receivable turnover: • sales ÷ accounts receivable	Financial ratio
Personnel cost per employee — average payroll-related costs per employee: • personnel cost ÷ number of employees	Ratio based on financial and non-financial data

Days' sales outstanding: • (accounts receivable ÷ sales) x days in period	Financial ratio
Sales and cost of sales: • as sales increase, we expect the cost of sales to increase	General relationship between accounts
Gross profit margin - i.e. gross profit as a percentage of sales: • (sales - cost of sales) ÷ sales • we expect gross profit margin to remain constant, absent known changes — e.g. an increase in sales prices	Financial ratio
Selling price per unit - average selling price per sales unit: • sales ÷ number of items sold	Ratio based on financial and non-financial data
Inventory turnover: • sales ÷ inventory	Financial ratio
Days sales in inventory: • (inventory ÷ cost of sales) x days in period	Financial ratio

1.2.5 Consider unusual or unexpected results in identifying and assessing RMMs [ISA | 551]

What do we do?

IF comparison of our expectations with the recorded amounts yields unusual or unexpected results, THEN take those results into account in identifying and assessing risks of material misstatement.

Why do we do this?

We compare our expectations of plausible relationships that exist between data with relationships derived from recorded amounts.

When the comparison yields unusual or unexpected results, this may indicate the existence of a potential RMM.

We therefore consider unusual or unexpected results, so that:

- we don't fail to identify and assess an RMM; and
- we develop an appropriate audit response.

Execute the Audit

How do we consider or take into account unusual or unexpected results in identifying and assessing RMMs? [ISA | 551.1300]

We consider unusual or unexpected results by:

- understanding the reasons for the results - e.g. inquiring of management or other relevant entity personnel; and/or
- obtaining additional evidence to explain the reasons for the results; and
- identifying possible RMMs, as necessary.

Unusual or unexpected results may mean that there is an RMM we have not previously identified.

For example, we may be prompted to investigate if we notice that:

- sales increased without a corresponding increase in accounts receivable; or
- there was an increase in accounts receivable that did not correspond with the increase in sales.

We may inspect additional documentation and inquire of management to help us:

- better understand why the results differ from our expectations; and
- identify and assess RMMs that are relevant to the audit.

This helps us to figure out the 'why?' — i.e. we seek the information that tells us *why* the recorded amounts did not meet our expectations.

When using the Account Analysis capability, we analyze unexpected account combinations according to the Account Analysis results evaluation approach (see activity 'Evaluate the Account Analysis results when the AA capability is used'.

Example

How might the results of our planning analytical procedures affect our identification and assessment of RMMs? [ISA | 551.1400]

The table below sets out examples of how the results from our planning analytical procedures might affect how we identify and assess RMMs.

Results of planning analytical procedures	How these might affect our identification and assessment of RMMs
Revenue has decreased and accounts receivable have increased when we	• This may indicate that the entity has trouble collecting certain debts, and we may identify an RMM related to the recording of the allowance for doubtful accounts.

would have expected them to also decrease	• This may also indicate that the entity has entered a new line of business, and may have changed the customer base or methods of distribution. These changes may affect the way the entity recognizes revenue, and we may identify an RMM related to the recording of revenue.
Gross margin percentage has increased from the prior period (revenue increased by 35%; cost of sales decreased by 10%)	• We may identify an RMM that revenue is being recognized in advance of meeting the requirements under the accounting standards. • Alternatively, this may indicate that there is an issue with how costs are recorded/accrued, and we may identify RMMs related to the recording of expenses and liabilities. • Or we may find out that this is simply because the entity raised its prices while costs remained the same — in which case we may not identify additional RMMs.
Gross margin has decreased from the prior period (revenue increased by 10%; cost of sales increased by 20%)	• This could result from many circumstances, such as introducing a new product line that is not profitable. In that case, the entity may feel pressure to meet certain sales targets, and may want to recognize revenue without meeting the criteria. • We may identify this as a fraud risk factor or an RMM that revenue is being recognized before the accounting standards' requirements are met.
Unfavorable change in the inventory turnover ratio from the prior period	• The entity may have released a new product, indicating that other inventory items are obsolete and need to be written off. Therefore, we may identify an RMM related to the valuation of inventory. • Alternatively, this may indicate that sales are slower than in the past, and that there is an excess of inventory that may need to be covered by a valuation reserve. Therefore, we may identify a separate RMM related to the valuation of inventory.
Payroll expense has increased from the prior period, and this increase is not commensurate with either sales or headcount	• This may indicate that the entity has awarded bonuses or has other payroll-related expenditures that we were previously unaware of. • We may identify RMMs based on the terms of the bonus, relating to: - the timing of recognition - the calculation of the amount

	- the fraud risk related to the targets on which the bonus is based, etc.

1.3 Group Audit | Perform analytical procedures at group level [ISA | 1499]

What do we do?

Perform analytical procedures at the group level.

Why do we do this?

Analytical procedures allow us to examine relationships that exist among both financial and non-financial data. We perform these procedures during risk assessment to help us understand the group's business and significant transactions that have occurred.

They help us identify and assess risks of material misstatement of the group financial statements (group RMMs). They also help us identify components at which there may be a reasonable possibility of a material misstatement to the group financial statements when abnormal fluctuations at those components are identified by our analytical procedures.

Execute the Audit

How do we perform analytical procedures for a group audit? [ISA | 1499.1300]

As the group auditor, when we perform analytical procedures for a group audit, our procedures are similar to the planning analytical procedures in a stand-alone audit. Performing analytical procedures for a group audit involves the following:

- using our understanding of the group and its environment, including its entities or business units, to develop expectations about relationships that we expect to exist among certain financial and non-financial data;
- comparing our expectations with the actual amounts recorded in the financial statements (and with non-financial data, if relevant);
- identifying areas in which the amounts are different from our expectations, and inquiring of group management to understand the reason for the difference; and
- performing our analytical procedures at a more disaggregated level and considering the financial information at entities and business units to identify components where specific risks may exist.

As the group auditor, we think about whether it is more effective to perform analytical procedures:

- *individually* for each entity or business unit; or
- grouping certain entities or business units together.

When aggregating information, remember that our intention is to provide us information about at which entities or business units group RMMs may exist. As a result, we are careful not to aggregate information in a way that could interfere with our ability to identify items that differ from our abnormal fluctuations at entities or business units.

In performing analytical procedures, we may compare different financial and non-financial information of components to identify amounts that do not align with our expectations, including:

- the balance sheet at the most recent, available period end with that of the prior period end;
- the income statement for the most recent, available period (including period-to-date results), with those of the prior corresponding period;
- key financial ratios for the most recent, available period with those of the prior period; and/or
- budgeted information for the most recent, available period with actual amounts.

Our goal is not to simply compare the amounts and identify changes — i.e. perform a 'flux' analysis. Relationships among data can be understood and analyzed in many ways, including:

- comparing the movement of specific financial statement accounts with our expectations;
- comparing ratios between components and over time;
- considering trends in relation to our understanding of the economy and the industry, and trends between components;
- drawing on our overall understanding of the group, its components and their industries; and
- drawing on past experience.

1.4 Consider other information relevant to identifying and assessing RMMs [ISA | 540]

What do we do?

Consider whether information from the client and engagement acceptance and continuance process, audit planning, past audits and other engagements is relevant to identifying and assessing risks of material misstatement

Why do we do this?

Information that can help us during risk assessment can come from a variety of sources other than the entity, its environment and its internal controls. For example, we may learn useful information through:

- our client acceptance and continuance (retention) process;
- audit planning; and
- our experience with the entity on past audits or other engagements.

We use this additional information to help us identify and assess risks of material misstatement (RMMs).

Execute the Audit

How do we consider other information relevant to identifying and assessing RMMs? [ISA | 540.11439]

We follow the below steps. Details of each step is outlined in the respective activities:

- Consider information from the CEAC process and audit planning in identifying and assessing RMMs;
- Consider information from past audits in identifying and assessing RMMs;
- Evaluate the relevance and reliability of information from past audits; and
- Consider information from other engagements in identifying and assessing RMMs.

The types of risks of material misstatement considered are due to fraud and/or error.

1.4.1 Consider information from the CEAC process and audit planning in identifying and assessing RMMs [ISA | 541]

What do we do?

Consider whether information obtained from the client and engagement acceptance and continuance process and audit planning is relevant to identifying and assessing RMMs

Why do we do this?

The information we obtain about the entity during our client and engagement acceptance and continuance (CEAC) process may help us identify risks of material misstatement (RMMs).

We therefore evaluate the information, and whether it is relevant to identifying and assessing RMMs.

Execute the Audit

What is the CEAC process? [ISA | 541.1300]

CEAC is our process for evaluating and re-evaluating member firm clients and engagements. During the CEAC process, we answer questions and collect information that helps us assess and document the risks associated with accepting prospective audit clients or continuing with existing audit clients and engagements.

The questions we answer during the CEAC process span a variety of topics, including:

- current and prior-period financial information;
- possible accounting and auditing complexities;
- information about senior management and their attitudes toward internal controls; and
- other publicly available information.

See the Global CEAC Resource Center for more information on the CEAC process.

How do we consider information from the CEAC process? [ISA | 541.1400]

We consider information obtained from the CEAC process to identify matters that may indicate potential RMMs. These matters may include:

- whether the entity has faced adverse media coverage or public scrutiny;
- deficiencies in internal controls identified in prior periods;
- the use of non-routine or unusual accounting treatments;
- signs of going concern risk;
- significant related party transactions; and
- concerns over the quality of information.

We also consider other information we learn about the entity during the CEAC process that highlights other risks - e.g. broad information about its accounting practices or possible significant transactions being considered, such as investments in digital assets.

In addition, we consider whether communications with the predecessor auditor during the CEAC process are relevant to identifying and assessing RMMs.

How do we consider information from our planning procedures? [ISA | 541.1500]

During audit planning procedures, we obtain various information and insights about the entity that help us identify RMs and further assess which of those are RMMs.

Our planning process and the information we collect are broad, so an RMM may not be apparent when we consider information in isolation. However, when we reflect on everything we learned about the entity from our planning procedures and evaluate the information from a 'big picture' perspective, we may see connections that help us identify and assess RMMs.

Examples

What information from our CEAC process may help us identify and assess RMMs? [ISA | 541.1600]

The table below sets out examples of information obtained from the CEAC process that may help us identify and assess RMMs, when the financial reporting framework is US GAAP or IFRS.

Information obtained from the CEAC process	Identified RMMs US GAAP	Identified RMMs IFRS
The entity's credit rating was downgraded from investment grade status to non-investment grade status — e.g. from BBB/Baa2 to BB/Ba2	**Going concern risk** • Conditions and events that may raise substantial doubt about an entity's ability to continue as a going concern are not appropriately evaluated https://alex.kpmg.com/AROWeb//document/lfc/US_DPP_RIA_205_FS/toc/US_DPP_RIA_205_FS?tocref=.	**Going concern risk** • Management does not appropriately assess the entity's ability to continue as a going concern https://alex.kpmg.com/AROWeb/DocumentWindow.aspx?ref=GSC_INTL_AUDDOC_010115031&from=attach. • Management's conclusion on the entity's ability to continue as a going concern is inappropriate.
The entity's market capitalization decreased by 10%	**Valuation of goodwill and/or other long-lived assets** • Indefinite lived intangibles are not tested for impairment at least annually, or more	**Valuation of goodwill and/or other long-lived assets** • Intangible assets with an indefinite useful life or an intangible asset not yet available for use (or cash-generating units that include

	frequently if events or circumstances warrant. • Indicators that an asset or asset group may be impaired are not appropriately identified.	such assets) are not tested for impairment at least annually, or more frequently if indications of impairment exist. • Indicators that an asset or cash-generating unit may be impaired are not appropriately identified
The entity has complex revenue arrangements with multiple performance obligations	**Revenue recognition for complex revenue arrangements** • The term of the contract is not accurately determined.	**Revenue recognition for complex revenue arrangements** • Revenue is not appropriately recognised because performance obligations in a contract are not appropriately determined.
The entity has taken on new debt with restrictive covenant compliance thresholds	**Recognition of new debt obligations** • Debt obligations are not completely identified and accurately recorded. **Pressure to comply with restrictive debt covenants** • Debt covenant violations are not completely identified or appropriately evaluated for their impact on the appropriateness of the classification of the debt obligation as long-term versus short-term (due to callable right provisions in the agreement).	**Recognition of new debt obligations** • Financial liabilities are recorded inappropriately when: - they are not accurately recorded, - they do not meet the recognition requirements, or - they do not exist. **Pressure to comply with restrictive debt covenants** • Debt covenant violations are not completely identified or appropriately evaluated for their impact on the classification of the debt obligation as current versus non-current.

1.4.2 Consider information from other engagements in identifying and assessing RMMs

[ISA | 544]

What do we do?

Consider whether information from other engagements is relevant to identifying and assessing risks of material misstatement

Why do we do this?

We may perform other services for an entity, beyond the annual audit. In doing so, we obtain information about the entity that could be relevant to our risk assessment.

We consider whether this information might lead us to identify and assess risks of material misstatement (RMMs).

Execute the Audit

How do we consider information from other engagements in identifying and assessing RMMs? [ISA | 544.11459]

We follow the below steps. Details of each step is outlined in the respective activities:

- Evaluate information from interim review engagements in identifying and assessing RMMs; and
- Understand and consider the nature of other services we have performed in identifying and assessing RMMs.

1.4.2.1 Evaluate information from interim review engagements in identifying and assessing RMMs

[ISA | 545]

What do we do?

IF we performed an interim review, THEN evaluate whether information obtained during the review is relevant to identifying and assessing risks of material misstatement in the period-end audit.

Why do we do this?

Sometimes, we may perform a review of interim financial information ('interim review'). In doing so, we may obtain:

- information about the entity broadly;
- information about significant events that occurred during the period; and
- other information that could be relevant to our risk assessment for the period-end audit.

This information can inform us about potential risks of material misstatement (RMMs), so we evaluate it as part of our risk assessment.

Execute the Audit

How do we identify information from an interim review that is relevant to identifying and assessing RMMs? [ISA | 545.1300]

When we have performed an interim review, we inspect key documentation which helps us identify and assess RMMs.

Relevant information can come from any part of our review. We pay close attention to the significant findings or issues and conclusions reached during each interim review engagement. These areas can highlight new RMMs or influence the way we assess RMMs that we consider during risk assessment.

What information may we use from our interim review to identify and assess RMMs? [ISA | 545.1400]

Information that may help us identify and assess RMMs may include:

- significant changes in industry, regulatory and external, and entity-specific factors;
- initial selection of, or changes in, significant accounting policies or how they are applied;
- key findings and/or unusual relationships identified in our analytical procedures;
- uncorrected and corrected misstatements, including disclosures;
- significant changes in or deficiencies in internal control;
- acts or allegations of fraud;
- significant unusual transactions;
- related party transactions identified;
- consultation matters; and
- communications with management, those charged with governance and others.

Example

How do we consider information obtained from an interim review in identifying and assessing RMMs? [ISA | 545.1500]

Fact pattern:

During the engagement team's review of interim financial information for the second quarter, they find out about a significant lawsuit that may threaten the entity.

As part of their interim review procedures, they inquire of management about the lawsuit and any potential losses, and obtain corroboration from the entity's general counsel and external counsel.

Analysis:

As part of their risk assessment during the period-end audit, the team evaluate the relevance of this information. They identify an RMM related to how the entity records and discloses liabilities related to commitments and contingencies.

1.4.2.2 Understand and consider the nature of other services we have performed in identifying and assessing RMMs [ISA | 546]

What do we do?

Obtain an understanding of the nature of the services that we, or other KPMG member firms have performed for the entity; and take into account relevant information obtained in identifying and assessing risks of material misstatement.

Why do we do this?

Beyond the current audit, we may perform other services for an entity — including audit-related, tax and other types of engagements. During these other engagements, we may learned something about the entity or come across events that are relevant to our risk assessment.

We therefore seek to understand the nature of these services and consider whether the information we obtained during these engagements points us to risks of material misstatement (RMMs), including significant risks and financial statement level risks, and/or other matters to be addressed in the current audit.

Execute the Audit

How may we identify the engagements that we or other KPMG member firms perform? [ISA | 546.1300]

Depending on the circumstances of the entity, we may use different sources of information to help identify other services we or other KPMG member firms have performed or are performing for the entity, such as:

- Sentinel report(s) for the entity, if available
- Other member firm specific reports of KPMG engagements, if any
- Management knowledge about other services performed by KPMG
- The entity's accounting records regarding professional services expenses
- For listed entities, we may keep a complete list of our services, including engagement letters.

How may we obtain an understanding of the nature of the engagements? [ISA | 546.1500]

To obtain our understanding of the nature of the engagements, we may inspect:

- the written descriptions of the nature of services provided in Sentinel and in the engagement letters, so that we understand the key aspects of the services provided; and
- the primary deliverables we provided to the entity as part of the services.

We may also inquire of the engagement partner and engagement manager about:

- the nature of the services provided;
- key findings and issues communicated; and
- information gathered about the entity that might help deepen our understanding.

How do we determine what information from other engagements is relevant? [ISA | 546.1600]

We use our judgment to determine what information from other engagements might help us identify and assess RMMs.

We may identify and assess RMMs based simply on the nature of the services or details of the results of our services. For example, our advisory practice may be engaged to:

- report on gaps or areas for improvement regarding an entity's people, processes, internal controls or information systems; or
- highlight challenges and opportunities facing an entity or an acquisition target.

Similarly, our tax practice may be engaged to help management with tax exposure or examination matters.

Example

What information from other engagements might help us identify and assess RMMs? [ISA | 546.1700]

Example 1

An entity is issuing new debt and has engaged the audit team to provide a comfort letter. While performing this service, the engagement team inspect the terms of the new debt issuance and identify a number of complex terms in the debt arrangement. These terms suggest that there may be RMMs related to the accounting for the new debt issuance.

Example 2

An entity is acquiring a target and has engaged the audit team to perform due diligence services.

The engagement team inspects information about the nature of the services, makes inquiries of the engagement partner and engagement manager, and reads the due diligence report. In doing so, they identify that the target has not quantified or recorded a liability for self-insured health and workers' compensation claims. The engagement team may identify an RMM for the unrecorded liabilities, related to the accounting for the business combination.

Example 3

After inspecting the Sentinel report for the entity and its affiliates, the engagement team identifies that specific team members with expertise in Tax provide tax compliance services to the entity.

The engagement team inspects information about the nature of these services, and inquires directly of the engagement tax partner and engagement tax manager. In doing so, the engagement team identifies additional information on a number of the entity's uncertain tax positions. The engagement team identifies an RMM related to the accounting for uncertain tax positions in several jurisdictions in which the entity operates.

1.4.3 Consider information from past engagements in identifying and assessing RMMs

[ISA | 542]

What do we do?

Consider whether information from past engagements is relevant to identifying and assessing risks of material misstatement

Why do we do this?

When we have obtained information from previous engagements with the entity, we have a significant knowledge base when we start our current audit — including knowledge about:

- risks of material misstatement (RMMs) we previously identified; and
- significant ongoing matters that can affect the current financial statements.

This knowledge is a helpful starting point to identify and assess RMMs in the current period. However, we cannot simply rely on past knowledge. Entities often undergo changes from period to period, as well as during the period. Combining our previous knowledge with our understanding of these changes helps us identify and assess the RMMs that are relevant to the current financial statements.

Execute the Audit

How may we identify information from past engagements that is relevant to identifying and assessing RMMs in the current period? [ISA | 542.1300]

We may identify information that helps us identify and assess RMMs in the current period by drawing on the experience of team members involved in auditing or reviewing the entity's prior periods' financial statements.

We may also inspect the prior-period audit or review files for key information about our findings and significant ongoing matters that affect how we think about RMMs in the current period.

Fact pattern:

In the prior-period audit, the engagement team identified an RMM related to the valuation of goodwill and other intangible assets, because of increased market competition and lower near-term projected earnings.

Since that audit, the goodwill and intangible asset balances have not significantly changed. The entity continues to operate in a similar business environment with similar margins.

Analysis:

Given the lack of changes and the risks that existed in the prior period, the team may identify an RMM in the current period related to the valuation of goodwill and other intangible assets.

What type of information from past engagements may be relevant to identifying and assessing RMMs in the current period? [ISA | 542.1400]

When we consider what information may be relevant to our current risk assessment, we focus on ongoing matters that:

- could have multi-period accounting effects; and/or
- point to potential RMMs in the current period.

Significant matters we may consider include:

- misstatements, and whether they were corrected on a timely basis — including disclosures;
- the nature of the entity and its environment, and the entity's internal controls — including deficiencies in internal controls that were not remediated at the end of the prior period;
- acts and/or allegations of fraud;
- areas where we had difficulty performing the audit procedures - e.g. a complex goodwill impairment calculation model;
- significant unusual transactions;
- related party transactions;
- consultation matters; and
- communications with management, those charged with governance and others.

If we identify significant changes in the entity and its operations from prior periods, how do we consider these in identifying and assessing RMMs? [ISA | 542.1500]

Through our risk assessment procedures, we may identify significant changes in the entity. These changes can highlight situations where RMMs may have changed between periods and lead us to conclude that:

- new RMMs have emerged;
- RMMs have changed; and/or
- RMMs from the prior period are no longer relevant.

When we identify changes during our risk assessment procedures, we may ask the following questions.

- How does this change our view about the RMMs affecting the entity?
- What changes would we make to the RMMs we identify and assess in our current audit?

Fact pattern:

In past audits, the engagement team identified an RMM related to how the entity measures its defined benefit plan obligation. In the current period, the entity settles the pension plan obligation with a lump-sum payment to the plan participants. This new, relevant information may change the RMM that the team previously identified.

Analysis:

The team decide that the RMM identified in the prior period is no longer relevant because of the changes identified in the current period - i.e. the settlement transaction. They also identify a new RMM related to how the entity accounts for and discloses the settlement of the pension plan obligation.

1.4.4 Evaluate the relevance and reliability of information from past audits [ISA | 543]

What do we do?

IF we plan to limit the nature, timing, or extent of risk assessment procedures by relying on information from past audits, THEN evaluate whether the prior periods' information remains relevant and reliable

Why do we do this?

As we perform our risk assessment procedures, we may identify that we have information from a past audit which might allow us to limit the nature, timing and extent of our risk assessment procedures in the current audit.

But first we cautiously evaluate whether prior-period information remains relevant and reliable. If there have been significant changes in industry, regulatory, external or entity-specific factors, then the effectiveness of this information may be reduced or eliminated.

Execute the Audit

When might we rely on prior-period information to limit our current risk assessment procedures? [ISA | 543.1300]

We rarely rely on prior-period information to limit our current risk assessment procedures. This is due to:

- the multitude of changes that often happen from one period to the next; and
- the importance of our risk assessment procedures.

We may rely on prior-period information when we have obtained evidence - e.g. specific documents, agreements - that we expect to be applicable and unchanged for several periods - e.g. information about long-term compensation arrangements or multi-year bonus plans that we obtained in a prior period.

How do we determine whether the prior-period information remains relevant and reliable? [ISA | 543.1400]

To determine the relevance and reliability of prior-period information, we may perform additional procedures, such as:

- inspecting documents from the current period;
- performing inquiries and observation and
- performing walkthroughs of relevant systems.

We perform these procedures to corroborate that no changes have occurred — but we don't simply 'check the box'. We still consider how our understanding of this information affects our identification and assessment of risks of material misstatement (RMMs) in the current audit.

For example, we consider:

- any changes that have occurred; and
- any disconfirming evidence that we identify throughout our current audit

that lead us to re-evaluate whether the prior-period information remains relevant and reliable.

What prior-period information do we not rely on to limit our risk assessment in the current period? [ISA | 543.1500]

We cannot rely on our understanding of processes and controls obtained in the prior period.

We may use this knowledge to start our risk assessment process. However, we perform procedures to obtain an understanding of business processes and evaluate the design and implementation of controls relevant to the audit every audit period.

We do this each period because of the dynamic nature of the entities we audit, and the risk that changes may have occurred that we do not know about.

Example

How may we use information from past audits in performing our risk assessment procedures? [ISA | 543.1600]

Fact pattern:

The engagement team obtained and inspected all the entity's compensation plan agreements during the prior-period audit and determined that they are effective for the next four years. The team therefore expect that they will not change before they expire.

Analysis:

Assessing the relevance and reliability of prior-period information

Inspecting these agreements again may be unnecessary. For the current audit, the team may be able to limit the risk assessment procedures they perform in obtaining an understanding of compensation agreements from senior management.

Before they limit their procedures, the team first evaluate whether these agreements are still relevant and reliable in the current period — for example, by:

- inspecting the entity's board minutes and compensation committee minutes to determine that the compensation agreements have not been amended;
- inspecting the entity's forms and statements filed with regulatory agencies to identify any amendments or new agreements that have been approved; and
- inquiring of management and the compensation committee members to determine whether they are aware of changes to the agreements.

If the team determine that these compensation agreements are still relevant and reliable, they may limit their risk assessment procedures in the current audit by relying on the information obtained in the prior period.

Identifying and assessing RMMs in the current period

In order to limit risk assessment procedures in the current audit, it's not enough for the team just to 'check the box' by obtaining the compensation agreements.

The team go further and consider how their understanding of these agreements affects how they identify and assess RMMs in the current audit - e.g. by thinking about:

- the RMMs that might exist when the compensation arrangements are complex or difficult to account for; or
- whether there are performance targets to meet.

Considering the impact of disconfirming evidence in identifying and assessing RMMs

As in other areas of the audit, the team also consider:

- changes that have occurred; and
- disconfirming evidence identified throughout the audit

that may lead them to re-evaluate whether the prior-period information continues to be relevant and reliable.

For example, when testing payroll expenses in the current audit, the team may discover a new compensation plan or a change to an existing plan that they hadn't previously identified. In these cases, the team:

- re-evaluate whether the previous information is still relevant and reliable; and
- design additional risk assessment procedures to consider the newly identified information.

1.5 Discuss matters affecting the identification and assessment of RMMs among the engagement team [ISA | 552]

What do we do?

Conduct a discussion among engagement team members regarding the risks of material misstatement

Why do we do this?

Holding a discussion among team members allows us to share experience, insights and opinions, and to generate questions about the entity and its risks of material misstatement (RMMs). Considering these questions helps us make our initial risk assessment and planning decisions.

Execute the Audit

Why do we discuss matters affecting the identification and assessment of RMMs among engagement team members? [ISA | 552.1300]

The engagement team discussion is an opportunity for us to understand and discuss possible RMMs with the key members of the engagement team. At KPMG, we call this the Risk Assessment and Planning Discussion (RAPD).

The RAPD allows us to harness the collective knowledge and different views of the engagement team regarding RMMs. Hearing others' points of view helps spur ideas and thinking, and helps engagement team members:

- give appropriate thought to the audit areas, events or matters which may indicate RMMs; and
- understand how the results of our audit procedures may affect other aspects of the audit — including decisions about the nature, timing and extent of further audit procedures.

The RAPD is a means to gather key engagement team members early in the audit, and collectively analyze what we know about the entity. It's most effective when all the key team members have been sufficiently involved in the risk assessment procedures and are fully engaged in the discussion.

We conduct the RAPD in an environment where all team members feel free to speak up and express their thoughts and concerns. This allows us to consider all their different viewpoints and observations.

Our RAPD is not merely a 'check-the-box' exercise — it's a key element of our overall risk assessment procedures, and of identifying and assessing the relevant RMMs up-front.

Who are the key members of the engagement team? [ISA | 552.11510]

The key members of the engagement team are, at the minimum, the engagement partner and engagement manager. The engagement partner may decide to involve other members of the engagement team in the RAPD or equivalent discussion.

Group Audit | Do we include component auditors in the RAPD? [ISA | 552.160035]

Yes, we include, at a minimum, the component engagement partner and component engagement manager in the RAPD. This can be achieved through a single RAPD with component engagement partners and component engagement managers or through a series of RAPDs.

When do we hold this discussion? [ISA | 552.1400]

The RAPD is most effective:

- after we've obtained an understanding of the entity and its environment — including all components of its internal control; but
- before we start designing and executing the remainder of our audit plan.

This information provides a better knowledge base for our discussion.

The auditing standards don't prevent us from holding engagement team discussions and communications more than once during an audit — in fact they promote it. The RAPD is a key element of risk assessment, but we can communicate information and risk factors at any time.

Risk assessment is an iterative process, so we remain alert throughout the audit to matters that may affect our identification and assessment of RMMs. Circumstances may arise, or we may obtain information, indicating that our identification and assessment of RMMs may be different from that determined in the RAPD.

We *may* discuss RMMs due to error separately from fraud risks. However, it's usually more convenient to hold the two discussions together — especially as all of the relevant members are already participating, and it leverages the same information we have gathered.

Who participates in the discussion? [ISA | 552.1500]

The lead engagement partner always participates in the discussion. Key engagement team members also participate in the discussion, but don't all have to participate at the same time.

The engagement partner may decide to involve other members of the engagement team in the RAPD or equivalent discussion by using professional judgment, prior experience with the entity and knowledge of current developments.

The other participants in the discussion may include:

- other partner(s)
- other audit senior manager(s)/manager(s)
- audit senior associate(s)/in-charge auditor(s)
- audit associate(s)
- tax partner(s) and manager(s)
- IT Audit partner(s) and manager(s)

- other specific team members and/or employed KPMG specialists partner(s) and manager(s) of member firms that are participating in the audit.
- In addition, the engagement quality review (EQR) partner and their delegates may attend the discussion to gain the necessary understanding of the entity.

Are there certain matters that we always discuss at the RAPD? [ISA | 552.1600]

Yes. At a minimum, we discuss the items included in the RAPD agenda https://alex.kpmg.com/AROWeb/document/lfc/GO_AR_KCW_AR_205900_RAPD_Agenda_LP template, unless the item is indicated as optional. We may add additional items.

What other topics may be discussed during our discussion? [ISA | 552.1700]

When the key engagement team members are gathered together, we may take this opportunity to discuss other important matters related to planning and organizing the audit — for example:

- the overall responsibilities of each key engagement team member;
- topics we may want to discuss throughout the audit with the EQR, specific team members, and other reviewers;
- whether the results of the latest Quality Performance Review apply to the audit, and any matters to pay close attention; and
- our preliminary thoughts on potential audit responses for other identified RMMs.

Group Audit | How may we incorporate group audit considerations in the RAPD? [ISA | 552.8079]

When we hold a RAPD for a group audit, we think about the items included in the RAPD agenda template in the context of the group audit and discuss those items not only for the group entity but for its components as relevant. We customize the RAPD agenda, as necessary, to document the contents of our discussion including: the significant decisions reached, how and when the discussion occurred, and the audit team members who participated.

Examples of items that we may discuss from a group audit perspective include:

- How the accounting principles have been communicated to management of entities or business units and how differences in accounting principles are identified and adjusted
- Fraud risk factors that are present across components that may indicate a fraud risk or non-compliance with national laws or regulations to the extent relevant to the group financial statements
- Significant risks to the group financial statements and the components where we plan to perform work to address those significant risks
- Financial statement level risks and the risk of management override and the components where we plan to perform work to address those
- Significant unusual transactions and related parties at the components
- Any other relevant group audit scoping considerations
- The overall responsibilities of component auditors

1.5.1 Discuss accounting policies or principles and susceptibility of financial statements to material misstatement [ISA | 553]

What do we do?

Discuss (1) the entity's selection and application of accounting policies or principles, including related disclosure requirements and (2) the susceptibility of financial statements to material misstatement due to error or fraud

Why do we do this?

Engaging in a meaningful discussion about the entity's accounting policies or principles, how they've been applied, and whether they're appropriate — while considering where the entity's financial statements may be more susceptible to material misstatement — is likely to confirm, or may point us to new, risks of material misstatement (RMMs).

Execute the Audit

What do we focus on when discussing the application of the financial reporting framework including accounting policies or principles, and related disclosure requirements? [ISA | 553.1300]

The Risk Assessment and Planning Discussion (RAPD) includes a meaningful, thought-provoking analysis of:

- the financial reporting framework, including the entity's accounting policies or principles;
- how they have been applied;
- whether they are appropriate to the entity and its circumstances, and
- related disclosure requirements.

Prior-period knowledge and understanding is valuable, and we incorporate it in our discussion. However, all participants in the discussion take a fresh look at these matters.

What questions might we ask during this discussion? [ISA | 553.11518]

Throughout the discussion, we may find it helpful to ask ourselves the following questions.

- Are the accounting policies or principles appropriate for the entity?
- Are they common practice in the industry?
- How have they been implemented — especially in emerging areas, or areas in which the accounting requirements are less prescriptive?
- Will changes in financial reporting requirements result in significant new or revised disclosures?
- Will changes in the entity's environment, financial condition or activities result in significant new or revised disclosures — e.g. a significant business combination in the period under audit?
- Has it been difficult in the past to obtain sufficient appropriate audit evidence for certain disclosures?
- Are there any disclosures about complex matters, including those involving significant management judgment as to what information to disclose?

How might we begin this discussion? [ISA | 553.11519]

We might begin the discussion by inspecting the results of our risk assessment procedures or the entity's accounting policies note from the prior period financial statements, and by considering any changes we are aware of in the current period.

Changes can occur for many reasons, including:

- changes in the entity's business during the period - e.g. a new line of business;
- new accounting policies or principles that were adopted during the period;
- recent significant changes in the economic, regulatory, industry, or other aspects of the environment in which the entity operates; and
- changes in the way the entity applies its current accounting policies or principles.

What do we focus on when discussing the susceptibility of the entity's financial statements to material misstatement? [ISA | 553.1400]

In discussing the susceptibility of the entity's financial statements to material misstatement, we:

- consider all the information gathered throughout risk assessment; and
- share our thoughts about where there may be indications of RMMs, due to both error and fraud.

Our discussion also includes specific consideration of the susceptibility of the financial statements to material misstatement due to error that could result from the entity's related party relationships and transactions.

This may include the matters raised during our RAPD discussion about selecting and applying accounting policies or principles, including related disclosure requirements.

However, we are not limited to items coming from the RAPD discussion. We might also use the prior-period financial statements and related notes as a springboard for discussion, combined with the results of our current-period risk assessment procedures to date.

Our primary goal is to have a robust discussion about the areas of the entity's financial statements that may be susceptible to material misstatements, and therefore evaluate whether RMMs may exist.

Example

What matters might we discuss regarding the entity's selection and application of accounting policies or principles? [ISA | 553.1500]

The table below sets out examples of matters we might identify during risk assessment, and discuss in the RAPD, about the selection and application of accounting policies or principles, including related disclosure requirements.

As we discuss these matters, we consider their effects on risk assessment — specifically on identifying and assessing RMMs.

Matter we identify	**Example discussion points**	Possible effect
The entity is in the early stages of its lifecycle and has just begun	This is the first time the entity is implementing a revenue accounting policy, so there are increased risks	We identify an RMM related to how the entity records and

to generate sales. It is now implementing revenue recognition policies.	associated with selecting and applying the policy. These are affected by the industry and nature of the sales process.	reports revenue in the financial statements and related disclosures.
The entity has completed a significant business combination and is therefore applying business combination accounting policies or principles for the first time.	This is the first time the entity is applying these accounting policies or principles, and the principles are complex. Significant judgments are involved in accounting for business combinations.	We identify an RMM related to the accounting for business combinations, including related disclosures.
The entity has changed its method for accounting for inventory (from FIFO to average cost).	We explore a series of questions, including: • What is the reason for change? • What is accepted within the industry? • Are the entity's systems equipped to manage the change — e.g. can its IT systems properly calculate the average cost? • Was the change adopted at the beginning of the period or mid-period? • How will this be disclosed?	We identify an RMM related to the cost of inventory recorded and consider whether a fraud risk exists.
Due to rising interest rates, the entity updates significant assumptions in its cash flow model for goodwill valuation.	Given the economic environment, the entity needed to update significant assumptions in its cash flow model for goodwill to account for the current economic environment, including the discount rate, inflation, and other projected financial information such as revenue and expenses.	We identify an RMM related to the valuation of goodwill, including related disclosures.

1.5.2 Communicate important matters to team members not involved in the RAPD [ISA | 555]

What do we do?

The lead engagement partner determines which matters are to be communicated to engagement team members not involved in the Risk Assessment and Planning Discussion. The lead engagement partner or other key engagement team members communicate those matters accordingly.

Why do we do this?

Key members of the engagement team may be unable to participate in the Risk Assessment and Planning Discussion (RAPD).

The lead engagement partner is responsible for making sure they are informed of the important matters that were discussed, as these will impact the procedures we perform in response to the risks of material misstatement (RMMs) identified.

Execute the Audit

Who attends the RAPD? [ISA | 555.1300]

Whether we hold one or multiple discussions with the key engagement team members, the lead engagement partner — or another key engagement team member, such as the lead engagement manager — participates in each discussion.

They do this to help maintain consistency, consider each of the key points raised and communicate important matters across the engagement team.

As we plan and conduct the discussion, we think about the overriding objective — to share knowledge and inform team members about important matters that can affect our audit.

Do all key team members participate in the RAPD? [ISA | 555.1400]

It's helpful to have all the key team members in the same place, so we try to find a time where everyone can gather in one place to have the discussion.

However, this may not always be practical, and we may choose to hold separate discussions with some members of the team. For example, an employed KPMG specialist may not be available at the same time as the rest of the team.

Rather than postpone the meeting and potentially delay the planning process, we may meet with those team members separately.

What if key engagement team members are unable to participate in the RAPD? [ISA | 555.1500]

When key engagement team members are unable to participate in the RAPD:

- the lead engagement partner determines which matters to discuss with them; and
- the lead engagement partner (or another key engagement team member) discusses those matters.

A communications plan, agreed by the engagement partner, may be useful.

How else might we hold the RAPD, so that all key engagement team members can be involved? [ISA | 555.1600]

When key engagement team members are unable to participate in person — e.g. if they're in multiple locations — there may be other ways to involve them in the RAPD.

For example, we may use conference calls and/or video-conferencing so that all appropriate people can participate in one discussion.

1.5.3 Communicate significant matters among team members throughout the audit [ISA | 556]

What do we do?

Communicate significant matters affecting risks of material misstatement among engagement team members, throughout the audit, including when conditions change

Why do we do this?

Any engagement team member may obtain significant information, or become aware of events, that could affect our identification and assessment of risks of material misstatement (RMMs).

These include changes in the entity that happened during the audit, and after our risk assessment and planning discussion (RAPD).

We communicate these matters among the engagement team promptly, to keep them informed about the matters and how they may impact the audit.

Execute the Audit

What types of significant matters or changes in the entity do we communicate? [ISA | 556.1300]

We communicate those matters or changes in the entity that occur and affect our identification and assessment of RMMs.

Examples of significant matters we communicate include:

- planned acquisitions or dispositions;
- changes in the operation of the entity or its business lines; and
- potential impacts to the entity's results due to changes in market conditions.

Changes in the entity may relate to a variety of matters, including:

- new transactions the entity enters into;
- control deficiencies that occur; or
- changes in the entity's processes or controls.

> For example, a senior associate on the team may learn, through inquiries with the assistant treasurer, that the entity is negotiating a new financing arrangement.
>
> In this case, the senior associate is expected to tell the engagement manager, so they can consider the effect, and discuss the matter with the engagement partner.

How do we communicate significant matters that occur during the audit? [ISA | 556.1400]

There is no one way to communicate significant matters that arise during the audit among the engagement team. We can use a meeting, a conference call or some other means.

Ultimately, the engagement partner is responsible for determining that changes affecting our risk assessment decisions are promptly communicated among the engagement team.

1.6 Read the meeting minutes of owners, management and those charged with governance

[ISA | 351]

What do we do?

Read the meeting minutes of owners, management and those charged with governance, including any relevant committees of these groups, as part of performing our risk assessment procedures.

Why do we do this?

Minutes record key matters discussed at meetings of owners, management and those charged with governance. Minutes often include decisions and discussions that are important to the entity's operations and business strategy, so reading them can help us gather information that is useful in identifying and assessing risks of material misstatement (RMMs).

Execute the Audit

What types of information might we gather by reading meeting minutes? [ISA | 351.1300]

When we read meeting minutes, we look for information about key decisions made or important matters discussed that could have accounting or financial reporting implications and summarize those items in our audit file. The items may include information about:

- related parties;
- litigation, claims and assessments;
- significant unusual transactions;
- illegal acts;
- going concern;
- fraud risks; and
- accounting estimates.

What types of committees generally exist? [ISA | 351.1400]

Entities are often governed by a board of directors with committees that focus on certain tasks or areas. These tasks generally involve monitoring and advising the entity.

Public entities typically have at least the following committees.

Committee	Description
Audit committee	Oversees the integrity and compliance of financial reporting

Compensation committee	Focuses on human resource policies and procedures, including the compensation of executive officers
Nominating/corporate governance committee	Sets general governance procedures, makes recommendations on new candidates for the board and other top executive positions, makes recommendations on assignments of directors to committees

Boards often form other committees — e.g. for strategy, finance, diversity, corporate social responsibility, diversity and technology.

Do we review the minutes for all committees of the board of directors? [ISA | 351.11564]

No. Our focus is on those committees of the board of directors that oversee and address matters that we believe could impact the financial statements or our audit approach.

What if minutes are not available? [ISA | 351.1500]

If the entity does not keep meeting minutes or has not prepared minutes for a particular meeting, we inquire of attendees — e.g. the secretary of the board of directors or general counsel — to understand the discussions that took place. In this situation, we may find it helpful to inquire of more than one attendee and/or inspect materials from the meeting to corroborate our inquiries about what was discussed at the meeting.

Examples

How might reading the meeting minutes inform our risk assessment? [ISA | 351.1600]

Fact pattern:

During our audit of Entity X, we reviewed the minutes of meetings of the board of directors and its subcommittees, including the audit committee. The minutes discuss the recent closure of a manufacturing facility.

Analysis:

We include this information in our risk assessment and may identify new or increased risks of misstatement arising from closing the manufacturing facility — e.g. risks related to restructuring charges and asset dispositions and impairments.

Understanding the Entity and Its Environment, and the Applicable Financial Reporting Framework

International Standards on Auditing: ISA 315.19-20

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

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

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

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

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

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

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

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

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

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

ISA Application and Other Explanatory Material: ISA 315.A48-A89

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

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

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

A48. Obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control is a dynamic and iterative process of gathering,

updating and analyzing information and continues throughout the audit. Therefore, the auditor's expectations may change as new information is obtained.

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

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

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

- Identifying and assessing risks of material misstatement of the financial statements in accordance with ISA 315 (Revised 2019) or other relevant standards (e.g., relating to risks of fraud in accordance with ISA 240 or when identifying or assessing risks related to accounting estimates in accordance with ISA 540 (Revised));
- Performing procedures to help identify instances of non-compliance with laws and regulations that may have a material effect on the financial statements in accordance with ISA 250;[27]
- Evaluating whether the financial statements provide adequate disclosures in accordance with ISA 700 (Revised);[28]
- Determining materiality or performance materiality in accordance with ISA 320;[29] or
- Considering the appropriateness of the selection and application of accounting policies, and the adequacy of financial statement disclosures.

---

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

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

29 ISA 320, Materiality in Planning and Performing an Audit, paragraphs 10.11

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

- Developing expectations for use when performing analytical procedures in accordance with ISA 520;[30]
- Designing and performing further audit procedures to obtain sufficient appropriate audit evidence in accordance with ISA 330; and

- Evaluating the sufficiency and appropriateness of audit evidence obtained (e.g., relating to assumptions or management's oral and written representations).

---

30 ISA 520, paragraph 5

Scalability

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

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

A53. The auditor's risk assessment procedures to obtain the required understanding may be less extensive in audits of less complex entities and more extensive for entities that are more complex. The depth of the understanding that is required by the auditor is expected to be less than that possessed by management in managing the entity.

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

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

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

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

The entity's organizational structure and ownership

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

- The complexity of the entity's structure.

Example:

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

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

Example:

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

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

Examples:

An entity may:

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

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

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

Automated tools and techniques

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

Considerations specific to public sector entities

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

Example:

A public sector entity may be subject to laws or other directives from authorities that require it to obtain approval from parties external to the entity of its strategy and objectives prior to it implementing them. Therefore, matters related to understanding the legal structure of the entity may

include applicable laws and regulations, and the classification of the entity (i.e., whether the entity is a ministry, department, agency or other type of entity).

Governance

Why the auditor obtains an understanding of governance

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

Understanding the entity's governance

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

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

The Entity's Business Model

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

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

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

Examples:

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

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

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

Understanding the entity's business model

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

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

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

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

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

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

Considerations specific to public sector entities

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

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

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

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

Industry factors

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

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

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

Example:

In the construction industry, long-term contracts may involve significant estimates of revenues and expenses that give rise to risks of material misstatement. In such cases, it is important that the engagement team include members with the appropriate competence and capabilities.[33]

33 ISA 220 (Revised), paragraph 25-28

Regulatory factors

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

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

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

34 ISA 250 (Revised), paragraph 13

Considerations specific to public sector entities

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

Other external factors

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

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

Why the auditor understands measures used by management

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

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

Measures used by management

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

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

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

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

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

Examples:

For some less complex entities, the terms of the entity's bank borrowings (i.e., bank covenants) may be linked to specific performance measures related to the entity's performance or financial position (e.g., a maximum working capital amount). The auditor's understanding of the performance measures used by the bank may help identify areas where there is increased susceptibility to the risk of material misstatement.

For some entities whose nature and circumstances are more complex, such as those operating in the insurance or banking industries, performance or financial position may be measured against regulatory requirements (e.g., regulatory ratio requirements such as capital adequacy and liquidity ratios performance hurdles). The auditor's understanding of these performance measures may help identify areas where there is increased susceptibility to the risk of material misstatement.

Other considerations

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

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

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

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

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

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

Considerations specific to public sector entities

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

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

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

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

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

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

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

Considerations specific to public sector entities

A84. The applicable financial reporting framework in a public sector entity is determined by the legislative and regulatory frameworks relevant to each jurisdiction or within each geographical area. Matters that may be considered in the entity's application of the applicable financial reporting requirements, and how it applies in the context of the nature and circumstances of the entity and its environment, include whether

the entity applies a full accrual basis of accounting or a cash basis of accounting in accordance with the International Public Sector Accounting Standards, or a hybrid.

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

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

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

A85. Understanding the entity and its environment, and the applicable financial reporting framework, assists the auditor in identifying events or conditions, the characteristics of which may affect the susceptibility of assertions about classes of transactions, account balances or disclosures to misstatement. These characteristics are inherent risk factors. Inherent risk factors may affect susceptibility of assertions to misstatement by influencing the likelihood of occurrence of a misstatement or the magnitude of the misstatement if it were to occur. Understanding how inherent risk factors affect the susceptibility of assertions to misstatement may assist the auditor with a preliminary understanding of the likelihood or magnitude of misstatements, which assists the auditor in identifying risks of material misstatement at the assertion level in accordance with paragraph 28(b). Understanding the degree to which inherent risk factors affect susceptibility of assertions to misstatement also assists the auditor in assessing the likelihood and magnitude of a possible misstatement when assessing inherent risk in accordance with paragraph 31(a). Accordingly, understanding the inherent risk factors may also assist the auditor in designing and performing further audit procedures in accordance with ISA 330.

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

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

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

Example:

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

A88. The greater the extent to which a class of transactions, account balance or disclosure is susceptible to misstatement because of complexity or subjectivity, the greater the need for the auditor to apply professional skepticism. Further, when a class of transactions, account balance or disclosure is

susceptible to misstatement because of complexity, subjectivity, change or uncertainty, these inherent risk factors may create opportunity for management bias, whether unintentional or intentional, and affect susceptibility to misstatement due to management bias. The auditor's identification of risks of material misstatement, and assessment of inherent risk at the assertion level, are also affected by the interrelationships among inherent risk factors.

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

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Obtain an understanding of the entity and its environment [ISA | 342]

What do we do?

Obtain an understanding of the entity and its environment.

Why do we do this?

Different events, conditions and activities - internally and externally - can affect an entity's business, overall financial position and results. Identifying this information at the audit's outset helps us assess risk and plan our audit, so we start our risk assessment procedures by understanding these different events, conditions and activities.

Execute the Audit

Enhanced | How do we obtain an understanding of the entity and its environment? [ISA | 342.6236]

We obtain an understanding of the entity and its environment for purposes of our risk assessment through specifically understanding the following:

- the relevant industry, regulatory and other external factors
- the nature of the entity
- the financial relationships and transactions with executive officers
- the entity's selection and application of accounting policies or principles, including related disclosures
- the entity's objectives, strategies and related business risks
- the entity's measurement and analysis of its financial performance

In addition to obtaining an understanding of the above information, we evaluate whether significant changes in the entity from prior periods affect RMMs.

Core and Less Complex | How do we obtain an understanding of the entity and its environment? [ISA | 342.6236]

We obtain an understanding of the entity and its environment for purposes of our risk assessment through specifically understanding the following:

- the relevant industry, regulatory and other external factors
- the nature of the entity
- the entity's selection and application of accounting policies or principles, including related disclosures
- the entity's objectives, strategies and related business risks
- the entity's measurement and analysis of its financial performance

In addition to obtaining an understanding of the above information, we evaluate whether significant changes in the entity from prior periods affect RMMs.

Enhanced | What procedures do we consider performing to obtain an understanding of the entity and its environment? [ISA | 342.11443]

To obtain an understanding of the entity, we consider performing the below procedures. The extent of the procedures will vary based on the amount of information available and our expectations about the insight we will gain about risks from performing them. These procedures include:

- reading public information about the entity that helps us evaluate the likelihood of material financial statement misstatements and, in an integrated audit, the effectiveness of the entity's internal control over financial reporting - e.g. entity-issued press releases and materials for presentations to analysts and investor groups, analyst reports;
- observing or reading transcripts of earnings calls and, where publicly available, other meetings with investors or rating agencies;
- understanding compensation arrangements with senior management other than executive officers, including incentive compensation arrangements, changes to those arrangements, and special bonuses;
- obtaining information about trading activity in the entity's securities and holdings in the entity's securities by significant holders to identify potentially significant unusual developments;
- inquiring of the chair of the compensation committee (or equivalent committee), as well as any compensation consultants that the compensation committee or the entity has engaged, about the design of the entity's compensation for executive officers; and
- understanding established policies and procedures for authorizing and approving executive officer expense reimbursements.

We may identify other information or perform other procedures that are useful in understanding the entity and its environment. When we perform procedures other than those listed above, we also document them.

Core and Less Complex | What procedures do we consider performing to obtain an understanding of the entity and its environment? [ISA | 342.11443]

To obtain an understanding of the entity, we consider performing the below procedures. The extent of the procedures will vary based on the amount of information available and our expectations about the insight we will gain about risks from performing them. These procedures include:

- reading public information about the entity that helps us evaluate the likelihood of material financial statement misstatements and, in an integrated audit, the effectiveness of the entity's

internal control over financial reporting - e.g. entity-issued press releases and materials for presentations to analysts and investor groups, analyst reports;
- observing or reading transcripts of earnings calls and, where publicly available, other meetings with investors or rating agencies; and
- obtaining information about trading activity in the entity's securities and holdings in the entity's securities by significant holders to identify potentially significant unusual developments.

Additionally, if deemed appropriate by the engagement team based on the engagement facts and circumstances, we may also:

- understand compensation arrangements with senior management other than executive officers, including incentive compensation arrangements, changes to those arrangements, and special bonuses;
- read the employment and compensation contracts between the entity and its executive officers;
- read entity filings with regulatory agencies that relate to the entity's financial relationships and transactions with its executive officers;
- inquire of the chair of the compensation committee (or equivalent committee), as well as any compensation consultants that the compensation committee or the entity has engaged, about the design of the entity's compensation for executive officers; and
- review minutes of compensation committee meetings;
- inquire of individuals who may know about transactions with executive officers;
- understand established policies and procedures for authorizing and approving executive officer expense reimbursements.
- analyze financial statement accounts that could be affected by the entity's financial relationships and transactions with its executive officers - e.g. related party accounts receivable.

We may identify other information or perform other procedures that are useful in understanding the entity and its environment. When we perform procedures other than those listed above, we also document them.

What questions might we ask the compensation committee chair and any compensation consultants? [ISA | 342.11444]

The following questions may be helpful when we inquire of the compensation committee chair (or equivalent) and any compensation consultants (engaged by the compensation committee or the entity) about the entity's compensation structure.

- How and for whom are incentive compensation arrangements created, and who has input into the terms?
- How much of management's target compensation is discretionary - i.e. not tied to specific measurable criteria - and why does the compensation committee believe that is appropriate?
- How is the compensation structure set and approved, including targets for measuring performance?
- How is an individual's performance evaluated against the terms of the compensation arrangement?
- How is fraudulent financial reporting considered in overseeing compensation arrangements?

What other information can help us understand the entity and its environment? [ISA | 342.11445]

Many other sources of information can help us understand an entity and its environment, but a few are helpful across most entities. Common sources include:

- information prepared by the entity for internal use:
  - internal financial reporting information, including management reports;
  - minutes of meetings of shareholders, board of directors and board committees;
  - budgets and long-term entity strategy presentations to the board of directors;
  - organizational and legal entity charts;
- information obtained through inquiries with accounting and non-accounting personnel, and the board of directors;
- government laws and regulations; and
- debt and other contractual agreements.

What information do we focus on when obtaining an understanding of the entity and its environment? [ISA | 342.11448]

We focus on obtaining information that will help us obtain the understanding to identify and assess RMMs. Therefore, information relevant to understanding the entity and its environment, including the entity's internal control is our primary focus. Some information may reveal RMMs directly. Other information may give us insights about the entity that help us assess risks, and plan and execute the audit.

As we perform these procedures, it's helpful to ask:

- "What could this information tell me about the entity that might be useful?"
- "Does this information highlight a risk that might cause a material misstatement?"

This can help us better identify risks to address in our audit and focus on the information that is most relevant to the audit.

How extensive an understanding of the entity and its environment do we obtain? [ISA | 342.11449]

We use professional judgment to determine the extent of our understanding of the entity and its environment. Our main consideration is whether that understanding is sufficient for us to identify and assess the RMMs. It does not need to be as deep as the understanding management needs to manage the entity.

For recurring audits, do we obtain this understanding of the entity and its environment for each period? [ISA | 342.11450]

Yes. We may think we already know enough about the entity from our past experience, or that some information we collect is not important to the audit. This thinking can be dangerous - we may fail to identify risks that are relevant to the audit.

Knowledge gained in prior periods often helps us assess risks in the current period's audit. However, we also think about whether changes have occurred since the previous audit that may affect its relevance to the current audit.

For recurring audits, we also consider:

- changes in the economy, legal and regulatory, industry sector, technology; and
- changes driven by the entity's decisions (e.g., strategic changes)

that may lead us to identify new risks or modify risks we identified in the prior period.

Approaching these activities with an open mind can help us avoid missing risks in the current period and shift our focus away from previously identified risks that are no longer relevant.

1.1 Understand relevant industry, regulatory and other external factors [ISA | 343]

What do we do?

Obtain an understanding of relevant industry, regulatory and other external factors.

Why do we do this?

Risks can arise from the entity's industry or regulatory environment, or from economic conditions.

For example, an oil and gas company is likely affected by risks from rising and falling commodity prices. These fluctuations can affect not only the entity's operations but also its asset values, its ability to service debt, and other areas that could lead to a risk of misstatement.

Understanding the industry, regulatory and other external factors helps us identify and assess risks of material misstatement (RMMs).

Execute the Audit

What does our understanding include? [ISA | 343.1300]

A broad range of topics may be relevant to our understanding. At a minimum, we understand:

- industry factors, including the competitive environment and technological developments;
- the regulatory environment, including the applicable financial reporting framework and the legal and political environment; and
- external factors, including general economic conditions.

See 'Understand the applicable legal and regulatory framework' for additional guidance.

What sources of information can help us understand the relevant industry, regulatory and other external factors? [ISA | 343.1400]

Along with the common sources of information we use to understand the entity and its environment, we can also use the Geographical Market Summaries https://alex.kpmg.com/AROWeb/bridge/6209/17939?d=INTL,US. These outline potential audit considerations and risks for specific geographic markets.

When we audit entities with operations in multiple locations, these summaries can help us understand the local operating environments.

What is a financial reporting framework? [ISA | 343.7468]

All financial statements are prepared in accordance with a 'financial reporting framework' — i.e. a set of criteria used to determine how material items are measured, recognized, presented and disclosed in the financial statements. Commonly used financial reporting frameworks include US GAAP and IFRS.

What matters might we consider when obtaining an understanding of the financial reporting framework? [ISA | 343.7469]

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 we may consider:

- The entity's financial reporting practices in terms of the applicable financial reporting framework, such as:
  - Accounting principles and industry-specific practices, including for industry-specific significant classes of transactions, account balances and related disclosures in the financial statements (for example, loans and investments for banks, or research and development for pharmaceuticals).
  - Revenue recognition.
  - Accounting for financial instruments, including related credit losses.
  - Foreign currency assets, liabilities and transactions.
  - Accounting for unusual or complex transactions including those in controversial or emerging areas (for example, accounting for cryptocurrency).
- Other accounting rules, regulations and guidance that may apply. For example:
  - Entities in the banking industry may follow other regulatory reporting requirements specific to the jurisdiction in which the entity operates.
  - Entities filing with the SEC also follow SEC rules, regulations and interpretative guidance.

What information might help us understand the industry, regulatory and other external factors? [ISA | 343.1600]

The table below sets out examples of information we may gather as we obtain our understanding of the relevant industry, regulatory and other external factors.

Type of understanding	Examples of information we may gather
Industry, including competitive environment and technological developments	• The entity's competitive environment, including demand, capacity and price competition. For example, the entity may operate in an industry populated with aggressively growth-focused start-ups, putting pressure on pricing and margins. • Highly cyclical or seasonal activity in the entity's industry. For example, entities in the retail industry may see higher sales during holiday seasons. • Technological developments. For example, rapid technological changes may make the entity's products obsolete. • Energy supplies and costs. For example, volatile fuel prices or disruptions in fuel supplies could affect the operations and financial results of a commercial airline.

Regulatory environment, including applicable financial reporting framework and legal and political environment	• Applicable financial reporting framework (e.g., US GAAP, IFRS), as well as specific industry practices and changes in accounting standards that are relevant to the entity. • Government legislation, regulation or policies. For example, the entity may receive government aid, or be subject to foreign exchange controls, fiscal tariffs or trade restrictions. • Tax and environmental laws. For example, the entity may be subject to complex tax laws in multiple tax jurisdictions.
External factors, including general economic conditions	• Changes in general economic conditions or interest rates. For example, the entity may operate in an inflationary environment or economy in recession. • Volatile commodity prices. For example, fluctuating oil prices could affect the operations and financial results of an oil and gas company. • Lack of available capital in the marketplace. For example, the entity may have to refinance debt in the next 12 months in a public market with very limited liquidity.

1.2 Understand the nature of the entity [ISA | 344]

What do we do?

Obtain an understanding of the nature of the entity, including understanding certain specific elements.

Why do we do this?

Risks can arise not only from external factors but also from entity-specific conditions. These include:

- the entity's defining characteristics;
- how the entity conducts business, including its business model; and
- how the entity is organized.

Understanding the nature of the entity can help us identify potential risks of material misstatement (RMMs) in the financial statements.

Execute the Audit

What do we consider when understanding the nature of the entity? [ISA | 344.1300]

Obtaining an understanding of certain specific elements of the business model can help us understand the nature of the entity overall. These include the entity's:

- organizational structure and management personnel, including ownership and governance structure, including the extent to which the business model integrates the use of IT;
- sources of funding for operations and investment activities, including its capital structure, non-capital funding - e.g. subordinated debt, dependencies on supplier financing - and other debt instruments;
- significant investments, including equity method investments, joint ventures, special-purpose entities and variable-interest entities;
- operating characteristics, including its size and complexity, which might affect the risks of misstatement (RMs) and how the entity addresses those risks;
- sources of earnings, including the relative profitability of key products and services; and
- key supplier and customer relationships.

Our goal in gathering this information is to obtain information that helps us identify and assess risk. We do not gather a detailed history of the entity - e.g. the period in which it was founded - unless we expect that information could lead us to identify RMMs.

What are examples for each of the specific elements? [ISA | 344.7474]

Obtaining an understanding of certain specific elements can help us understand the nature of the entity overall.

The table below sets out examples for each of the specific elements.

Elements	Examples
Organizational structure and management personnel, including ownership and governance	• The scope of the entity's activities, and why it does them. • The entity's structure and scale of its operations. • Whether the entity operates in multiple locations with multiple management levels. Complex structures may give rise to RMMs. For example, there may be RMMs related to accounting for goodwill, joint ventures, investments and special-purpose entities. • Relationships between owners and other people or entities. For example, this information helps determine whether related-party transactions were appropriately identified, accounted for and disclosed in the financial statements. • Few owners with significant ownership interests and seats on the board of directors. • Publicly traded and thus owned by many shareholders. • In some cases, some or all of those charged with governance may be involved in managing the entity. In other cases, those charged with governance and management may comprise different persons. • Governance of the entity may be the collective responsibility of a governing body - e.g. board of directors, supervisory board, partners, trustees, equivalent persons. • In smaller entities, one person may be charged with governance, such as an owner-manager or sole trustee.

Sources of funding for operations and investment activities, including capital structure, non-capital funding, and other debt instruments	• Relies on debt financing involving complex debt covenants. • Has significant off-balance sheet financing or leasing arrangements. • The entity's capital structure - i.e. proportion of debt versus equity - may have changed from prior periods. • Uses derivative financial instruments. • The entity may have subsidiaries and associated entities, including consolidated and unconsolidated structures. • The beneficial owners may be local or foreign, with or without appropriate business reputation and experience. • Obtained financing from a related party. • Using newly created digital assets to raise capital in the form of an ICO (initial coin offering).
Significant investments, including equity method investments, joint ventures special-purpose entities and variable-interest entities	• Significant equity method investments or consolidated SPEs or VIEs, including some with a limited or specific purpose. • Holds cryptocurrencies or digital assets as investments for long-term capital appreciation or as a means of exchange during normal operations. • Has or plan to make non-recurring acquisitions or divestitures, which may count as significant unusual transactions. • Plans to carry out substantial research and development, or make capital expenditures. • Investments and dispositions of securities and loans.
Operating characteristics, including size and complexity	• The entity may be large and complex, operating in several markets and geographic locations. • Operates some business segments centrally and others de-centrally. • 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. • Uses multiple, distinct IT systems in its business processes. • Nature of revenue sources, products or services, and markets. • Extent of integration of electronic commerce into the entity's operations, for example, in 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.
Sources of earnings, including relative profitability of key products and services	• One profitable revenue stream and others that are near break-even or making losses. • Earns a significant net income from non-operating activities.
Key supplier and customer relationships	• Depends on only a few suppliers for its main income-earning activities. • Sells specialized products and services to only a few key customers. • Key supplier may have recently filed for bankruptcy.

What sources of information can help us understand the nature of the entity? [ISA | 344.1400]

We can use the common sources of information related to understanding the entity and its environment.

How does the organizational structure and physical locations of the entity factor into our understanding of the nature of the entity? [ISA | 344.11456]

We understand the organizational structure of the entity in order to better understand how the entity's physical and geographic locations and presence can generate risks of material misstatement. The information also helps us determine whether the audit represents a group audit or multi-location audit, and how to best organize the audit to address the risks rising from the entity's locations and / or components.

Why does the governance of the entity factor into our understanding of the nature of the entity? [ISA | 344.7471]

We understand the governance of the entity in order to better understand the entity's ability to provide appropriate oversight of its system of internal control. However, this understanding may also provide evidence of deficiencies, which may indicate an increase in the susceptibility of the entity's financial statements to risks of material misstatement.

What is a business model? [ISA | 344.7487]

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 of the business lines), processes, growth opportunities, globalization, regulatory requirements and technologies. The entity's business model describes how the entity creates, preserves and captures financial or broader value, for its stakeholders.

Why does the entity's business model factor into our understanding of the nature of the entity? [ISA | 344.7472]

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

For example, an entity's business model may rely on the use of IT in different ways -

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

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

See 'Understand the entity's objectives, strategies and related business risks' for more information.

What if the entity has invested in special purpose entities (SPEs) or variable-interest entities (VIEs)? [ISA | 344.1500]

Financial reporting frameworks often set conditions that are deemed to amount to control or circumstances for consolidating an SPE or VIE. The frameworks may also set different bases for recognizing income from them. To interpret these requirements, we often obtain a detailed knowledge of the agreements involving the SPE or VIE.

What may we understand about how the entity integrates IT into the business model? [ISA | 344.8074]

Our understanding may include the extent and automation of electronic communication with third parties including customers, suppliers, and governments. Additionally, we may understand the extent of use of cryptocurrencies and digital assets including blockchain.

What are cryptocurrencies and digital assets? [ISA | 344.8080]

A digital asset, in the context of currency and finance, is characterized by its ability to be used for a variety of purposes, including as a means of exchange, as a representation to provide or access goods or services, or as a financing vehicle, such as a security, among other uses. The terms crypto asset and cryptocurrency refer to a type of digital asset that uses cryptography to secure transactions digitally recorded on a distributed ledger (such as a blockchain) and purports to be an item of inherent value (similar, for instance, to real assets like gold or virtual assets) that are designed to enable purchases, sales, barter or other financial transactions.

Blockchain is a distributed ledger technology that records a list of records, referred to as blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp and transaction data. A block is a collection of digital asset transactions to be recorded on a blockchain.

Virtual currencies, tokens and coins may entitle the holder to other rights as well, such as rights to goods or services from the issuer of the token or a right to financial distributions from the issuing entity or the right to virtual digital assets.

Blockchains, virtual currencies, tokens, and virtual coins may be fully decentralized (i.e. they are not associated with a particular individual or organization), or they may be associated with a particular

backing organization (or several organizations in a consortium). In certain cases, whether backed by a traditional organization or not, such digital assets may be considered as being securities.

What may we understand about the extent of use of cryptocurrencies and digital assets? [ISA | 344.8089]

Addressing certain considerations can be helpful when identifying and assessing risks of misstatement related to cryptocurrency and digital assets when an entity transacts or invests in cryptocurrency and digital assets. These may include:

- What is the purpose or strategy for transacting in digital assets and how do those strategies align with the nature of the entity (e.g. operating characteristics, key performance indicators, sources of earnings, etc.)? Are there associated business risks related to digital asset transactions? What is the entity's underlying business and how do the digital assets relate to the entity's business model?
- Are digital asset transactions intended to be used as a source of funding for the entity's operations (e.g. an initial coin offering or "ICO")? Does the entity keep certain digital assets off the balance sheet?
- What are the relevant legal and regulatory requirements governing the entity's use of digital assets? For example, sales of digital assets (e.g. in an ICO), may represent sales of securities subject to jurisdictional regulations and securities laws. Entities that buy and sell digital assets for others may be subject to other laws and regulations, such as money transmitter rules, 'Anti-Money Laundering' and 'Know Your Customer' considerations. Has the entity considered laws and regulations over digital assets and ICOs in other countries and jurisdictions?
- Does the entity use a third-party exchange or service provider to transact digital assets? Has the entity evaluated whether any of the digital assets it holds or transacts (directly or indirectly through a third-party exchange or servicer) are appropriately registered with securities regulators? Does the entity use exchanges that are appropriately registered based on the nature of the digital assets?
- Has the entity identified relevant regulatory frameworks and compliance requirements (i.e. Bank Secrecy Act 'BCA' or Foreign Account Tax Compliance Act 'FATCA', federal securities laws, depository and/ or custodial regulations)? What policies and procedures are in place related to compliance with regulatory frameworks?
- Do the digital assets carry specific rights and obligations including rights to cash flows, ownership characteristics, or utility/discount rights?
- What are the entity's accounting policies related to digital assets, including related disclosures? Has the entity evaluated alternative accounting literature and treatments that could apply to its facts and circumstances? Do accounting and finance personnel have the appropriate knowledge and understanding of the digital asset transactions and how to apply existing accounting policies or principles?
- For subsequent measurements associated with digital assets (e.g., when measuring an impairment of a cryptocurrency investment), how does the entity determine the principal market? For example, some digital assets are listed on multiple exchanges while others are not listed on any exchange and as such an entity may have to employ different methods to subsequently measure these assets in an environment where there may be limited trading history and significant volatility for the asset.

- Are the digital assets held by the entity more common (e.g. Bitcoin, litecoin, XRP, Ether), less common, or emerging? Less common or emerging digital assets are likely to carry additional risks resulting in additional considerations.
- Does the entity offer new products or services to customers that incorporate digital assets (e.g. new investment funds)? How do these products or services differ from the entity's existing product and service lines? Is the entity holding onto the digital assets from a speculative perspective or obtaining the assets through a form of payment related to its primary business? Is the entity consistently trading the digital assets or buying and holding?
- Has the entity considered potential risks associated with the IT requirements to transact in digital assets and compatibility with existing systems? If so, has the entity identified and implemented appropriate policies and procedures to address these potential IT risks?

What other considerations exist regarding cryptocurrencies and digital assets? [ISA | 344.11457]

Blockchain, distributed ledger technologies, and associated 'digital assets' (e.g. cryptocurrencies, tokens, and coins) can raise a number of auditing, accounting, and financial reporting considerations. Where cryptocurrencies and digital assets are significant to the financial statements, we consider the consultation requirements in the Global Quality and Risk Management Manual section 9.1.4. https://www.gqrmm-prod.kworld.kpmg.com/G/0/Content/81?jm=82-policy-23021

1.3 Enhanced | Understand financial relationships and transactions with executive officers [ISA | 345]

What do we do?

Obtain an understanding of the entity's financial relationships and transactions with its executive officers with the objective of identifying risks of material misstatement.

Why do we do this?

Executive officers can often exert significant authority or influence over the entity's business activities, financial position and results. An entity's relationships with executive officers can differ from its relationships with other parties. Many executive officers are also shareholders, so some of their personal net worth may depend on the entity's performance.

For these reasons, investors or regulators may focus on compensation agreements and transactions between the entity and its officers. We may also focus on these financial relationships and transactions in our audit, particularly as it relates to fraud risks.

Execute the Audit

Enhanced | How can understanding these relationships and transactions with executive officers help us identify risks? [ISA | 345.1300]

Understanding the entity's financial relationships and transactions with its executive officers can help us identify possible risks of material misstatement (RMMs), particularly potential fraud risk factors. For example, we may learn that the majority of the CEO's compensation is variable and tied to entity performance targets - e.g. revenues, income, EBITDA. That compensation relationship may

provide incentives or pressures for the CEO to manipulate the entity's operating results, or engage in transactions to meet performance targets and increase personal compensation. Therefore, these pressures and incentives may raise more risk for the entity and highlight possible fraud risk factors.

We may also gain insights about other risks. For example, we may learn that the compensation structure is complex, with different share-based compensation arrangements requiring customized valuation models to determine the award's fair value. This knowledge may reveal an RMM related to how share-based compensation is measured and recorded.

Enhanced | What are examples of executive officers? [ISA | 345.1400]

Executive officers may vary from one entity to another. They are usually appointed by the entity's board of directors. They may be defined by local law or regulation. For example, the SEC defines 'executive officers' of SEC registrants to include the following.

For issuers	For broker-dealers
• President • Any vice president in charge of a principal business unit, division or function - e.g. sales, administration, finance • Any other officer who performs a policy-making function • Any other person who performs similar policy-making functions for an entity	• Chief executive officer • Chief financial officer • Chief operations officer • Chief legal officer • Chief compliance officer • Directors • Individuals with similar statuses or functions

Executive officers of subsidiaries may also be deemed executive officers if they perform policy-making functions for the entity.

For non-SEC registrants, executive officers may be individuals in roles substantially similar to those for an SEC registrant.

Enhanced | What procedures can help us identify RMMs related to the entity's financial relationships and transactions with executive officers? [ISA | 345.1500]

At a minimum, we perform the following procedures to identify RMMs related to the entity's financial relationships and transactions with executive officers:

- read employment and compensation contracts between the entity and its executive officers; and
- read the proxy statements and other relevant entity filings with the SEC and other regulatory agencies that relate to the entity's financial relationships and transactions with its executive officers.

We may perform additional procedures to obtain information that helps us identify and assess risks. These may include:

- reviewing minutes of compensation committee meetings;
- inquiring of individuals who may know about transactions with executive officers; and
- analyzing financial statement accounts that could be affected by the entity's financial relationships and transactions with its executive officers - e.g. related-party accounts receivable.

Enhanced | What if we are auditing an entity that is not a SEC registrant? [ISA | 345.1600]

When we audit an entity that is not a SEC registrant, we perform the same procedures as we do for SEC registrants, except for reviewing proxy statements. Even though proxy statements may not be applicable, the entity may file information with other regulatory agencies that is relevant to this procedure.

Examples

Enhanced | What information might we gather that will help us understand the entity's financial relationships and transactions with its executive officers? [ISA | 345.1700]

The table below sets out examples of information we may gather to understand the entity's financial relationships and transactions with its executive officers.

Procedure	Examples of information we may gather
Reading the employment and compensation contracts between the entity and its executive officers	• The CEO's compensation includes significant variable compensation based on revenue, earnings per share and/or stock price performance targets that are determined annually. • The CEO's variable compensation is payable in the entity's shares or cash at the CEO's discretion. • The CEO's employment contract has limited time remaining - e.g. five years - and variable compensation could be clawed back if the financial statements are restated.
Reading the proxy statements and other relevant entity filings with the SEC and other regulatory agencies related to the entity's financial relationships and transactions with its executive officers	• The executive officers as a group own 20% of the entity's shares. • The executive officers' share-based payment agreements allow for full vesting of their awards if the officers are dismissed without cause. • The CEO owns significant equity in a key supplier. • The entity's compensation policies are more aggressive than similar entities in the industry.

1.4 Understand and evaluate the entity's selection and application of accounting policies or principles, including related disclosures [ISA | 346]

What do we do?

Understand and evaluate the entity's selection and application of accounting policies or principles, including related disclosures.

Why do we do this?

An entity's accounting policies or principles can create risks of misstatement (RMs), generally at the assertion level. Our understanding and evaluation of the accounting policies or principles that the entity has selected and applied (including related disclosures) can help us identify and assess risks of material misstatement (RMMs). Without this understanding, we may be unable to determine whether the entity's transactions are recorded in accordance with generally accepted accounting principles (GAAP), or identify relevant RMs that could stem from applying the financial reporting framework.

Execute the Audit

What is the output of understanding the entity's selection and application of accounting policies or principles? [ISA | 346.160220]

The output of this activity is generally a technical accounting analysis for each audit area. This analysis outlines our understanding of the accounting policies or principles selected and applied for each audit area. Among other things, the analysis covers the related disclosures, and considers the expertise and experience of the entity's financial reporting personnel. We generally analyze more complex accounting areas in more detail than less complex areas.

What are accounting policies or principles? [ISA | 346.1400]

Accounting policies or principles are standards and guidelines an entity selects and applies when preparing and presenting financial statements in accordance with a financial reporting framework.

For example, when US GAAP is the financial reporting framework, the FASB's Accounting Standards Codification is the authoritative source of accounting principles. US GAAP entities that are SEC registrants also follow SEC rules and interpretive releases.

Many accounting policies or principles set out in financial reporting frameworks are complex or call for considerable judgment. This is because the underlying economics of a business transaction may be complex or difficult to present without applying judgment or providing detailed disclosures.

In some cases, the financial reporting framework allows an entity to select an accounting principle from a number of alternatives. For example, the entity may have alternatives such as first-in-first-out (FIFO) or average cost for measuring its inventory costs. In other cases, the entity has no choice.

What sources of information can help us understand the entity's selection and application of accounting policies or principles? [ISA | 346.1600]

The common sources of information we use to understand the entity and its environment can help us understand the accounting policies or principles the entity has selected and how they are applied. Additional sources that can help us to obtain this understanding include:

- the accounting policies disclosed in the financial statements and, if applicable, management's description of the entity's critical accounting policies and estimates — e.g. information included in an annual report;
- the entity's formal accounting policies and procedures manual;

- authoritative literature from financial reporting standard setters - e.g. FASB Accounting Standards Codification, SEC Staff Accounting Bulletins - and firm publications and interpretations about accounting policies or principles, which can help us understand, for example:
  - whether the standards are complex;
  - whether they require judgment or estimation;
  - what the disclosure requirements are;
  - whether alternative accounting treatments exist;
- resumes and credentials of financial reporting personnel; and
- prior-period work papers, which can help us identify disclosures or accounting policies for which obtaining sufficient appropriate evidence may be difficult.

How do we use this information to understand the entity's selection and application of accounting policies or principles? [ISA | 346.1700]

The common sources of information about the entity and its environment, along with additional sources of information about its accounting framework, policies and practices, can help us understand the entity's selected accounting policies or principles and how they are applied. We begin to obtain our understanding by reading this information, making inquiries and using our knowledge of the financial reporting framework and industry.

In particular, we focus on:

- comparing the entity's accounting policies or principles to those normally used in the industry;
- areas where there is more judgment and complexity in the accounting;
- areas where there are new or revised accounting standards; and
- areas that are ambiguous or not addressed by the entity's financial reporting framework, with attention to information that could help us identify and assess risk.

We then assess those potential risk areas, including those involving complexity, judgment, significant unusual transactions, and changes from the prior period.

How do we evaluate whether the entity has selected and applied the accounting policies or principles appropriately? [ISA | 346.1800]

Once we understand the entity's selection and application of accounting policies or principles, we evaluate their appropriateness. The table below sets out the questions we consider, along with examples of the information we may gather.

Are the accounting policies or principles:	Example
Appropriate for the entity's business?	If the entity chose to depreciate a piece of equipment on a straight-line basis and that method is not a systematic and rational allocation of cost based on the asset's expected usage, we may determine that the related accounting policies or principles are not appropriate for the business.

Consistent with the applicable financial reporting framework?	If the entity uses an accelerated tax depreciation method to depreciate its property, plant and equipment for book purposes, we may determine that the accounting principle selected is not consistent with the entity's applicable financial reporting framework.
Consistent with the accounting policies or principles used in the entity's industry?	If the entity uses the retail method to account for inventory but is not a retailer, we may determine that the accounting principle selected is not consistent with the entity's business and industry.

What other matters do we evaluate while obtaining an understanding of the entity's selection and application of accounting policies or principles? [ISA | 346.1900]

In certain areas, the likelihood of potential misstatements may be increased. Evaluating these areas may help us understand the accounting policies or principles selected and how they are applied. These areas include:

- The entity's financial reporting practices in terms of the applicable financial reporting framework. This may include items such as:
  - Accounting principles and industry-specific practices, including for industry-specific significant classes of transactions, account balances and related disclosures in the financial statements (for example, loans and investments for banks, or research and development for pharmaceuticals).
  - Revenue recognition.
  - Accounting for financial instruments, including related credit losses.
  - Foreign currency assets, liabilities and transactions.
  - Accounting for unusual or complex transactions including those in controversial or emerging areas (for example, accounting for cryptocurrency).
- An understanding of the entity's selection and application of accounting policies, including any changes to those policies as well as the reasons for the changes, 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.

When we determine that any of the above matters are present, we seek more information that may help us understand whether these matters affect the identification and assessment of RMMs. This understanding can be particularly useful when we are assessing the likelihood and potential magnitude of misstatements that could occur.

How do we identify and assess RMMs related to omitted, incomplete or inaccurate disclosures? [ISA | 346.2000]

We obtain an understanding of the entity and the environment which helps us identify and assess RMMs related to omitted, incomplete or inaccurate disclosures.

To support our understanding, we may review prior-period disclosure checklists prepared by the entity (if it exists), as well as our own disclosure checklist.

Also keep in mind that disclosure requirements may change from the prior period because of changes in the entity or the applicable financial reporting framework. Therefore, we also consider any changes in the entity and the environment and those changes necessary to comply with the applicable financial reporting framework in the current period.

Our understanding of the entity can also help us recognize areas where disclosures may be subject to factors that increases the risk of a material misstatement, such as:

- new and/or complex disclosure requirements;
- subjectivity in relation to their preparation;
- whether they may use data that comes from outside of the general ledger and subsidiary ledgers;
- omissions or errors identified in prior periods.

Examples

What information might we gather that helps us understand the selection and application of accounting policies or principles? [ISA | 346.2200]

The table below sets out examples of information we may gather as we obtain our understanding of the entity's selection and application of accounting policies or principles.

Matter	Examples of information we may gather
Significant changes in the entity's accounting policies or principles, financial reporting policies or disclosures, and the reasons for such changes	• The entity may have completed a significant business combination and be applying business combination accounting policies or principles for the first time.
Financial reporting competencies of personnel involved in selecting and applying significant new or complex accounting policies or principles	• Business combinations may be uncommon for the entity, so the entity's accounting personnel may lack experience and expertise in selecting or applying business combination accounting policies or principles and disclosures, or performing necessary internal controls.
Accounts or disclosures requiring judgment in applying significant accounting policies	• The entity may have recognized goodwill and intangible assets, which have complex accounting policies or principles for subsequent measurement.

or principles, especially in determining management's estimates and assumptions	• The entity may have revenue streams with significant variable consideration that is difficult to identify or measure.
Effect of significant accounting policies or principles in controversial or emerging areas lacking authoritative guidance or consensus	• The entity may have adopted a new accounting standard, raising questions about applying the standard for which authoritative guidance or consensus is not yet available.
Methods used to account for significant unusual transactions	• The entity may create a joint venture with an entity controlled by its CEO to conduct business activities that seem designed to keep the entity's liabilities off its balance sheet.
Financial reporting standards and laws and regulations that are new to the entity, including when and how the entity will adopt such requirements	• An entity may have a high number of leases, and a comprehensive new lease accounting standard may require a significant change to the entity's financial statements, processes and internal controls.

1.5 Understand the entity's objectives, strategies and related business risks [ISA | 347]

What do we do?

Obtain an understanding of the entity's objectives, strategies and related business risks.

Why do we do this?

Industry, regulatory and other internal and external factors set the context for the entity's business. In response to these factors, the entity's management or those charged with governance define overall plans, or 'objectives', for the entity. 'Strategies' are the approaches that management plans to take to achieve these objectives. Strategies and objectives may change over time as internal and external forces evolve.

Even with the best intentions and well-reasoned decisions, objectives and strategies may not lead to the expected outcomes, resulting in business risks with financial consequences. Understanding the business risks facing the entity can help us identify risks of material misstatement (RMMs).

Execute the Audit

What sources of information can help us understand the entity's objectives, strategies and related business risks? [ISA | 347.1300]

We may have already obtained information relevant to understanding the entity's objectives, strategies and business risks when we performed other procedures to understand the entity and its environment, including its internal controls.

We can also obtain information to help us understand the entity's objectives, strategies and related business risks by:

- considering the common sources of information that we use to understand the entity and its environment; and
- reviewing the entity's enterprise risk assessment — i.e. its process to assess risks and opportunities related to achieving its objectives.

The risks identified through an enterprise risk assessment and discussed with those charged with governance (often in the form of a heat map) may result in risks of misstatement (RMs).

What are business risks? [ISA | 347.1400]

Business risks are risks that threaten an entity's ability to generate profits or to meet its goals. They generally comprise any factors that may contribute towards business failure — such as loss of customers, increase in production costs, decline in product demand, increase in market competition etc.

Business risks may arise from change or complexity, or from failing to see a need for change. For example, a business risk may arise from:

- developing new products or services that may fail;
- developing a market that may be inadequate to support a product or service;
- developing a flawed product or service that may lead to liabilities and reputational risk;
- new entrant to the market increases competition and lowers margins;
- new technology causes disruption and loss of market share; or
- changes in laws and regulations increase costs of doing business, making some business lines significantly less profitable.

What is the difference between a business risk and an RMM? [ISA | 347.1500]

Business risks can give rise to RMMs — especially financial statement-level RMMs, which may have a more pervasive impact.

However, not all business risks result in RMMs. In fact, some business risks may relate purely to the operations of the business and may not result in misstatement of the financial statements.

Do we obtain an understanding of all the business risks facing the entity? [ISA | 347.1600]

No. We are not responsible for identifying and assessing all business risks because not all business risks give rise to risks of material misstatement.

When we understand the entity's objectives and strategies, we consider whether there are related business risks that may give rise to a risk of material misstatement.

How can business risks affect the financial statements? [ISA | 347.1700]

Business risks can affect financial statements in a variety of ways. Their effects may be immediate or long-term, and impacts may arise at the financial statement level or assertion level. For example:

- the business risk from a shrinking customer base in a consolidating industry may raise an RM for valuations of accounts receivable and inventory that have become obsolete (immediate assertion-level RM); or
- the business risk of a decline in the entity's industry may affect the entity's ability to continue as a going concern (long-term financial statement-level RM)

Examples

In what situations might business risks lead to RMMs? [ISA | 347.1800]

The table below sets out examples of matters we may consider when obtaining an understanding of the entity's objectives, strategies and related business risks that may result in RMMs.

Situation	Examples of related business risk
Industry developments	The entity does not have the personnel or expertise to deal with a change in the industry.
New products and services	A newly introduced product or service may expose the entity to liability, and/or the new product or service may not succeed.
Changes in supply chain	Changes in the supply chain may impact the profitability of the entity's products. Disruptions in the supply chain may impact the entity's ability to fulfill customer orders.
Use of information technology (IT)	Some of the entity's systems and processes may be incompatible. New IT systems may not be implemented properly and/or migrated data may not be complete and accurate. There may be inconsistencies between the entity's IT strategy and its business strategies.
New accounting requirements	A new accounting requirement may not be implemented properly or completely, or the requirement may increase costs.
Expansion of the business	The demand for the entity's products or services may not have been accurately estimated.

Effects of implementing a strategy, particularly effects that lead to new accounting requirements	The strategy may not be implemented properly or completely.
Current and prospective financing requirements	The entity's inability to meet financing requirements may lead to a loss of financing.
Regulatory requirements	Regulatory requirements may increase the entity's legal exposure.

1.6 Understand the entity's measurement and analysis of its financial performance [ISA | 348]

What do we do?

Obtain an understanding of the entity's measurement and analysis of its financial performance.

Why do we do this?

Management and external stakeholders measure and review what they consider important. Performance measures, whether external or internal, create pressures for the entity. In turn, these pressures may prompt management action to improve business performance or misstate the financial statements.

Gathering information about how the entity, analysts, investors and rating agencies measure and analyze the entity's financial performance helps us understand financial statement line items that may pose greater risk of material misstatement. This understanding may help us identify accounts that may be open to manipulation, as well as accounts that the entity uses to monitors its operations.

Execute the Audit

How do we understand how the entity measures and analyzes its financial performance? [ISA | 348.1300]

We first identify the performance measures the entity considers most relevant and the measures the entity or external parties actively track.

We may have already identified some performance measures when understanding:

- the relevant factors and metrics used to establish materiality for the financial statements; and
- the nature of the entity.

Considering the common sources of information that we use to understand the entity and its environment may also reveal performance measures we have not already identified, or help us better understand how using performance measures we have identified may affect the identification and assessment of risks of material misstatement (RMMs).

In essence, we are searching the information produced by the entity, analysts, investors, rating agencies and others to identify the specific financial and other metrics they focus on in their reports.

Lastly, inquiries of management may reveal that it relies on certain key indicators, whether publicly available or not, for evaluating financial performance and taking action.

How can we use our understanding to identify and assess risks? [ISA | 348.1400]

Once we've identified the relevant performance measures, we may further seek to understand the following factors for each identified relevant performance measure:

- How aggressively are targets for each performance measure set by management?
- Does the entity have a history of achieving the set targets?
- How significantly is the management compensation linked to each performance measure?
- How are the performance measures defined?

The first three factors can help us gauge the importance of each performance measure to the entity and management, which may influence our assessment of risks of material misstatement connected to these performance measures.

Performance measures may also help us identify risks of misstatement. For example, understanding certain performance measures may indicate that the entity has unusually rapid growth or profitability when compared to that of other entities in the same industry. Such information, particularly if combined with other factors such as performance-based bonus or incentive remuneration, may indicate a potential risk of management bias in the preparation of the financial statements or possible fraud risk.

The last factor on understanding how the performance measure is defined, helps us identify specific accounts or disclosures that may create a greater risk of material misstatement from error or fraud. For example, when the entity and its investors and analysts use adjusted EBITDA as a relevant performance measure, we may obtain an understanding of how adjusted EBITDA is calculated and which accounts are included in the calculation.

Inspecting information about the entity's performance measures may also help us to identify items to focus on in our analytical reviews. We may identify unexpected results or trends that could indicate greater risk of material misstatement from error or fraud. For example, revenue growth that is unusually rapid compared to other entities in the same industry may indicate a potential risk of management bias in financial statement preparation — particularly when combined with other factors, such as performance-based bonus or incentive remuneration.

Can an entity's performance measures include non-GAAP measures? [ISA | 348.1500]

Yes. An entity's performance measures may and often do include both GAAP and non-GAAP measures. Commonly used non-GAAP performance measures include EBITDA and adjusted EBITDA, as well as net income, cash flow from operations, and other key financial ratios.

How may our procedures to understand the entity's performance measures differ depending on its size or complexity? [ISA | 348.7475]

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

For some less complex entities, it may only be the terms of the entity's bank borrowings (i.e., bank covenants) that are linked to specific performance measures related to the entity's performance or financial position (e.g., a maximum working capital amount).

Whereas, for some entities whose nature and circumstances are more complex, such as those operating in the insurance or banking industries, performance or financial position may also be measured against regulatory requirements (e.g., regulatory ratio requirements such as capital adequacy and liquidity ratios performance hurdles).

Our understanding of these performance measures may help identify areas where there is increased susceptibility to the risk of material misstatement.

Examples

What performance measures might an entity use? [ISA | 348.1600]

The table below sets out examples of performance measures an entity may use that may be relevant to our risk assessment.

Where and how performance measures may be used	Examples of performance measures
As the basis for contractual commitments or incentive compensation arrangements	• Financial measures - e.g. revenue, net income, EBITDA • Period-on-period financial performance analyses • Industry-specific financial measures - e.g. Funds from Operations for real estate investment trusts, same-store sales for retailers • Non-financial measures - e.g. number of subscribers or users • Common ratios in loan agreements - e.g. debt-to-equity, interest coverage • Growth rates in financial and non-financial measures
By external parties - e.g. analysts, rating agencies - to review the entity's performance	
By the entity, to monitor its operations that may also highlight unexpected results and trends that management investigates and corrects, including correction of misstatements	• Ratios — e.g. accounts receivable and inventory turnover • Specific categories of operating expenses • Comparisons to budgets or forecasts • Segment or divisional operating results • Comparisons to competitors' operating results

	• Employee performance measures and incentive compensation policies

1.7 Evaluate whether significant changes in the entity from prior periods affect RMMs [ISA | 349]

What do we do?

Evaluate whether significant changes in the entity from prior periods affect the risks of material misstatement.

Why do we do this?

Changes in the entity from period to period may create new risks or modify risks we identified and assessed in the prior period. Evaluating these changes can reveal information that assists us to identify and assess risks of material misstatement (RMMs).

For example, a retailer could decide to launch a new product line in the current period and purchase a significant amount of inventory in advance. The retailer's limited experience with the product may have led it to inadequately project demand or pricing for the new product, creating RMMs related to the inventory's value. Not identifying the change may prevent us from identifying the risk or properly assessing whether the level of risk has changed since prior periods.

Execute the Audit

How do we identify significant changes in the entity from prior periods? [ISA | 349.1300]

We inquire of management if there have been, or whether they expect, any significant changes in the entity's business or environment, including internal control from the prior period. We may also identify significant changes from other risk assessment procedures.

In doing this, we are not looking for every change in the entity but are focusing on those changes that may impact our risk identification and assessment.

The entity's risk assessment process (Risk Assessment component of CERAMIC) may be one of the ways the entity monitors and assesses changes.

Understanding this component can help us identify changes from prior periods that may affect our identification and assessment of the risks of material misstatement.

1.8 Assess likelihood and magnitude of potential misstatements to determine RMMs [ISA | 565]

What do we do?

Assess the likelihood and magnitude of potential misstatements, including the possibility of multiple misstatements, to determine RMMs and inherent risk

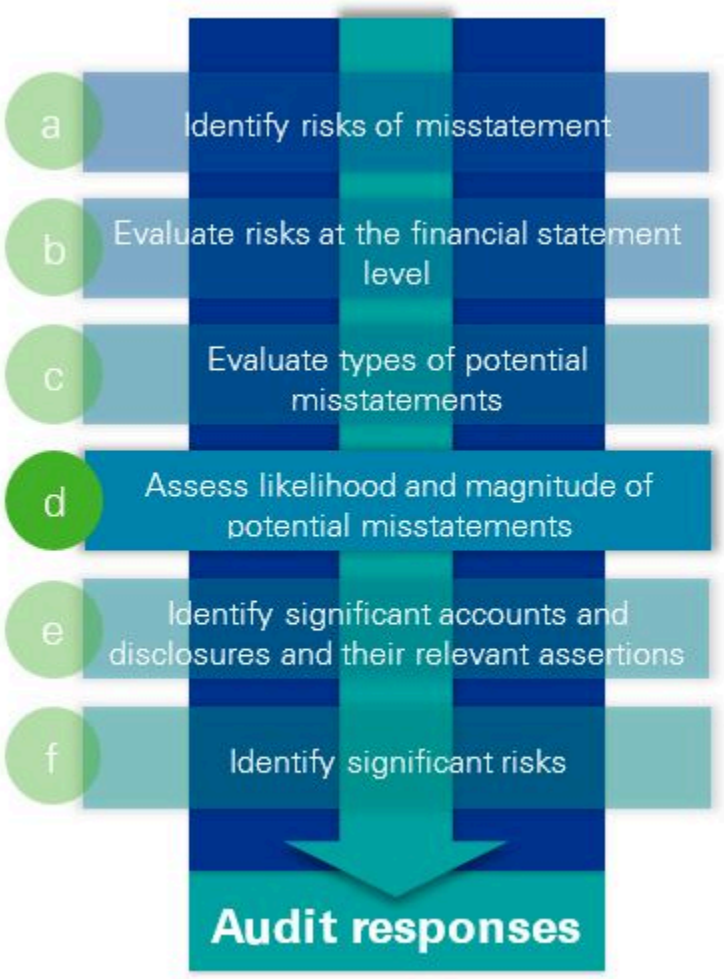
Why do we do this?

We assess the likelihood and magnitude of potential misstatements to:

- Identify risks of material misstatements (RMMs);
- Determine where on the continuum of inherent risk the RMM sits (which informs our design of further audit procedures to respond to the RMM); and
- Assist in the determination of significant risks.

Execute the Audit

Where are we in our risk assessment? [ISA | 565.1300]



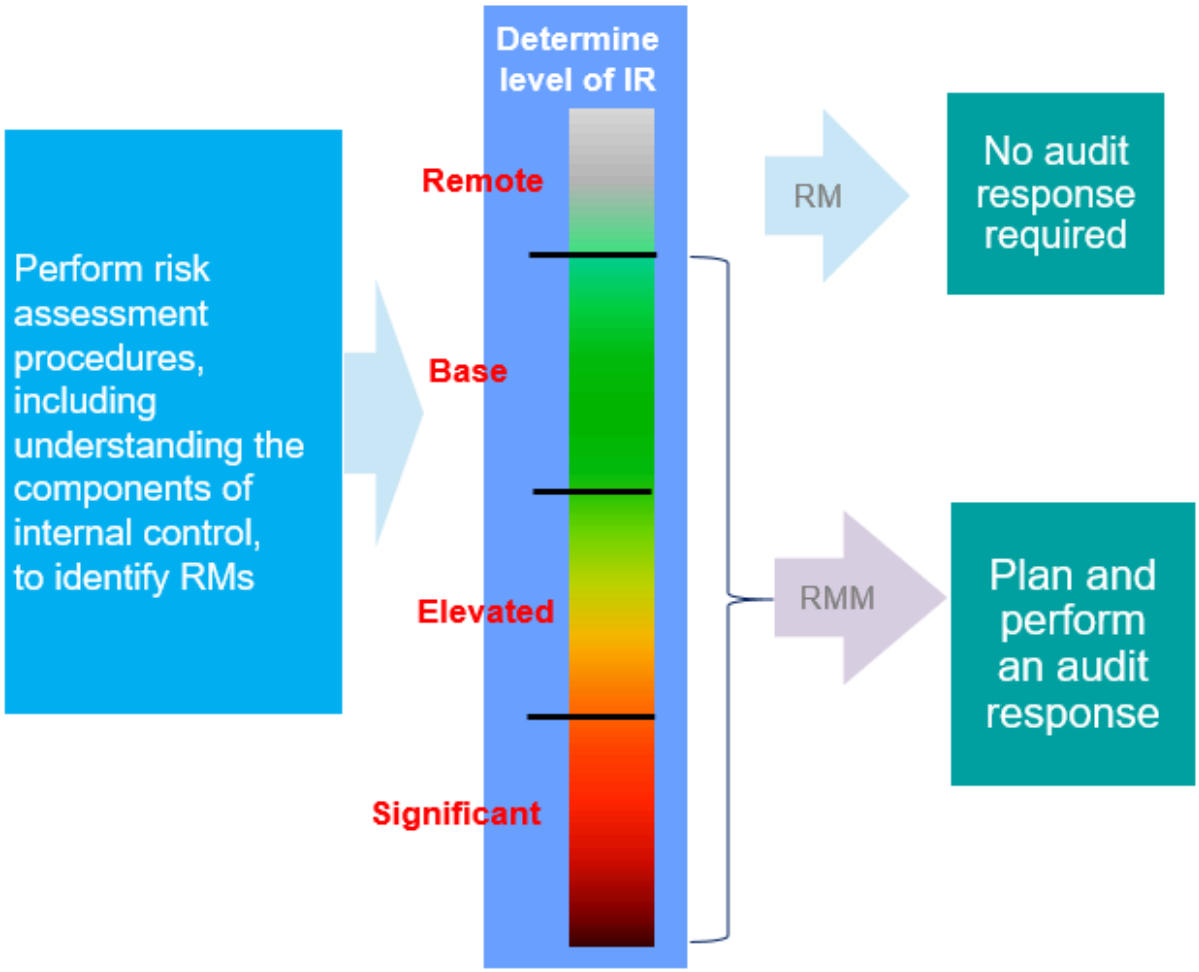
How does assessing likelihood and magnitude of potential misstatements help us determine RMMs and level of inherent risk? [ISA | 565.8701]

Assessing the likelihood and magnitude of potential misstatements helps us gauge where we are on the inherent risk continuum and whether we've reached the level where inherent risk is more than

remote for that risk. An RM is simply a risk on the "remote" part of the inherent risk continuum, where no audit response is necessary*.

When the likelihood and magnitude of potential misstatement is more than remote, we assess inherent risk for each RMM at one of three levels - Base, Elevated or Significant, depending on where it is on the continuum (significant risks are closer to the upper end of the continuum).

The following diagram illustrates the inherent risk continuum and how we think about RMs, RMMs and our inherent risk assessment in relation to that continuum:



Not assessing a risk as an RMM has ramifications — it means we don't address it further in our audit*.

* There are certain areas within the financial reporting process where procedures are always performed even if there is no RMM (e.g. disclosures: agree/reconcile information in the disclosure to the underlying accounting records).

How do internal controls affect our assessment of likelihood and magnitude? [ISA | 565.1700]

We don't consider the effects of control activities when we determine which risks are RMMs.

Our understanding of CERAMIC, however, can influence our assessment of inherent risk. When there are deficiencies in CERAMIC, it may highlight an increased chance of material misstatements occurring. For example, when we identify deficiencies related to the entity's ability to attract, develop, and retain competent individuals, there is a higher likelihood of misstatements occurring

broadly because unqualified or lower competence individuals are more prone to record transactions incorrectly.

How do we assess likelihood and magnitude? [ISA | 565.8704]

The table below sets out examples of how an engagement team might assess likelihood and magnitude when they determine RMMs and level of inherent risk.

Description of RM and related accounts / disclosures and assertions	Considerations related to likelihood and magnitude of potential misstatement	Assessment of RMM and level of inherent risk
Prepayments are not accurately recorded or do not exist. (Existence of prepaid expenses)	• The size of the prepaid expenses account is less than two times performance materiality and has not changed significantly from the prior year, which is consistent with our expectations. • The account comprises a small number of routine prepayments to vendors for materials that the entity expects to consume within 12 months. • The individual balances are homogeneous and not subject to accounting complexities. • There is no risk of aggregation with other non-significant accounts.	Although the engagement team has identified an RM, they assess that the likelihood and magnitude that a material misstatement may occur is remote given the low number and dollar value of transactions and lack of accounting complexity associated with the risk. The engagement team assess the risk as not an RMM.
Indicators that an asset or cash-generating unit may be impaired are not appropriately identified. (Valuation of PP&E)	• The size of the PP&E account is relatively large (40 times performance materiality) and has not changed significantly from the prior year. • All of the PP&E is included within a single long-lived asset group.	Given the more favorable economic conditions and reduced complexity (e.g. not having a significant number of different asset groups), there is a *lower* likelihood of a material misstatement occurring. However, given the magnitude of the balance of PP&E and

	• The information identified from our inquiries of management indicated no changes in the use of the PP&E. • The favorable interim results of operations reviewed in our planning analytical procedures indicate a reduced risk of exposure to losses in this account. • Asset values have fluctuated in the past and there have been impairments taken in the last three years.	susceptibility in recent periods to changes in value, the engagement team concludes that there is still *more than a remote* chance of a material misstatement occurring. The engagement team assesses the risk to be an RMM and inherent risk is assessed to be Base.
An inappropriate amount is estimated and recorded for the value of rights of return. Additional risk description: Risk relates to products sold through a new distribution channel. (Existence and Accuracy of revenue and accounts receivable)	• Based on our risk assessment procedures, we identified that the entity planned to begin selling a new product to resellers in the last quarter of the fiscal year. • Previously, the entity had only sold its products directly to end users and these new contracts include unique rights of return. • The entity has relatively little experience with product returns and limited data related to these new sales arrangements. • Although the product is new, the entity expects its sales volumes to represent approximately 10% of revenue for the year.	Given the complexity and judgment in determining the estimate for returns, there is an increased chance that a misstatement could occur. Considering the increased likelihood along with the fact that the revenue from the new product is a substantial portion of total revenues, resulting in magnitude of potential misstatement being material, the engagement team concludes that there is more than a remote chance of a material misstatement occurring. The engagement team assesses the risk to be an RMM and considering the degree of complexity in the measurement of the estimate for returns, and the wide range of measurement uncertainty, the inherent risk assessment is Significant.
The disclosure is incomplete,	• The entity is manufacturer with point-of-sale revenue recognition.	Given there is no judgment or complexity in the policies, and no changes nor expected changes

inaccurate, or not fairly presented. Additional risk description: Risk related to the required disclosures of revenue accounting policies	• Revenue is material to the financial statements and important to its users. • There have not been new accounting pronouncements or changes in the entity's accounting policies for revenue in the past two years.	in the revenue accounting policies disclosures, the engagement team assesses the risk to be an RM.
The disclosure is incomplete, inaccurate, or not fairly presented. Additional risk description: Risk relates to the required disclosure of disaggregated revenue amounts. (Presentation of revenue)	• Revenue is material to the financial statements and important to users of the financial statements. • The entity completed an acquisition in the current reporting period, adding a new business line in a geographic region in which the entity has not previously operated.	Given the magnitude of the balance of revenue and changes in the disclosure from the prior period given the entity's acquisition, the engagement team assesses the risk to be an RMM. As disaggregating revenue amounts does not require judgment, inherent risk is assessed to be Base.

Group Audit | How do we assess RMMs of the group financial statements? [ISA | 565.2200]

As the group auditor, we assess the risks of material misstatement of the group financial statements, whether due to fraud or error, including with respect to the consolidation process by applying the same guidance for assessing RMMs in a stand-alone audit. However, since most assertion-level RMMs of the group financial statements, or group RMMs, will arise in components, we, as the group auditor, will often involve component auditors in risk assessment procedures to assess group RMMs.

Group Audit | Who is responsible for assessing the RMMs of the group financial statements? [ISA | 565.160255]

The lead group auditor takes responsibility for assessing the RMMs of the group financial statements in a group audit.

Group Audit | What does 'take responsibility for' mean? [ISA | 565.160253]

'Take responsibility for' means the lead group auditor may either design and/or perform procedures, tasks, or actions themselves or are permitted to assign the design and/or performance of procedures, tasks or actions to other appropriately skilled or suitably experienced members of the engagement team, including component auditors.

Assigning the design and/or performance of procedures to another member of the engagement team, however, does not relieve the lead group auditor of their responsibility for the overall design and performance of the audit

Group Audit | Do we assess different RMMs in a group audit? [ISA | 565.11097]

Yes. As the group auditor, we also assess RMMs related to the consolidation process, including sub-consolidations, which are not linked to any specific significant accounts or disclosures. However, we respond to consolidation RMMs similar to assertion-level RMMs (i.e., design substantive procedures and when applicable, identify PRPs and relevant control activities) rather than designing overall responses like we do for financial statement-level RMMs.

Group Audit | Why may RMMs of the group financial statements be assessed differently at components? [ISA | 565.160257]

Examples of when an RMM at the component may be assessed differently than the RMMs of the group financial statements include:

- the component auditor assesses the magnitude of potential misstatements associated with an RMM considering the component performance materiality for the component; however, the potential misstatement to the group financial statements is not considered material or at a magnitude that warrants the same assessment as that at the component; or
- RMMs at the component are identified based on an RMMs that relates to local financial reporting framework which are not RMMs under the financial reporting framework used by the group.

In circumstances where a component auditor has assessed an RMM as either Elevated or Significant that we as the group auditor have not assessed at the same inherent risk level, we document why we consider those RMMs not to be at the same inherent risk level.

> For example, suppose that the group auditor has assessed RMMs associated with capitalized software costs as Base because the magnitude to the group financial statements is 2x group performance materiality.
>
> However, a component auditor has assessed RMMs associated with capitalized software costs as Elevated due to the magnitude at the component and the judgment involved in determining the amounts to capitalize. The component auditor communicates this assessment to the group auditor.
>
> The group auditor documents why the RMM is not assessed as Elevated for the group financial statements.

How do we determine whether our assessment of inherent risk for an RMM is Base, Elevated or Significant? [ISA | 565.8705]

In addition to our consideration of inherent risk factors (see question 'What are the inherent risk factors?'), it may be helpful to:

- first determine which risks are closer to the upper end of the inherent risk continuum and are significant risks (see activity 'Determine significant risks'); and
- then assess the remaining risks by evaluating whether they are relatively lower or higher on the inherent risk continuum — i.e. Base or Elevated.

When we are trying to determine whether a risk is Base or Elevated, it may be useful to compare our assessments across non-significant risks.

> For example, suppose that:

- the engagement team have assessed risks associated with several smaller and less complex accounts — e.g. prepaid expenses — as Base; and
- they are trying to determine whether a risk associated with a higher-volume, more complex account is Base or Elevated.

The team may find it helpful to consider whether they really believe the lowest level of inherent risk — i.e. Base — makes sense for both types of risks.

Questioning this can help us better determine where the RMM falls on the continuum.

What factors do we consider in assessing likelihood and magnitude and level of inherent risk? [ISA | 565.2000]

We consider:

- Inherent risk factors;
- Significant risk factors (see question 'How do we determine whether any of the identified and assessed RMM are significant risks?'); and
- Estimates risk factors, if applicable (see question 'What are the additional risk factors that we evaluate when identifying significant accounts and disclosures involving accounting estimates?').

We consider each factor for each RM, to gauge whether it is an RMM, and if so where it sits on the inherent risk continuum. When considering these factors, a key consideration is the degree to which the inherent risk factors affect the combination of likelihood of misstatement occurring and magnitude of misstatement. The higher the combination of likelihood and magnitude, the higher the assessment of inherent risk; the lower the combination of likelihood and magnitude, the lower the assessment of inherent risk.

What are the inherent risk factors? [ISA | 565.8706]

The following table describes the inherent risk factors:

Inherent risk factors	**Additional description and examples**
Factors that affect the susceptibility to misstatement of an assertion about a class of transactions, account balance or disclosure	
Quantitative or qualitative significance, including: • Size and composition of the account • Nature of the account or disclosure • Existence of related party transactions in the account • Possibility of significant contingent liabilities arising	***Size and composition:*** As the size of an account increases, so does the potential magnitude of a misstatement in that account or disclosure. Often, this is because in larger account balances, errors that represent a small percentage of the account balance may still exceed materiality. For example, a 2% misstatement in an account that is 60 times materiality exceeds materiality. Understanding the composition of an account helps us evaluate the other factors and determine whether relevant assertions exist for a particular account and whether there is an RMM we haven't yet identified and assessed.

from the activities reflected in the account or disclosure
- Exposure to losses in the account

For example, if an entity has domestic sales and international sales, the risk for each type may be different. If there are uncertainties about a foreign countries' economic stability, there may be greater risk in their international operations than their domestic operations.

Nature of accounts and disclosures: When we consider the nature, we think about numerous characteristics of an account, disclosure or assertion, including:

- its importance or prominence in the financial statements
- the way it is recorded or presented
- the basic types of transactions that affect it.

These factors, along with others, can affect how likely a material misstatement is to occur for a specific assertion.

For example:

- accrual balances, by their nature, often have more risk of understatement than overstatement
- assertions related to accounting estimates are more likely to contain a material misstatement related to the valuation assertion
- assertion disclosures related to revenue or significant judgments in applying the related revenue accounting policies or principles are important or prominent in the financial statements
- an accounting estimate often involves management making significant judgments about the assumptions to use. These judgments can involve uncertainty, and introduce more potential for human error.

Existence of related party transactions: Related party transactions involve close relationships between parties, so there is more chance that they might involve fraud or be inappropriate, and lack a clear business purpose and not be appropriately disclosed.

These issues may arise because the entity doesn't account for the transaction properly, or because the substance of a related party transaction might be different from its form.

For example, an entity may structure a related party transaction solely to avoid recording and disclosing a liability in the financial statements. The risk to the financial statements

	increases because the entity and its related parties control both sides of the transaction. Given this risk, a material misstatement is more likely in an account that includes related party transactions. ***Possibility of significant contingent liabilities:*** The nature of an entity's transactions and business activities could lead to significant contingencies. For example, selling goods could lead to sales returns or warranty claims on defective products. Or certain fixed assets may exist (such as underground storage tanks containing gasoline) that could lead to asset retirement obligations or environmental liabilities. Contingent liabilities may be difficult to identify, and judgment may be involved to determine the amount to be recorded or disclosed in the financial statements. Therefore, they may be more likely to contain a material misstatement. ***Exposure to losses in the account:*** The more exposure an account has to losses, the more chance it may contain an error. Factors in the entity's general environment may expose a particular account to losses. We also think about accounts that may have lower recorded balances but a higher exposure to losses. For example, an entity may record a small legal accrual, but face several lawsuits with potential unfavorable outcomes that expose it to significant losses. This potential for loss may increase the likelihood of material misstatement over the completeness, valuation and presentation assertions for the legal accrual.
Volume of activity, complexity and homogeneity of the individual transactions processed through the account or reflected in the disclosure	***Volume*** **:** The more transactions processed through a class of transactions, account balance or reflected in a disclosure, the greater the chance that it contains a material misstatement. There is more risk that multiple items could be misstated that could aggregate to a material misstatement. We consider the volume of transactions in all accounts and disclosures, but we don't dismiss those with smaller balances without carefully considering the volume of transactions.

	For example, a cash account may have a zero balance at the period end, but the entity may process a high volume of cash transactions through it during the period. This may be an account with a reasonable possibility of a material misstatement. ***Complexity:*** More complex transactions can suggest more judgment or present a greater opportunity for errors. For example, transactions that result from complex calculations often have multiple inputs, each of which may present a possibility for error. Simple calculations with fewer inputs may have a lower chance of error. More complex calculations increase the likelihood of material misstatements related to particular assertions — e.g. valuation — of a particular account or disclosure. ***Homogeneity:*** In certain cases, when transactions are homogeneous, misstatements in one transaction may indicate additional misstatements in others. As such, multiple errors could occur, which could increase the magnitude of any potential misstatement. In this case, the homogeneity may increase the possibility of a material misstatement. Conversely, when transactions lack uniformity in the composition of the items processed in the account or class of transactions may increase susceptibility to misstatement in the related account or disclosure.
Susceptibility to misstatement due to error	Some accounts, disclosures and assertions, by their nature, are more susceptible to misstatement - including those more likely to be affected by human error. This may be due to the types of transactions processed in an account, the nature of the account or disclosure itself, or many other factors. This higher susceptibility to misstatements increases the likelihood that a material misstatement will occur. For example, when substantial doubt about an entity's ability to continue as a going concern is raised but is alleviated by management's plans, the disclosures could be more susceptible to misstatement whether due to error or fraud.

Factors relating to preparation of the information required by the financial reporting framework	
Complexity, including accounting and reporting complexities associated with the account or disclosure	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. As another example, complexity may arise in developing disclosures for a business combination because several individuals from different departments may be involved and different sources of information from multiple IT systems may be necessary in preparing the disclosures. Complex accounting and reporting can often: • be more challenging for an entity to evaluate; • involve a greater degree of judgment; and • necessitate a greater degree of skill, knowledge and experience. For example, accounting for income taxes can be complex, especially when an entity operates in multiple jurisdictions. Such complexities can make errors or incorrect judgments more prevalent, and increase the likelihood of material misstatement. Complexity may arise from changes in the applicable financial reporting framework that create new disclosure requirements, or changes in the entity's transactions and activities that result in new accounting policies or principles.
Subjectivity (including judgment in the recognition or measurement of financial information related to the risk)	Subjectivity arises from inherent limitations in the ability to prepare necessary information in an objective manner, due to limitations in the availability of knowledge or information, such that management may need to make an election or subjective judgment about the appropriate approach to take and about the resulting information to include in the financial statements.

	Because of different approaches to preparing the required information, different outcomes could result from appropriately applying the requirements of the applicable financial reporting framework. As limitations in knowledge or data increase, the subjectivity in the judgments that could be made by reasonably knowledgeable and independent individuals, and the diversity in possible outcomes of those judgments, will also increase. For example, management's selection of a valuation technique or model for a non-current asset, such as investment properties. Additionally, subjectivity can arise for disclosures that are subjective in relation to their preparation. For example, disclosures related to a lawsuit and related loss contingency could be more susceptible to misstatement given their subjective nature.
Change(s), including changes from the prior period in account/ disclosure characteristics Risk relates to recent significant economic, accounting or other developments	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 principles or how accounting estimates are made or related disclosures are determined. As another example, rising interest rates may affect management's projected financial information utilized in the valuation of goodwill, including an impact on the discount rates used and projected revenue and expenses. This change in business environment may also have an impact on management's disclosures of judgments applied in performing the annual impairment test.

	Changes from the prior period may indicate that the risks have changed or that entity has entered into new types of transactions with a different risk profile. The more significant the change, the greater the likelihood that a material misstatement could occur. For example, an entity may change its mix of investment securities from government treasury securities to private hedge funds - i.e. from Level 1 investments to Level 3 investments. This change involves a new and potentially more complex valuation model. It may increase the likelihood of a material misstatement related to the valuation and presentation assertions.
Uncertainty	Uncertainty arises when the required information cannot be prepared based only on sufficiently precise and comprehensive data that is verifiable through direct observation (e.g. pending litigation). In these circumstances, an approach may need to be taken that applies the available knowledge to prepare the information using sufficiently precise and comprehensive observable data, to the extent available, and reasonable assumptions supported by the most appropriate available data, when it is not. Constraints on the availability of knowledge or data, which are not within the control of management (subject to cost constraints where applicable) are sources of uncertainty and their effect on the preparation of the necessary information cannot be eliminated. For example, estimation uncertainty arises when the required monetary amount cannot be determined with precision and the outcome of the estimate is not known before the date the financial statements are finalized.
Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk (including significant unusual transactions)	Results from conditions that create susceptibility to intentional or unintentional failure by management to maintain neutrality in preparing the information. For example:

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

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.

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.

See activity 'Identify fraud risk factors' for additional considerations when considering other fraud risk factors.

We perform risk assessment procedures to obtain an understanding of how these inherent risk factors affect susceptibility of assertions to misstatement and the degree to which they do so, in the preparation of the financial statements in accordance with the applicable financial reporting framework.

It is not expected that an inherent risk factor is selected in the applicable workflow just because it is "relevant", if it does not impact where the risk sits on the inherent risk continuum. For example, where the RM is associated with the transaction (e.g. PPE additions) we would select volume of activity and homogeneity of the transaction, rather than the size and composition of the account as volume of activity and homogeneity factors impact where the risk sits on the inherent risk continuum.

Will all inherent risk factors be relevant? [ISA | 565.11100]

No. Depending on the specific risk we are assessing, some inherent risk factors may not be relevant or are not impactful to our assessment.

For example, when there are no related party transactions that are associated with a particular risk, that factor is not relevant or important in our assessment.

We focus on the factors that are most relevant to our assessment of whether the risk rises to an RMM and the related level of inherent risk. We also think about the relative significance of each inherent risk factor during our evaluation.

Does the number of relevant factors impact the level of inherent risk? [ISA | 565.11102]

No. There is not a specific number of factors that are present before something moves from one inherent risk level to another (e.g. base to elevated), because the factors are considered on a continuum and not in a binary manner.

It is often helpful to take a step back and compare the risks aggregated at an account level against other risks from other accounts.

For example, suppose that:

- We have assessed the risks associated with several smaller and less complex accounts, e.g., prepaid expenses, as Base.
- We are trying to determine whether a risk associated with a higher-volume, more complex account is Base or Elevated.

It may be helpful to think about whether the lowest level of inherent risk, (i.e., Base), makes sense for both types of risks.

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

What if the risk is on the threshold between two levels of inherent risk? [ISA | 565.11103]

If, we assess a risk as being on the threshold between two levels of inherent risk — e.g. Base/Elevated or Elevated/Significant — it may be appropriate to 'round up', or pick the higher risk level, documenting our rationale for the decision as part of our assessment of likelihood and magnitude.

Remember: assessing a risk as too low may result in an insufficient audit response and an unacceptable increase in audit risk.

What if an RMM includes multiple portions of an account balance with varying levels of inherent risk? [ISA | 565.11104]

If this is the case, we may have defined the RMM too broadly. In this situation, it may be appropriate to disaggregate the RMM into separate components that have varying levels of inherent risk and associate a disaggregated RM/RMM to each component. This may mean we create a duplicate RM/RMM. Adding an additional risk description can clarify how the disaggregated RMMs apply to each component.

We then perform our assessment of likelihood and magnitude of potential misstatements for each of the disaggregated RMs we identified. In performing this assessment, we may determine that one or more of the RMs does not rise to the level of an RMM. This concept applies for both accounts and disclosures.

For example, we identify the following RMM: An inappropriate amount is estimated for the net realizable value (NRV) of inventory, or an inaccurate amount is recorded for the lower of cost and NRV.

Raw materials inventory comprises multiple types of raw materials that are subject to different levels of inherent risk - including steel.

If steel prices are volatile, that may increase the risk of steel-based inventory being overvalued.

We assess inherent risk differently for the steel-based raw materials than for the remaining raw materials inventory.

As a result, we break down the risk into two separate risks - one relating to the steel-based raw materials, and the other relating to the remaining raw materials.

This disaggregation leads us to identify and assess one RMM as Significant (the risk relating to steel-based raw materials) and another as Elevated (the risk relating to the remaining raw materials) based on the relevant inherent risk factors.

As another example, we may disaggregate an RM related to the existence of cash and cash equivalent balances between different cash and cash equivalents accounts because management may use them in varying ways in different locations for different purposes (e.g. payroll, accounts payable and expense disbursement, treasury function for interest and dividend receipts, or revenue receipts) and therefore the related inherent risks may vary based on account/ location/component because of differing risk profiles.

What do we do if we have identified the same RMM due to error and due to fraud? [ISA | 565.8702]

If we have identified the same RMM due to error and due to fraud, then we create 2 separate RMMs within the KPMG Clara workflow, and assess them separately. A fraud risk is always a significant risk, but a risk due to error may have a different inherent risk assessment.

We perform procedures to respond to the fraud risk and demonstrate our special audit consideration in response to the related significant risk. These procedures/responses may differ to our response to the RMM due to error (particularly if our CAR assessment is different). By identifying and assessing these RMMs separately, we can appropriately tailor our response to obtain sufficient appropriate audit evidence for both.

How do we consider whether there is an RMM in aggregate? [ISA | 565.2100]

We assess for each business process and across all business processes if there are any indications that there is an RMM in aggregate within those assertions, transactions, account balances and disclosures that do not have any RMM associated with them. Signs that might indicate that there are reasonable possibilities of RMM in the aggregate include the following:

- identifying multiple risks that relate to the same accounts/disclosures and assertions;
- determining that the combined magnitude of potential misstatements related to the remaining risks is material; or
- identifying multiple risks with similar characteristics, which may indicate several potential misstatements that could aggregate to a material misstatement.

We assess risks in the aggregate in a manner similar to our risk assessment over each risk on an individual basis. That is, when performing this aggregation assessment, we consider the same inherent risk factors (see question 'What factors do we consider in assessing likelihood and magnitude and level of inherent risk?').

When assessing risks in the aggregate across all business processes, we step back and focus on those accounts and disclosures that were not identified as significant and the assertions were not

identified as relevant (see question 'How do we identify significant accounts and disclosures and their relevant assertions?').

What do we do when we have determined that RMs identified represent an RMM when assessed in the aggregate? [ISA | 565.11107]

When we have identified that RMs aggregate to one or more RMMs, we

- change the assessment of RMs to RMMs until the remaining RMs do not aggregate to an RMM, or
- add a custom RMM that identifies the aggregate risk.

Is there anything we additionally consider when accounting estimates are involved? [ISA | 565.11116]

Yes. We perform the risk assessment procedures related to accounting estimates in the KAEG chapter on estimates (ISA 540, AU-C 540 or AS 2501). We perform certain risk assessment procedures in order to identify and assess RMMs related to accounting estimates, as outlined in 'Perform risk assessment procedures related to accounting estimates'.

Is there anything additional we consider when the financial reporting process is involved? [ISA | 565.6463]

Yes. 'Risk considerations' are used when available, within the financial reporting process screens in KPMG Clara workflow - i.e. financial statements, cash flows, segment information, disclosures - and may assist us in:

- identifying the risks of misstatement (RMs);
- determining whether the RMs are risks of material misstatement (RMMs); and/or
- designing appropriate audit responses for those assessed as RMMs.

How do the 'risk considerations' assist us in determining whether the RMs are RMMs? [ISA | 565.6469]

The 'risk considerations' let us see more clearly the individual items that contribute to the corresponding RMs within the financial reporting process, individually or in combination.

As a result, we can appropriately assess the inherent risk for the RMs, by assessing the likelihood and magnitude of potential misstatements and other relevant factors.

We assess inherent risk at the RM level, not at the risk consideration level.

How do the 'risk considerations' assist us in designing appropriate audit responses? [ISA | 565.6470]

For each RM we assess as an RMM, we design appropriate audit responses taking into account the more detailed information provided by the 'risk considerations'.

Our response is at the RMM level, not the risk consideration level.

What do we do with financial statement-level RMs? [ISA | 565.6468]

As with other risks, we assess financial statement-level RMs and determine whether there is a possibility of a material misstatement to the financial statements by considering the likelihood and magnitude of potential misstatements.

When determining whether a financial statement-level RM is an RMM, we also consider whether it affects the assessment of RMMs at the assertion level.

If the financial statement-level RM is an RMM, it affects how we conduct our audit broadly and we design and implement overall responses. See activity 'Design and implement overall responses' for information about overall responses.

What key success factors might help us in our inherent risk assessment? [ISA | 565.11119]

The table below sets out examples of key success factors that can help us when assessing inherent risk.

Key success factor	How it may help
Timely partner and manager involvement	An effective inherent risk assessment relies on the judgments of the engagement team's most senior members at a sufficiently detailed level early in the audit - especially for risks on the thresholds between Base and Elevated, and Elevated and Significant.
Not being anchored in prior-period inherent risk assessments	We use the information obtained through our risk assessment process to form up-to-date inherent risk assessments based on the current period's factors. Prior-period knowledge is helpful, but we combine it with everything we learn during planning and risk assessment in the current period.
Thinking about inherent risk as a continuum	The inherent risk continuum includes varying levels of risk. Thinking about where each RMM falls on that continuum can help us identify whether an account/disclosure contains components, or groups of transactions, with varying degrees of risk that are subject to different processes and controls. This can help us better identify significant accounts or disclosures.
Paying attention to what's documented in our audit file	Fully capturing how we considered the factors in our inherent risk assessment has several benefits: Our inherent risk assessments involve judgment, and so may warrant more

	persuasive audit evidence and robust documentation. Documenting the basis for our conclusions demonstrates how we applied professional skepticism. The process of documenting our rationale may lead us to rethink our initial conclusion and revisit that assessment when it is not appropriate.
Leveraging management's risk assessment process	Reconciling our inherent risk assessments with management's risk assessments can help us evaluate the effectiveness of management's internal control over financial reporting — i.e. the Risk Assessment component.
Holding risk assessment meetings at the right times	We may hold meetings to discuss risk assessment throughout the audit - not just during planning and before issuing the audit opinion. The best ideas may come when we ask people to invest time thinking about risk assessment before these meetings. Risk Assessment and Planning Discussion (RAPD) meetings provide excellent opportunities to discuss risks holistically - but to be most effective, we plan and conduct these at the right times.
Completion of an Accounting Disclosure Checklist (ADC)	Completion of relevant sections of an ADC during risk assessment in connection with each business process assists in understanding disclosures to be expected for the process. The prior period financial statements and related disclosures, and previously completed ADC combined with current year activity, changes within existing business processes and events and circumstances that may require disclosures, all while being mindful to take a 'fresh lens' approach, assists in assessing inherent risk.

Examples

How do we consider the inherent risk factors when assessing RMs around disclosures? [ISA | 565.159465]

Below are examples of how an engagement team considers the inherent risk factors when assessing RMs around disclosures.

Fact Pattern:

RM	Initial risk assessment to identify and assess RMs
Disclosures of significant accounting policies that are an integral part of the financial statements are incomplete, inaccurate or not fairly presented Additional risk description - goodwill and intangible asset accounting policies	Significant accounting policies related to recognition of goodwill and intangible assets for an acquisition are complex and involve judgment. The entity has not been involved in a significant business combination in several years, and the acquisition is material to the financial statements and intended users. Based on these factors, the engagement team has assessed the risk of the accounting policy disclosures is an RMM.
The disclosures is incomplete, inaccurate, or not fairly presented. Additional risk description - revenue note disclosures.	The entity's revenue streams have significant variable consideration that is difficult to identify and measure. Revenue is significant to the users of the intended users and the recognition policy is complex. Based on these factors, the engagement team has assessed the risk of the revenue note disclosures is an RMM.

What are additional examples of how we determine the inherent risk level? [ISA | 565.11149]

See some examples below on how we determine the inherent risk levels.

Expected credit losses (ECL) allowance

The engagement team identified the following RMM: An inappropriate amount is estimated and recorded for the expected credit losses (ECL) allowance for financial assets or contracts.

Fact Pattern:

The ECL has several factors that are high on the inherent risk continuum:

- The most complex estimate for the entity (factors *complexity* and *subjectivity* are very high on the risk continuum, and possibly *exposure to losses, significant accounting, or economic factors, susceptibility of error*, etc.)
- The most heavily scrutinized by regulators and investors (factors *nature of the account, exposure to losses*).

Analysis:

Based on these factors alone, the engagement team assesses the inherent risk as Significant for related RMMs.

Deposits

The engagement team identified the following RMM: Deposits are recorded inappropriately when:

- they are not accurately recorded
- they do not meet the recognition requirements or
- they do not exist.

Fact Pattern:

The only factor that is higher on the risk continuum is volume/amount. All other factors are quite low on the risk continuum (low complexity even on a relative basis to other processes, no judgment, no exposure to losses, no SUTs or related parties, etc.).

Analysis:

Based on this fact pattern, the engagement team assesses the inherent risk of RMMs associated with deposits as Base.

Product Returns

The engagement team identified an RMM related to the rights of return estimate, including the related disclosures.

Fact Pattern:

While volume/amount are lower on the risk continuum, exposure to losses and changes from the prior period are higher on the risk continuum (given certain changes in the entity's revenue contracts and uncertainty in the economic environment).

Analysis:

Based on this fact pattern, the engagement team assesses the inherent risk for both the account and related disclosures as Elevated.

Control environment

International Standards on Auditing: ISA 315.21

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

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

Control environment

21. The auditor shall obtain an understanding of the control environment relevant to the preparation of the financial statements, through performing risk assessment procedures, by: (Ref: Para. A99-A100)

(a) Understanding the set of controls, processes and structures that address: (Ref: Para. A101.A102)

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

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

(iii) The entity's assignment of authority and responsibility;

(iv) How the entity attracts, develops, and retains competent individuals; and

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

and

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

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

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

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

ISA Application and Other Explanatory Material: ISA 315.A96-A108

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

A96. The controls in the control environment, the entity's risk assessment process and the entity's process to monitor the system of internal control are primarily indirect controls (i.e., controls that are not

sufficiently precise to prevent, detect or correct misstatements at the assertion level but which support other controls and may therefore have an indirect effect on the likelihood that a misstatement will be detected or prevented on a timely basis). However, some controls within these components may also be direct controls.

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

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

A98. Because these components are foundational to the entity's system of internal control, any deficiencies in their operation could have pervasive effects on the preparation of the financial statements. Therefore, the auditor's understanding and evaluations of these components affect the auditor's identification and assessment of risks of material misstatement at the financial statement level, and may also affect the identification and assessment of risks of material misstatement at the assertion level. Risks of material misstatement at the financial statement level affect the auditor's design of overall responses, including, as explained in ISA 330, an influence on the nature, timing and extent of the auditor's further procedures.[35]

---

35 ISA 330, paragraphs A1-A3

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

Scalability

A99. The nature of the control environment in a less complex entity is likely to be different from the control environment in a more complex entity. For example, those charged with governance in less complex entities may not include an independent or outside member, and the role of governance may be undertaken directly by the owner-manager where there are no other owners. Accordingly, some considerations about the entity's control environment may be less relevant or may not be applicable.

A100. In addition, audit evidence about elements of the control environment in less complex entities may not be available in documentary form, in particular where communication between management and other personnel is informal, but the evidence may still be appropriately relevant and reliable in the circumstances.

Examples:

- The organizational structure in a less complex entity will likely be simpler and may include a small number of employees involved in roles related to financial reporting.
- If the role of governance is undertaken directly by the owner-manager, the auditor may determine that the independence of those charged with governance is not relevant.
- Less complex entities may not have a written code of conduct but, instead, develop a culture that emphasizes the importance of integrity and ethical behaviour through oral communication

and by management example. Consequently, the attitudes, awareness and actions of management or the owner-manager are of particular importance to the auditor's understanding of a less complex entity's control environment.

Understanding the control environment (Ref: Para. 21(a))

A101. Audit evidence for the auditor's understanding of the control environment may be obtained through a combination of inquiries and other risk assessment procedures (i.e., corroborating inquiries through observation or inspection of documents).

A102. In considering the extent to which management demonstrates a commitment to integrity and ethical values, the auditor may obtain an understanding through inquiries of management and employees, and through considering information from external sources, about:

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

Evaluating the control environment (Ref: Para. 21(b))

Why the auditor evaluates the control environment

A103. The auditor's evaluation of how the entity demonstrates behavior consistent with the entity's commitment to integrity and ethical values; whether the control environment provides an appropriate foundation for the other components of the entity's system of internal control; and whether any identified control deficiencies undermine the other components of the system of internal control, assists the auditor in identifying potential issues in the other components of the system of internal control. This is because the control environment is foundational to the other components of the entity's system of internal control. This evaluation may also assist the auditor in understanding risks faced by the entity and therefore in identifying and assessing the risks of material misstatement at the financial statement and assertion levels (see paragraph A86).

The auditor's evaluation of the control environment

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

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

Example:

Direct involvement by a single individual may be key to enabling the entity to meet its growth and other objectives, and can also contribute significantly to an effective system of internal control. On the other hand, such concentration of knowledge and authority can also lead to an increased susceptibility to misstatement through management override of controls.

A106. The auditor may consider how the different elements of the control environment may be influenced by the philosophy and operating style of senior management taking into account the involvement of independent members of those charged with governance.

A107. Although the control environment may provide an appropriate foundation for the system of internal control and may help reduce the risk of fraud, an appropriate control environment is not necessarily an effective deterrent to fraud.

Example:

Human resource policies and procedures directed toward hiring competent financial, accounting, and IT personnel may mitigate the risk of errors in processing and recording financial information. However, such policies and procedures may not mitigate the override of controls by senior management (e.g., to overstate earnings).

A108. The auditor's evaluation of the control environment as it relates to the entity's use of IT may include such matters as:

- Whether governance over IT is commensurate with the nature and complexity of the entity and its business operations enabled by IT, including the complexity or maturity of the entity's technology platform or architecture and the extent to which the entity relies on IT applications to support its financial reporting.
- The management organizational structure regarding IT and the resources allocated (for example, whether the entity has invested in an appropriate IT environment and necessary enhancements, or whether a sufficient number of appropriately skilled individuals have been employed including when the entity uses commercial software (with no or limited modifications)).

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Understand and evaluate the Control Environment component [ISA | 1310]

What do we do?

Obtain an understanding of and evaluate the entity's control environment relevant to the preparation of the financial statements, including the policies and actions of management and those charged with governance concerning the entity's control environment.

Why do we do this?

We obtain an understanding of and evaluate the entity's control environment relevant to the preparation of the financial statements to support our identification and assessment of risks of material misstatement (RMMs).

Execute the Audit

What is the Control Environment? [ISA | 1310.1300]

An entity's Control Environment is the set of controls, processes and structures that provide the basis for carrying out internal control across the entity.

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 to the entity.

The Control Environment sets the tone of an organization, influencing the control consciousness of its people and provides the overall foundation for the operation of the other components of the entity's system of internal control

Does the Control Environment encompass all levels of an entity? [ISA | 1310.11898]

Yes. The Control Environment underpins how ICFR is carried out across the organization and at all levels. So we may assess the Control Environment at levels below the parent or corporate level - e.g. regions, divisions, operating units and functional areas.

Does the Control Environment encompass third-party service providers and business partners? [ISA | 1310.11899]

Yes. The Control Environment also includes third-party service providers and business partners. Although the organization may rely on an outsourced service provider to conduct business processes, policies, and procedures on behalf of the entity, management retains ultimate responsibility for meeting the requirements for an effective system of internal control.

Why is the Control Environment an important component of ICFR? [ISA | 1310.1400]

If we consider the entity's internal control structure as like the structure of a house, the Control Environment is the foundation; thus it is the foundation for ICFR.

Process-level control activities directly affect financial reporting, but often affect only just one particular stream of transactions. In contrast, the Control Environment's effect on ICFR is indirect, yet it may have a pervasive effect on multiple business processes throughout the organization.

Not Integrated Audit | How do we obtain an understanding of the entity's Control Environment? [ISA | 1310.1800]

We obtain an understanding of the entity's Control Environment by:

- understanding, through inquiry, the set of controls, processes and structures that address the following elements/principles:
  - how the entity demonstrates a commitment to integrity and ethical values
  - how the board of directors/those charged with governance demonstrates independence and oversight of internal control
  - structures, reporting lines, and authorities and responsibilities
  - how the entity demonstrates a commitment to attract, develop, and retain competent individuals
  - how the entity holds individuals accountable for their internal control responsibilities
- performing procedures to obtain an understanding of the CERAMIC components:
  - begin by performing inquiries to obtain an understanding of each element/principle within the component.
  - consider whether certain factors apply to determine whether to perform more than inquiry
  - If at least one of the factors apply, design additional procedures to obtain an understanding (i.e. observation and/or inspection)
- Based on our understanding obtained, evaluating the control environment component.

We also consider how information is being used in our procedures and determine the appropriate audit procedures to evaluate the reliability of the information used to obtain an understanding.

If we identify a control deficiency, we perform the following:

- evaluate the severity of the control deficiency and assess the impact on our audit; and
- evaluate whether the control deficiency is indicative of a fraud risk factor.
- evaluate whether control deficiencies undermine the other components of the entity's system of internal control.

What do we do if there are unaddressed elements after we obtain an understanding of CERAMIC? [ISA | 1310.8653]

When those charged with governance are not separate from management, it is appropriate for the following elements to be unaddressed:

- Element 2 - Those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Element 11 - The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

In all other circumstances, if there are unaddressed elements after we have obtained an understanding of the CERAMIC component, we identify a control deficiency in the related CERAMIC component.

What are the five elements of the Control Environment component? [ISA | 1310.11926]

We obtain an understanding over the following five elements in order to evaluate the Control Environment component of ICFR.

Elements of the Control Environment component	Element 1: The organization demonstrates a commitment to integrity and ethical values. Element 2: When those charged with governance are separate from management, those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control. Element 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. Element 4: The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. Element 5: The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

How may the Control Environment component for less complex entities be different? [ISA | 1310.2000]

Although the same principles / elements underlying the Control Environment component apply for both simpler and complex organizations; the entity's approach to address the CERAMIC component is likely to differ.

For example, a less complex entity may not have a written code of conduct, but instead, develops a culture that emphasizes the importance of integrity and ethical behavior through oral communication and by management example. Further, compared to a more complex entity, communication may be less structured and easier to achieve in a less complex entity since there may be fewer levels of responsibility and management may be more available and have greater visibility. As such, there is often more direct interaction between management and employees such that the organizational structure, reporting lines, and responsibilities are clear and evident.

A less complex entity's commitment to integrity and ethical values may appear in the variety of policies and procedures it employs or the attitudes, awareness and actions of those charged with governance and management.

Examples

1.1 Understand how the entity demonstrates a commitment to integrity and ethical values [ISA | 1311]

What do we do?

Obtain an understanding of how management's oversight responsibilities are carried out such as creating and maintaining the entity's culture and demonstrating a commitment to integrity and ethical values (Element 1).

Why do we do this?

Deficiencies identified can impact our audit approach, including how we identify and assess risks of material misstatement.

Our understanding of how management's oversight responsibilities are carried out, such as creating and maintaining the entity's culture and demonstrating commitment to integrity and ethical values, helps us to evaluate whether management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior and whether the control environment provides an appropriate foundation for the other components of the entity's system of internal control considering the nature and complexity of the entity

Execute the Audit

What is Element 1 of the Control Environment component? [ISA | 1311.1300]

Element 1:

"*The organization demonstrates a commitment to integrity and ethical values.*"

This includes how management's oversight responsibilities are carried out, such as creating and maintaining the entity's culture.

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 behavioural standards or codes of conduct, how then 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 promote 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.

What are the points of focus for Element 1? [ISA | 1311.1400]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us obtain an understanding of the set of controls, processes and structures that are intended to address the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus for Element 1, along with questions that may help us obtain an understanding of how the entity addresses Element 1 and the related Control Environment component.

Points of Focus	Questions
• Sets the tone at the top • Establishes standards of conduct • Evaluates adherence to standards of conduct • Addresses deviations in a timely manner	• How does management and those charged with governance demonstrate through its directives, actions and behavior the importance of integrity and ethical values to support the functioning of ICFR? • If the entity has a written code of conduct and/or formal and documented policies / procedures: - Do the standards of conduct apply throughout the organization - to all levels, geographies and external partners? - How are the standards of conduct communicated to employees (e.g. through regular training, website postings and newsletters)? • If the entity does not have a written code of conduct and/ or formal and documented policies / procedures, how does management and those charged with governance develop a culture that emphasizes the importance of integrity and ethical behavior? • How are violations identified, reported and addressed? How does the entity enforce the standards of conduct and their commitment to integrity and ethical values? Are violations remedied in a timely and consistent manner? • Are there clear consequences for deviating from the standards of conduct at every level? • Does management emphasize this message? • Is the tone at the top consistently demonstrated in the informal and routine actions and communications of the leaders at all levels of the entity?

What is the tone at the top? [ISA | 1311.1500]

Management and the board of directors / those charged with governance are expected to lead by example creating and maintaining the entity's culture by developing values, a philosophy and an operating style for the entity. Tone at the top and throughout the organization are fundamental to the functioning of an internal control system.

How does the tone at the top manifest itself? [ISA | 1311.11953]

An entity often documents the expectations of management and the board of directors / those charged with governance in the form of:

- missions and value statements;
- standards or codes of conduct;
- policies and practices;
- operating principles, directives, guidelines and other supporting communications;
- actions and decisions made by management and the board of directors / those charged with governance;
- attitudes and responses to violations and deviations; and
- informal and routing actions and communications of management and the board of directors / those charged with governance throughout all levels of an entity.

What drives the tone at the top? [ISA | 1311.11954]

The tone at the top is affected by:

- operating style and personal conduct of management and the board of directors / those charged with governance;
- attitudes toward risk;
- conservative versus aggressive positions - e.g. on estimates and policy choices; and
- degree of formality - e.g. in a small family business, controls may be more informal.

Why is tone at the top important to the Control Environment? [ISA | 1311.11955]

A consistent tone from the board and senior management through to operating unit management levels helps establish a common understanding of the values, business drivers and expected behavior of employees and partners of the entity.

Not having a consistent tone at the top to support a strong culture of internal control undermines the awareness of risk and can lead to:

- inappropriate responses to risks;
- lack of focus and discipline around control activities that may result in deficiencies in their design and operating effectiveness;
- lack of information and faltering communication; and
- lack of action on feedback from monitoring activities.

The tone at the top can therefore either drive or impede internal control.

Personal indiscretions, lack of receptiveness to bad news or unfairly balanced compensation practices could affect the culture and encourage inappropriate conduct. By contrast, a history of ethical and responsible behavior by management and the board of directors / those charged with governance and a demonstrated commitment to addressing misconduct send strong messages in support of integrity. Employees are likely to develop the same attitudes about right and wrong - and about risks and controls - as those shown by management.

Examples

1.2 Understand how the board of directors / those charged with governance demonstrates independence and oversight of internal control [ISA | 1312]

What do we do?

When those charged with governance are separate from management, obtain an understanding of how those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control (Element 2).

Why do we do this?

Deficiencies in the entity's control environment can impact our audit approach, including how we identify and assess risks of material misstatement.

Our understanding of how those charged with governance demonstrate independence from management and exercises oversight of the entity's system of internal control helps us to evaluate whether management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior and whether the control environment provides an appropriate foundation for the other components of the entity's system of internal control considering the nature and complexity of the entity.

Execute the Audit

What is Element 2 of the Control Environment component? [ISA | 1312.1300]

Element 2:

"When those charged with governance are separate from management, those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control."

This includes the nature and extent of oversight and governance that the entity has in place over management's process for making accounting estimates.

What are the points of focus for Element 2? [ISA | 1312.1400]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us obtain an understanding of the set of controls, processes and structures that are intended to address the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus for Element 2, along with questions that may help us obtain an understanding of how the entity addresses Element 2 and the related Control Environment component.

Points of focus	Questions

• Establishes oversight responsibilities • Applies relevant expertise • Operates independently • Provides oversight for the system of internal control	• Has the entity formalized its bylaws and committee charters consistent with applicable local regulatory requirements? • Do management and those charged with governance have defined roles, responsibilities and powers of delegation? Do those charged with governance actively oversee external financial reporting and management's performance of internal control? • Do those charged with governance periodically evaluate the skills and expertise required by its members to enable them to appropriately oversee, question and evaluate the senior management team? • Do those charged with governance have sufficient individuals who are independent of management, and are they objective in their evaluations and decision making? • When those charged with governance are not independent of management, are there established oversight roles such that members of management are acting in a governance role? • Do those charged with governance review and assess the performance of key members of management? • Has the entity established channels of communication between all relevant parties at regular intervals using formal agendas? • Has the entity established a structure to investigate whistle-blower allegations that appropriately involves those charged with governance? • How do those charged with governance oversee the risk of management override of ICFR?

When are those charged with governance separate from management? [ISA | 1312.8487]

Those charged with governance are separate from management when at least one member of those charged with governance is not a member of management.

For smaller, less complex entities (i.e. simpler operations and/or financial reporting), those charged with governance will likely not include any members separate from management. Additionally, the role of governance may be undertaken directly by the 'owner-manager' when there are no other owners.

What if those charged with governance are not separate from management? [ISA | 1312.8488]

When those charged with governance are not separate from management, they are not able to demonstrate their independence or exercise oversight responsibility over themselves. Accordingly, Element 2 of the Control Environment component is not applicable.

In this situation, the entity may put in place different controls, processes and structures that result in adequate oversight responsibility for the design, implementation, and conduct of internal control by management operating in a governance role as compared to when those charged with governance

are separate from management. As a result, the attitudes, awareness and actions of management are of particular importance when understanding the control environment.

What is the role of those charged with governance within an entity's ICFR? [ISA | 1312.8489]

The 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 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.

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

Why is the effectiveness of the design of the control environment influenced by the independence of those charged with governance from management? [ISA | 1312.8490]

Independent members of those charged with governance provide value through their impartiality, healthy skepticism, and unbiased evaluation. It allows them to question and scrutinize management's activities, present alternative views, and have the courage to act in the face of obvious or suspected wrongdoing.

How do we obtain an understanding of whether those charged with governance demonstrate independence from management? [ISA | 1312.8492]

We obtain an understanding of whether those charged with governance demonstrate independence from management by considering whether or not those charged with governance has sufficient independent individuals based upon the size, nature, and complexity of the entity.

Individuals are independent when they have no current or recent personal or professional relationship with the entity. Their independence is demonstrated through their objectivity of mind, action, appearance, and fact.

The larger and more complex the entity's operations and/or financial reporting, the higher the proportion of independent individuals within those charged with governance is necessary for the effectiveness of the design of the control environment. A publicly listed company is typically required to have a majority of those charged with governance to be independent. In some jurisdictions, there is also a requirement for some or all members of some committees to be independent, such as audit committees.

For smaller, less complex entities, those charged with governance may include only one independent member or a small proportion of independent members. This may be sufficient for smaller, less complex entities, because they have simpler operations and/or financial reporting. As an alternative, the entity may put in place different controls, processes and structures that result in

adequate oversight responsibility for the design, implementation, and conduct of internal control by management operating in a governance role as compared to when the majority of those charged with governance are independent of management. In this instance, the attitudes, awareness and actions of management are of particular importance when understanding the control environment.

If based upon the size, nature, and complexity of the entity, there are not sufficient independent individuals within those charged with governance, we identify a control deficiency.

What are examples of how those charged with governance exercise oversight for the development and performance of internal control? [ISA | 1312.8493]

Examples of how those charged with governance exercise oversight for the development and performance of internal control are included in the table below:

Internal Control Component	Oversight activities
Control Environment	• Oversee the definition of and apply the standards of conduct of the entity • Establish the expectations and evaluate the performance, integrity, and ethical values of the chief executive officer or equivalent role • Establish oversight structures and processes aligned with the objectives of the entity (e.g., board and committees as appropriate with requisite skills and expertise) • Commission board oversight effectiveness reviews and address opportunities for improvement • Exercise fiduciary responsibilities to shareholders or owners and due care in oversight (e.g., prepare for and attend meetings, review the entity's financial statements and other disclosures) • Challenge senior management by asking probing questions about the entity's plans and performance, and require follow-up and corrective actions, as necessary (e.g., questioning transactions that occur repeatedly at the end of interim or annual reporting periods)
Risk Assessment	• Consider internal and external factors that pose significant risks to the achievement of objectives; identify issues and trends (e.g., sustainability implications of the entity's business operations) • Challenge management's assessment of risks to the achievement of objectives, including the potential impact of significant changes (e.g., risks associated with entering a new market), and fraud or corruption

	• Evaluate how proactively the entity assesses risks relating to innovations and changes such as those triggered by new technology or economic and geopolitical shifts
Information and Communication	• Communicate direction and tone at the top • Obtain, review, and discuss information relating to the entity's • achievement of objectives • Scrutinize information provided and present alternative views • Review disclosures to external stakeholders for completeness, • relevance, and accuracy • Allow for and address upward communication of issues
Monitoring Activities	• Assess and oversee the nature and scope of monitoring activities, any management overrides of controls, and management's evaluation and remediation of deficiencies • Engage with management, internal and external auditors, and others, as appropriate, to evaluate the level of awareness of the entity's strategies, specified objectives, risks, and control implications associated with evolving business, infrastructure, regulations, and other factors
Control Activities	• Make specific inquiries of management regarding the selection, development, and deployment of control activities in significant risk areas and remediation as necessary (e.g., in response to significant risks emerging from internal or external factors) • Oversee senior management in its performance of control activities

Examples

1.3 Understand structures, reporting lines, and authorities and responsibilities [ISA | 1313]

What do we do?

Obtain an understanding of how the entity's management establishes, with the oversight of those charged with governance, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives (Element 3).

Why do we do this?

Deficiencies identified can impact our audit approach, including how we identify and assess risks of material misstatement.

Understanding of how the entity's management establishes, with oversight from those charged with governance, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives helps us to understand whether risks may arise, such as:

- lines of reporting have not been established such that that responsibilities are not appropriately carried out and information does not flow as needed;
- authority and responsibility have not been delegated based on demonstrated competence, and roles are not defined based on who is responsible for or kept informed of decisions;
- appropriate authority has not been delegated such that inappropriate risks are accepted (e.g., a new vendor is not taken on without the requisite due diligence review); or
- duties are not segregated such that there is a risk of inappropriate conduct in the pursuit of objectives

Execute the Audit

What is Element 3 of the Control Environment component? [ISA | 1313.1300]

Element 3:

"Management establishes, with the oversight of those charged with governance, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives."

What are the points of focus for Element 3? [ISA | 1313.1400]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us obtain an understanding of the set of controls, processes and structures that are intended to address the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus for Element 3, along with questions that may help us obtain an understanding of how the entity addresses Element 3 and the related Control Environment component.

Points of Focus	Questions
• Considers all structures of the entity • Establishes reporting lines • Defines, assigns and limits authority and responsibilities	• Has the entity created an organizational chart that defines the roles, responsibilities and reporting lines to support the achievement of its financial reporting objectives? Does the organizational chart take into account segregation of duties and include clear reporting lines and communication channels? • Does the organizational chart support the entity's control structure? Does it consider departmental responsibilities, geographies, levels of management and third-party service providers? • Is authority and responsibility delegated based on demonstrated competence? Are appropriate segregation of duties and potential conflicts of interest considered?

	• Are authorities and responsibilities assigned across the entity and at all levels? Are they appropriate and sufficiently well-defined to enable accountability over operating units and functional areas? • Are the mechanisms employed by management sufficient to monitor the assignment of authorities and responsibilities across the entity and at all levels? • Are decentralized decision makers sufficiently knowledgeable? How do they learn about new regulations or changes to regulations? How strong are the lines of communication? • Is management effectively managing outsourced service providers through service-level agreements?

Examples

1.4 Understand how the entity demonstrates a commitment to attract, develop, and retain competent individuals [ISA | 1314]

What do we do?

Obtain an understanding of how the entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives (Element 4).

Why do we do this?

Deficiencies identified can impact our audit approach, including how we identify and assess risks of material misstatement.

Understanding whether the entity demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives helps us to understand whether risks may arise, such as:

- individuals not having the appropriate skills necessary to carry out assigned responsibilities and to support internal control in the achievement of the entity's objectives or
- lack of performance evaluations and incentives to motivate and reinforce expected levels of performance and desired conduct

Execute the Audit

What is Element 4 of the Control Environment component? [ISA | 1314.1300]

Element 4:

"The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives."

This includes how management identifies the need for, and applies, specialized skills or knowledge related to the accounting estimate, including with respect to the use of a specialist.

What are the points of focus for Element 4? [ISA | 1314.1400]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us obtain an understanding of the set of controls, processes and structures that are intended to address the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus for Element 4, along with questions that may help us obtain an understanding of how the entity addresses Element 4 and the related Control Environment component.

Points of Focus	Questions
• Establishes policies and practices • Evaluates competence and addresses shortcomings • Attracts, develops and retains individuals • Plans and prepares for succession	• Has the entity established competence requirements for people in key financial reporting and internal audit roles across the organization and for those charged with governance? • Does the entity properly address any identified knowledge gaps by hiring qualified individuals, training existing employees or using qualified management's specialists or service providers, where necessary? • Does the entity develop and maintain policies that reflect the entity's values and objectives? Does the entity review and update these policies regularly? • Does the entity ensure these policies are used as a basis to make decisions on hiring, retention, termination and promotion? • Does the entity have programs in place that demonstrate management's commitment to attract, develop, and retain competent personnel (e.g. mentoring and training)? • Does the entity have a process for evaluating the performance of its personnel on a periodic basis, including the use of development plans? • Has the entity implemented a process to ensure adequate staffing levels, including contingency and succession plans?

Examples

1.5 Understand how the entity holds individuals accountable for their internal control responsibilities [ISA | 1315]

What do we do?

Obtain an understanding of how the entity holds individuals accountable for the internal control responsibilities in the pursuit of objectives (Element 5).

Why do we do this?

Deficiencies identified can impact our audit approach, including how we identify and assess risks of material misstatement.

Obtaining an understanding of whether the entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives helps us to understand whether risks may arise, such as:

- lack of accountability and implementation of corrective actions may result in individuals not performing their internal control responsibilities;
- inappropriate performance measures, incentives and rewards for those responsible for the entity's system of internal control may drive unwanted behaviour (e.g. manipulation of the financial statements or accounting records, high-pressure sales tactics, negotiations directed at increasing quarterly sales or profit at any cost, or implicit offers of kickbacks); or
- the creation of undue pressures that cause employees to fear the consequences of not achieving objectives and circumvent processes or engage in fraudulent activity or corruption.

Execute the Audit

What is Element 5 of the Control Environment component? [ISA | 1315.1300]

Element 5:

"The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives."

What are the points of focus for Element 5? [ISA | 1315.1400]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us obtain an understanding of the set of controls, processes and structures that are intended to address the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus for Element 5, along with the questions that may help us obtain an understanding of how the entity addresses Element 5 and the related Control Environment component.

Points of Focus	Questions

• Enforces accountability through structures, authorities and responsibilities • Establishes performance measures, incentives and rewards • Evaluates performance measures, incentives and rewards for ongoing relevance • Considers excessive pressures • Evaluates performance and rewards or disciplines individuals	• Does the entity hold individuals within the entity accountable? Do employees certify that they have fulfilled their internal control responsibilities during any given period-i.e. are employees asked to certify their results to instill responsibility and accountability? • Is there a performance measurement and reward plan aligned with the entity's ethical values and financial reporting objectives? • Does the incentive plan balance the pressures of achieving performance objectives against maintaining effective ICFR and financial reporting objectives? • Do management and those charged with governance monitor the appropriate amount of pressure on achieving financial reporting results and the effect that it has on people and the effectiveness of ICFR? • Does the entity evaluate performance of key personnel within the financial reporting process against the established performance measures? • Are shortcomings appropriately addressed?

Examples

1.6 Not Integrated Audit | Perform procedures to obtain an understanding of the CERAMIC components [ISA | 7843]

What do we do?

Perform procedures to obtain an understanding of the CERAMIC components

Why do we do this?

We perform procedures to obtain an understanding of the CERAMIC components as part of our risk assessment to support our identification and assessment of risks of material misstatement (RMMs).

Execute the audit

What type of procedures do we perform to obtain an understanding of the CERAMIC components? [ISA | 7843.8495]

We begin by performing inquiries to obtain an understanding of the CERAMIC components. However, inquiry alone may not be sufficient to obtain the necessary understanding of the components when certain factors exist. We consider whether certain factors apply to determine whether to perform more than inquiry.

What factors do we consider when determining whether to perform more than inquiry in order to obtain an understanding of CERAMIC? [ISA | 7843.8496]

We consider the factors in the table below. When certain circumstances exist, there is a rebuttable presumption that we will perform more than inquiry in order to obtain an understanding over one or more of the CERAMIC components.

Factor	Impact on nature, timing, and extent of procedures
Size and complexity of the entity	The larger and more complex an entity, the more robust and comprehensive its set of controls, processes, structures, and communications necessary to address the elements/principles within each CERAMIC component. As such, for a large and/or complex entity, it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Conversely, less complex entities require simpler set of controls, processes, structures, and communications to achieve their objectives. For example, the entity may develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication rather than have a written code of code. Due the simplicity of their processes, inquiry alone may be sufficient to obtain an understanding of the entity's CERAMIC. The size of an entity (e.g. number of employees) may be an indicator of its complexity. However, some smaller entities may be complex, and some larger entities may be less complex. Refer to 'What characteristics of the entity do we think about to assess its complexity?' for additional information.
Our existing knowledge of the entity's system of internal control	When we have less knowledge of the entity's system of internal control (e.g. we are performing an initial audit), it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC.
Reliance on the entity's control activities	It is presumed that inquiry alone is not sufficient to obtain an understanding of CERAMIC when we plan to place reliance on the entity's control activities to reduce our control risk.
Nature and extent of changes in entity's systems and operations	Where there have been extensive changes in the entity's systems (e.g. new IT system implementation) and/or operations (e.g. product line or geographic expansion, significant changes in management or personnel) from the prior year, the entity's system of internal control may have significantly changed such that

	it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Inquiry alone may also not be sufficient when changes to the entity's CERAMIC have occurred to remediate prior year deficiencies.

What if we conclude that it is appropriate to rebut the presumption that 'inquiry alone is not sufficient'? [ISA | 7843.8497]

When we conclude that rebutting the presumption that 'inquiry alone is not sufficient' is appropriate in the circumstances of the engagement, and accordingly have only obtained an understanding of CERAMIC through inquiry, we document the reasons for that conclusion.

What characteristics influence the complexity of an entity? [ISA | 7843.8498]

The characteristics below influence the complexity of an entity. No one characteristic is more indicative than another of an entity's complexity. The presence of one characteristic that indicates 'more complexity' does not necessarily indicate a 'more complex' entity. We collectively think about all the characteristics when considering the factor 'size and complexity of the entity.'

Factor	Impact on nature, timing, and extent of procedures
Size and complexity of the entity	More robust and comprehensive sets of controls, processes, structures, and communications are necessary at larger and more complex entities to address the elements/principles within each CERAMIC component. As such, for a large and/or complex entity, it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Conversely, less complex entities require a simpler set of controls, processes, structures, and communications to achieve their objectives. For example, the entity may develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication rather than have a written code of code. Due the simplicity of their processes, inquiry alone may be sufficient to obtain an understanding of the entity's CERAMIC. The size of an entity (e.g. number of employees) may be an indicator of its complexity. However, some smaller entities may be complex, and some larger entities may be less complex. Refer to 'What characteristics influence the complexity of an entity ?' for additional information.
Our existing knowledge of the entity's system of internal control	When we have less knowledge of the entity's system of internal control (e.g. we are performing an initial audit), it is presumed

	that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC.	
Reliance on the entity's control activities	It is presumed that inquiry alone is not sufficient to obtain an understanding of CERAMIC when we plan to place reliance on the entity's control activities to reduce our control risk.	
Nature and extent of changes in entity's systems and operations	Where there have been extensive changes in the entity's systems (e.g. new IT system implementation) and/or operations (e.g. product line or geographic expansion, significant changes in management or personnel) from the prior year, the entity's system of internal control may have significantly changed such that it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Inquiry alone may also not be sufficient when changes to the entity's CERAMIC have occurred to remediate prior year deficiencies.	
Characteristics	Examples of less complexity	Examples of more complexity
Organizational structure and management personnel	An entity has few business segments or lines of business with a small management team and no internal audit.	An entity has several business segments or lines of business with multiple levels of management and a sophisticated internal audit department.
Ownership and governance structure	An owner-manager is responsible for the governance and direct oversight of the operations and accounting / financial reporting for the entity.	The entity is publicly traded, and those charged with governance operate independently of management.
Operating characteristics	The entity is a single legal entity with operations in only a few geographic locations.	The entity is a group that has many components that operate in several markets and geographic locations and are decentralized.

Nature of assets, liabilities and transactions	The entity processes routine transactions and the accounts do not require complex accounting or significant judgments.	The entity processes non-routine or unusual transactions, including in controversial or emerging areas, and the accounts require complex accounting or significant judgments.
Nature of the accounting processes and controls	The entity has simple record-keeping with few accounting processes with primarily manual control activities performed by a few people.	The entity has many IT systems (or many instances of a single system) and customizes the systems for the entity's specific needs.
IT systems	The entity has few IT systems and the entity uses pre-packaged purchased applications that are not able to be customized by the entity.	The entity has many IT systems (or many instances of a single system) and customizes the systems for the entity's specific needs.

1.7 Conclude on the overall Control Environment component [ISA | 5575]

What do we do?

Based on our understanding of the control environment, evaluate whether (a) management, with the oversight of those charged with governance, created and maintained a culture of honesty and ethical behavior, (b) the control environment provided an appropriate foundation for the other components of ICFR considering the nature and complexity of the entity and (c) control deficiencies identified in the control environment undermine the other components of the entity's system of internal control.

Why do we do this?

We evaluate the Control Environment component of internal control over financial reporting (ICFR) to support our identification and assessment of risks of material misstatement (RMMs), particularly financial statement level risks.

Execute the Audit

Not Integrated Audit | How do we evaluate the Control Environment component of ICFR? [ISA | 5575.1300]

Based on our understanding of the control environment, we identify a CERAMIC control deficiency (refer to 'Evaluate the severity and assess the impact of CERAMIC control deficiencies' for additional information) if:

- there are unaddressed principles/elements or
- the entity's set of controls, processes and structures do not appropriately address the principle/element considering the nature and complexity of the entity.

When there is at least one principle/element that is unaddressed or not appropriately addressed, we conclude one or more of the following depending upon the principle/element:

- Management, with the oversight of those charged with governance, has not created and maintained a culture of honesty and ethical behavior.
- The control deficiencies identified undermine the other components of the entity's system of internal control.
- The control environment has not provided an appropriate foundation for the other components of ICFR considering the nature and complexity of the entity.

If we have any of the conclusions above, we identify a financial statement level risk (see activity 'Evaluate RMs at the financial statement level' for additional information) and respond to the risk in line with activity 'Design and implement overall responses'.

How may the Control Environment component for less complex entities be different? [ISA | 5575.2000]

Although the same principles / elements underlying the Control Environment component apply for both simpler and complex organizations; the entity's approach to address the CERAMIC component is likely to differ.

For example, a less complex entity may not have a written code of conduct, but instead, develops a culture that emphasizes the importance of integrity and ethical behavior through oral communication and by management example. Further, compared to a more complex entity, communication may be less structured and easier to achieve in a less complex entity since there may be fewer levels of responsibility and management may be more available and have greater visibility. As such, there is often more direct interaction between management and employees such that the organizational structure, reporting lines, and responsibilities are clear and evident.

A less complex entity's commitment to integrity and ethical values may appear in the variety of policies and procedures it employs or the attitudes, awareness and actions of those charged with governance and management.

What additional items do we think about when performing our evaluation? [ISA | 5575.11921]

When performing our evaluation, we also think about:

- the results of other risk assessment procedures, including our understanding of other CERAMIC components; and

> For example, a lack of response / dismissal of control deficiencies identified as a result of the entity's monitoring activities may be indicative of management's disregard of the importance of internal control. Conversely, effective monitoring activities and management that is focus on

addressing control deficiencies in a timely manner is indicative of a Control Environment that provides an appropriate foundation for the other components of ICFR.

- evidence of issues with the overall Control Environment / tone at the top identified during our audit.

For example, known instances of fraud or intentional non-compliance with laws and regulations is an indication that management, with the oversight of those charged with governance, has not created and maintained a culture of honest and ethical behavior.

1.8 Evaluate whether deficiencies in the Control Environment indicate a fraud risk factor [ISA | 1316]

What do we do?

IF we identify a control deficiency in the entity's control environment, THEN we evaluate the extent to which the control deficiency indicates a fraud risk factor.

Why do we do this?

When we identify a deficiency related to the Control Environment, the deficiency may indicate a fraud risk factor that, in turn, may indicate the existence of a risk of material misstatement due to fraud.

Execute the Audit

What are fraud risk factors? [ISA | 1316.11964]

Fraud risk factors can cover a broad range of events and conditions. They are specific events and conditions we observe or identify that promote or foster an environment where fraud could occur.

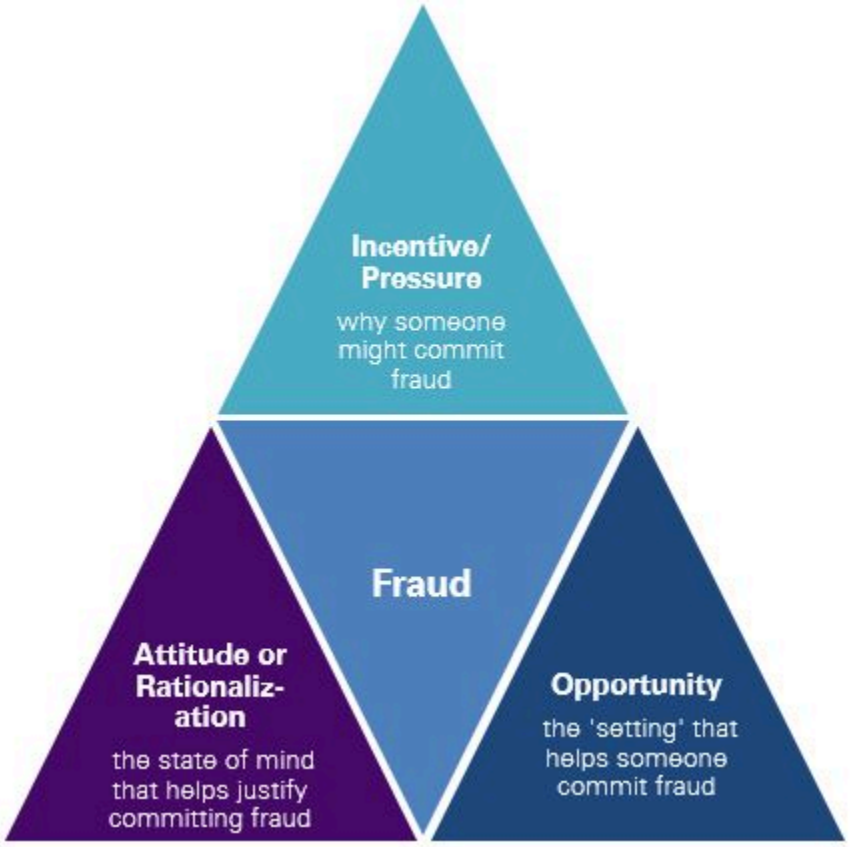
Understanding these factors helps us consider where fraud risks may exist that call for a specific audit response.

Identifying fraud risk factors does not necessarily mean that fraud exists or will eventually occur. But these factors are often present in circumstances in which fraud exists.

Category of fraud risk factor	Description	Example
Incentive or pressure	Why someone might commit fraud	An employee may be in financial distress (internal incentive), or management may be under extreme pressure to meet financial targets (external incentive). These situations can be a catalyst for committing the

		fraud, and could be internal or external to the entity or the person committing the fraud.
Opportunity	The 'setting' that helps someone commit fraud	Deficiencies in CERAMIC or poorly designed control activities can make it easier for an individual to carry out fraud.
Attitude or rationalization	The state of mind that helps justify committing fraud	Management's attitude that the entity will meet its targets at all costs, or a justification claiming that the fraud doesn't really harm anybody.

These three categories of fraud risk factors form the fraud triangle.



What fraud risk factors might be present when we identify deficiencies in the Control Environment? [ISA | 1316.1400]

The table below sets out each element related to the Control Environment component, along with some possible fraud risk factors if deficiencies are identified.

Element within which a control deficiency is identified	Possible fraud risk factor

Element 1: The organization demonstrates a commitment to integrity and ethical values	*Attitude or rationalization:* Ineffective communication, implementation, support and enforcement of the entity's values or ethical standards by management -or- the communication of inappropriate values or ethical standards
Element 2: When those charged with governance are separate from management, those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control	*Opportunity:* Ineffective oversight by those charged with governance or audit committee over the financial reporting process and internal control
Element 3: Management establishes, with the oversight of those charged with governance, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives	*Opportunity:* Complex or unstable organizational structure involving unusual managerial lines of authority Ineffective oversight by those charged with governance or audit committee over the financial reporting process and internal control
Element 4: The organization demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives	*Opportunity:* High turnover of senior management, counsel or those charged with governance High turnover or employment of ineffective accounting, internal audit or IT staff
Element 5: The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives	*Opportunity:* Inadequate monitoring of controls, including automated controls and controls over interim financial reporting *Attitude or rationalization:* Ineffective communication, implementation, support and enforcement of the entity's values or ethical standards by management -or- the communication of inappropriate values or ethical standards

	Excessive interest by management in maintaining or increasing the entity's stock price or earnings trends A management practice of committing to analysts, creditors and other third parties to achieve aggressive or unrealistic forecasts Recurring attempts to justify marginal or inappropriate accounting on the basis of immateriality

Will every deficiency in an entity's Control Environment lead us to identify a fraud risk factor or fraud risk? [ISA | 1316.1500]

No, not every control deficiency in the Control Environment component will result in the identification of a fraud risk factor or fraud risk.

The extent to which a control deficiency in the Control Environment is indicative of a fraud risk factor is based on the specific facts and circumstances of the control deficiency. For example, a control deficiency in the Control Environment that is determined to be a significant deficiency or material weakness, is more likely to result in the identification of a fraud risk factor.

Examples

How do we determine whether a deficiency in the Control Environment indicates a fraud risk factor? [ISA | 1316.1700]

Fact pattern

Widget & Co, a widget manufacturer, recently relocated its headquarters from Los Angeles to Atlanta. While most of the key financial reporting personnel moved with the entity, several individuals responsible for the sales and accounts receivable (A/R) process resigned.

No succession plan was in place, so management hired several replacement personnel in Atlanta and reassigned some sales and A/R activities to other staff members.

Over the next several months, the entity struggled with timely accounting for its sales and A/R, including calculation of a key estimate - i.e. the allowance for doubtful accounts.

On audit, the engagement team did not identify errors in the related accounts during the period. Nevertheless, they identified deficiencies in the entity's Control Environment, particularly Element 4, which involves the policies and procedures in place for retaining competent individuals and preparing for succession in key financial reporting roles.

Analysis

The deficiency identified in Widget & Co's Control Environment lead the engagement team to determine whether the deficiency indicates an additional fraud risk factor to consider as they identify fraud risks.

The engagement team identifies an additional fraud risk factor related to high turnover rates and employment of ineffective accounting staff, particularly in the sales and A/R process. '

The engagement team then considers the additional fraud risk factor together with other fraud risk factors previously identified - e.g. excessive pressure on management to meet the requirements or expectations of third parties to meet sales targets set by those charged with governance and senior management.

This leads them to identify an additional fraud risk related to manipulating estimates for revenue recognition, including the shipping transit time and the determination of sales return allowances.

The entity's risk assessment process

International Standards on Auditing: ISA 315.22-23

The entity's risk assessment process

22. The auditor shall obtain an understanding of the entity's risk assessment process relevant to the preparation of the financial statements, through performing risk assessment procedures, by:	
(a) Understanding the entity's process for: (Ref: Para. A109.A110) (i) Identifying business risks relevant to financial reporting objectives; (Ref: Para. A62) (ii) Assessing the significance of those risks, including the likelihood of their occurrence; and (iii) Addressing those risks;	and (b) Evaluating whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity. (Ref: Para. A111.A113)

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

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

(b) Consider the implications for the auditor's evaluation in paragraph 22(b).

ISA Application and Other Explanatory Material: ISA 315.A96-A98 | ISA 315.A109-A113

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

A96. The controls in the control environment, the entity's risk assessment process and the entity's process to monitor the system of internal control are primarily indirect controls (i.e., controls that are not

sufficiently precise to prevent, detect or correct misstatements at the assertion level but which support other controls and may therefore have an indirect effect on the likelihood that a misstatement will be detected or prevented on a timely basis). However, some controls within these components may also be direct controls.

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

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

A98. Because these components are foundational to the entity's system of internal control, any deficiencies in their operation could have pervasive effects on the preparation of the financial statements. Therefore, the auditor's understanding and evaluations of these components affect the auditor's identification and assessment of risks of material misstatement at the financial statement level, and may also affect the identification and assessment of risks of material misstatement at the assertion level. Risks of material misstatement at the financial statement level affect the auditor's design of overall responses, including, as explained in ISA 330, an influence on the nature, timing and extent of the auditor's further procedures.[35]

---

35 ISA 330, paragraphs A1-A3

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

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

A109. As explained in paragraph A62, not all business risks give rise to risks of material misstatement. In understanding how management and those charged with governance have identified business risks relevant to the preparation of the financial statements, and decided about actions to address those risks, matters the auditor may consider include how management or, as appropriate, those charged with governance, has:

- Specified the entity's objectives with sufficient precision and clarity to enable the identification and assessment of the risks relating to the objectives;
- Identified the risks to achieving the entity's objectives and analyzed the risks as a basis for determining how the risks should be managed; and
- Considered the potential for fraud when considering the risks to achieving the entity's objectives.[36]

---

36 ISA 240, paragraph 19

A110. The auditor may consider the implications of such business risks for the preparation of the entity's financial statements and other aspects of its system of internal control.

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

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

A111. The auditor's evaluation of the entity's risk assessment process may assist the auditor in understanding where the entity has identified risks that may occur, and how the entity has responded to those risks. The auditor's evaluation of how the entity identifies its business risks, and how it assesses and addresses those risks assists the auditor in understanding whether the risks faced by the entity have been identified, assessed and addressed as appropriate to the nature and complexity of the entity. This evaluation may also assist the auditor with identifying and assessing financial statement level and assertion level risks of material misstatement (see paragraph A86).

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

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

Scalability

A113. Whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity is a matter of the auditor's professional judgment.

Example:

In some less complex entities, and particularly owner-managed entities, an appropriate risk assessment may be performed through the direct involvement of management or the owner-manager (e.g., the manager or owner-manager may routinely devote time to monitoring the activities of competitors and other developments in the market place to identify emerging business risks). The evidence of this risk assessment occurring in these types of entities is often not formally documented, but it may be evident from the discussions the auditor has with management that management are in fact performing risk assessment procedures.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Understand and evaluate the risk assessment process [ISA | 1317]

What do we do?

Obtain an understanding of management's risk assessment process and evaluate whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity.

Why do we do this?

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

If an entity does not have a risk assessment process that is appropriate for its nature and complexity, it may lead to unidentified / unaddressed risks relevant to its financial reporting objectives, ineffectively designed control activities and an increase in the possibility of a material misstatement in the financial statements.

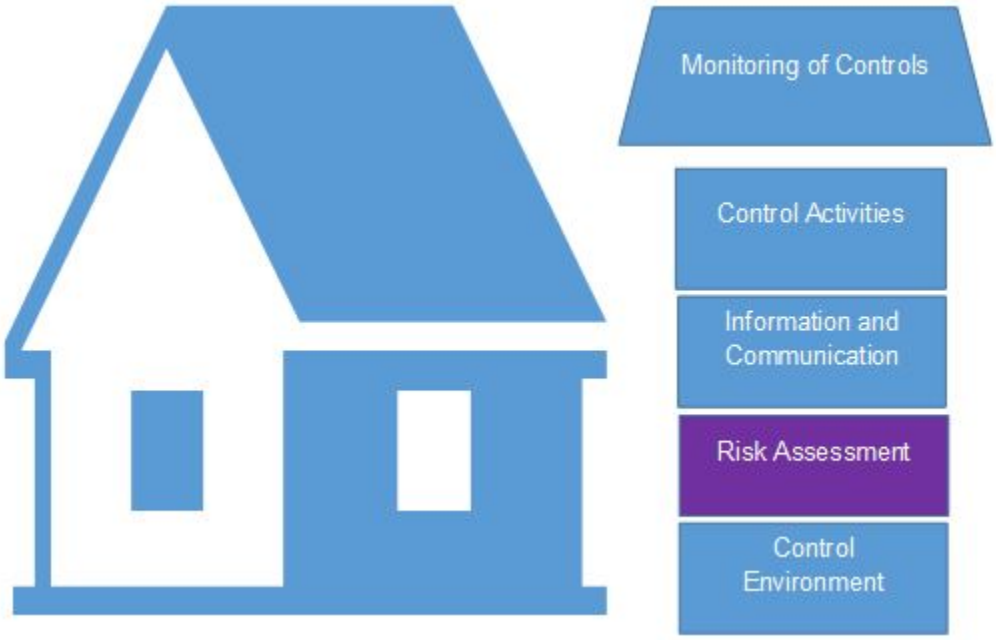
Our understanding and evaluation of the entity's risk assessment process assists us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

Why is risk assessment an important component of ICFR? [ISA | 1317.1400]

Risk assessment is an essential component of ICFR because it forms the basis for how management identifies and analysis risks relevant to its financial reporting objectives and how they determine the risks to be managed. If an entity does not have a risk assessment process that is appropriate for its nature and complexity, it may lead to unidentified / unaddressed risks relevant to its financial reporting objectives, ineffectively designed control activities and an increase in the possibility of a misstatement in the financial statements.

Using our house example, the risk assessment process is the blueprint or map of the house, and is needed to appropriately design the house.



Understanding the entity's risk assessment process, relevant to the preparation of the financial statements, gives us insight into whether the entity is appropriately identifying risks (and have a sound ICFR), which may affect our risk assessments. In addition, it also helps us plan and execute our audit and gives us insight into potential RMMs that we may not have considered.

When does an entity perform its risk assessment process? [ISA | 1317.1600]

An effective risk assessment process is iterative in nature. The four principles / elements within the Risk Assessment component are not always considered sequentially because there is considerable overlap among the principles / elements. Further, as an entity performs and monitors controls, management may identify items that require earlier risk determinations to be reassessed.

How do we obtain an understanding of the entity's risk assessment process? [ISA | 1317.1900]

We obtain an understanding of the entity's risk assessment process by:

- understanding, through inquiry, the processes that address the following elements/principles:
  - how the entity specifies objectives to identify and assess risks
  - how the entity identifies and analyses risks
  - how the entity considers fraud when assessing risks
  - how the entity identifies and assesses changes that impact internal control
- performing procedures to obtain an understanding of the CERAMIC components:
  - begin by performing inquiries
  - consider whether certain factors apply to determine whether to perform more than inquiry
  - If at least one of the factors apply, design additional procedures to obtain an understanding (i.e. observation and/or inspection)
- based on the above, evaluating the entity's risk assessment process.

We also consider how information is being used in our procedures and determine the appropriate audit procedures to evaluate the reliability of the information used to obtain an understanding.

If we identify a control deficiency in a CERAMIC component(s), we evaluate the severity of the control deficiency and assess the impact on our evaluation.

What do we do if there are unaddressed elements after we obtain an understanding of CERAMIC? [ISA | 1317.8653]

When those charged with governance are not separate from management, it is appropriate for the following elements to be unaddressed:

- Element 2 - Those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Element 11 - The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

In all other circumstances, if there are unaddressed elements after we have obtained an understanding of the CERAMIC component, we identify a control deficiency in the related CERAMIC component.

What are the four elements of the Risk Assessment component? [ISA | 1317.1800]

When management has an established risk assessment process, we consider the four elements outlined in the table below when obtaining an understanding of the Risk Assessment component of ICFR.

Elements of the Risk Assessment component	Element 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. Element 7: The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed. Element 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives. Element 9: The organization identifies and assesses changes that could significantly affect the system of internal control.

Our understanding includes how the entity's risk assessment process identifies and addresses risks related to accounting estimates.

Why is it important for an entity to consider the potential for fraud? [ISA | 1317.11847]

Every entity faces some risk of fraud from within, but the very nature of fraud makes it difficult to detect. It can also evolve and change over time, which makes fraud prevention or detection even more difficult.

At the same time, as shown by major corporate fraud scandals in nearly every decade of the past century, fraud can have a significant negative effect on an entity's financial reporting process, the reliability of its financial statements, and investor confidence.

Principle / Element 8 highlights the importance of fraud risks to make it clear that an appropriate risk assessment process should specifically consider the vulnerability of the entity to fraudulent activity.

Why is it important for an entity to monitor changes? [ISA | 1317.11848]

Experience suggests that entities control routine business processes well. However, when something new or unusual happens, the system of ICFR is unable to process the new events or transactions in a controlled manner. This, in turn, may lead to material errors in the financial statements and deficiencies in internal control.

Identifying new transactions and events ahead of time through an entity's 'early warning systems' allows the entity time to make the necessary adjustments to the existing system of ICFR.

Principle / Element 9 highlights the importance of considering whether changes result in additional risks, and whether the entity has designed and implemented control activities that appropriately mitigate those additional risks.

How do the auditing standards map to the four elements of the Risk Assessment Process component?

[ISA | 1317.11849]

The following table maps each of the processes that comprise the risk assessment process in the auditing standards to the related elements of the Risk Assessment Process component.

Process	Related Elements
Identifying business risks relevant to financial reporting objectives	Element 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. Element 7: The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed. Element 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives. Element 9: The organization identifies and assesses changes that could significantly impact the system of internal control.
Estimating the significance of the risks and assessing the likelihood of their occurrence	Element 7: The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed. Element 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives. Element 9: The organization identifies and assesses changes that could significantly impact the system of internal control.
Deciding about actions to address those risks	Element 7:

	The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed. Element 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives. Element 9: The organization identifies and assesses changes that could significantly impact the system of internal control.

How may the Risk Assessment Process component for smaller, less complex entities be different? [ISA | 1317.2200]

In some less complex, smaller entities, and particularly owner-managed entities, an appropriate risk assessment may be performed through the direct involvement of management or the owner-manager (for example, the manager or owner-manager may routinely devote time to monitoring the activities of competitors and other developments in the market place to identify emerging business risks). The evidence of this risk assessment occurring in these types of entities is often not formally documented. However, discussions we have with management, corroborated by e-mails or other correspondence between management and other personnel, may provide evidence that management is, in fact, performing risk assessment procedures appropriate to the nature and complexity of the entity.

Examples

1.1 Understand how the entity specifies objectives to identify and assess risks [ISA | 1318]

What do we do?

Understand how management identifies and specifies the objectives for the business sufficiently to allow them appropriately identify the risks to achieving these objectives.

Why do we do this?

If an entity has not specified its objectives with sufficient precision and clarity, it may not be able to properly identify and assesses the risks relating to the objectives. This may lead to unidentified / unaddressed risks relevant to its objectives, ineffectively designed control activities and an increase in the possibility of a misstatement in the financial statements.

Our understanding and evaluation of the entity's risk assessment process assists us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

What is Element 6 of the Risk Assessment component? [ISA | 1318.1300]

Element 6:

The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

The objectives are those relevant to financial reporting, including accounting estimates.

What are the points of focus for Element 6? [ISA | 1318.1400]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us obtain an understanding of the process that is intended to address the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus for Element 6, along with questions that may help us obtain an understanding of how the entity addresses Element 6 and the related Risk Assessment component.

Points of focus	Questions
• Complies with applicable accounting standards • Considers materiality • Reflects entity activities	• Does the entity understand the objective of ICFR? • When the entity reviews and updates its understanding of applicable accounting and financial reporting standards, does it consider how those changes affect its financial reporting objectives? • What does the entity consider material, and is the amount consistent with what a reasonable stakeholder / investor might determine? • What qualitative and quantitative factors does the entity consider when determining if something is material? • How does the entity identify its significant components (segments, subsidiaries, divisions, operating units, functions)? • How does the entity identify risks relevant to financial reporting, including the related accounts / disclosures in the financial statements and relevant assertions? • How is overall materiality cascaded down to each component and each significant account (risk tolerance)?

Examples

1.2 Understand how the entity identifies and analyses risks [ISA | 1319]

What do we do?

Obtain an understanding of how the entity identifies risks to achieving its objectives at the entity and process levels and analyzes risks to determine how they should be managed.

Why do we do this?

If an entity does not have a risk assessment process that is appropriate for its nature and complexity, it may lead to unidentified / unaddressed risks relevant to its financial reporting objectives, ineffectively designed control activities and an increase in the possibility of a misstatement in the financial statements.

Our understanding and evaluation of the entity's risk assessment process assists us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

What is Element 7 of the Risk Assessment component? [ISA | 1319.1300]

Element 7:

The organization identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.

These risks are business risks relevant to financial reporting objectives, including risks related to accounting estimates.

What are the points of focus for Element 7? [ISA | 1319.1400]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us obtain an understanding of the process that is intended to address the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus for Element 7, along with questions that may help us obtain an understanding of how the entity addresses Element 7 and the related Risk Assessment component.

Points of focus	Questions
• Includes entity, subsidiary, division, operating unit, and functional levels • Analyzes internal and external factors • Involves appropriate levels of management • Estimates significance of risks identified	• Does the entity perform or update its risk assessment at least annually – and more frequently if changes in circumstances require a reassessment? • Does the entity's risk assessment process involve appropriate levels of management, including key personnel from throughout the entity, such as Legal, HR, IT, or management in other locations? • Does the risk assessment process focus sufficiently on risks to achieving its financial reporting objectives? • Is the entity's risk assessment process designed to capture both internal factors (e.g. change in management

• Determines how to respond to risks	responsibilities, IT changes) and external factors (e.g. economic changes, changes in customer demand)? • Does the entity link the identified risks to the relevant financial statement assertions, accounts and disclosures across all levels? • Does the entity consider the significance of the identified risks in terms of the: - likelihood of the risk occurring; - effect; - velocity (or speed) to impact upon occurrence of the risk; and - persistence (or duration of time) of impact after occurrence of the risk? • Does the risk assessment process address: - how the risks are managed; - how much risk is tolerated; and - what is done to accept, avoid, reduce or share the risk at the appropriate level across the entity? • Are those charged with governance appropriately involved in the risk assessment process?

What factors does an entity consider as part of their risk assessment? [ISA | 1319.1500]

An entity considers both internal and external risk factors, as well as sources of risk such as those that affect the entity's ability to initiate, authorize, process and record transactions and other adjustments that are reflected in the financial statements.

The table below sets out examples of internal and external risk factors that an entity may consider as part of the risk assessment process.

External factors	Examples
Economic	Changes that can affect financing, capital availability and barriers to competitive entry.
Natural environment	Natural or human-caused catastrophes, or ongoing climate change that can lead to: • changes in operations; • reduced availability of raw materials; or • loss of information systems, highlighting the need for contingency planning

Regulatory	A new financial reporting standard that can require different or additional reporting by a legal entity, management operating model, or line of business; a new anti-trust law or regulation that can force changes in operating or reporting policies and strategies
Foreign operations	A change of government in a foreign country of operation that results in new laws and regulations or altered tax regimes
Social	Changing customer needs or expectations that can affect: • product development • the production process • customer service • pricing • warranties
Technological	Developments that can affect: • the availability and use of data; • infrastructure costs; and • the demand for technology-based services
Internal factors	
Infrastructure	• Decisions on the use of capital resources that can affect operations and the ongoing availability of infrastructure • Entering into new business areas or transactions with which an entity has little experience. • Significant and rapid expansion of operations which can strain controls and increase the risk of a breakdown of controls. • Expansion or acquisition of foreign operations may introduce new types of transactions e.g. foreign currency transactions.
Management structure	A change in management responsibilities that can affect the way certain controls are effected
Personnel	The quality of personnel hired and methods of training and motivation that can influence the level of control consciousness within the entity; expiration of labor agreements that can affect the availability of staff
Access to assets	The nature of the entity's activities and employee accessibility to assets that can contribute to misappropriation of resources

Technology	Significant and rapid changes in the information system or incorporation of new technologies into production processes or the information system can affect the entity's system of internal control. A disruption in information systems processing that can adversely affect the entity's operations

When should an entity's risk assessment process be documented? [ISA | 1319.11900]

Because much of the risk assessment process takes place in meetings and discussions - including at the senior management and board of directors / those charged with governance level - timely documentation of the risk assessment activities undertaken by the entity and their results helps demonstrate an effective assessment of the entity's ICFR, by both management and us.

Examples

1.3 Understand how the entity considers fraud when assessing risks [ISA | 1320]

What do we do?

Obtain an understanding of how the entity considers the potential for fraud in assessing risks to the achievement of objectives.

Why do we do this?

Every entity faces some risk of fraud from within, but the very nature of fraud makes it difficult to detect. It can also evolve and change over time, which makes fraud prevention or detection even more difficult.

If an entity's risk assessment process does not consider the risk of fraud, appropriate for its nature and complexity, it may lead to unidentified / unaddressed risks relevant to its financial reporting objectives, ineffectively designed control activities and an increase in the possibility of a misstatement in the financial statements.

Our understanding and evaluation of the entity's risk assessment process assists us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

What is Element 8 of the Risk Assessment component? [ISA | 1320.1300]

Element 8:

The organization considers the potential for fraud in assessing risks to the achievement of objectives.

This includes the entity's process for considering the potential for fraud in accounting estimates, including the susceptibility of accounting estimates to management bias.

What are the points of focus related to Element 8? [ISA | 1320.1400]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us evaluate obtain an understanding of the process that is intended to address the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus for Element 8, along with questions that may help us obtain an understanding of how the entity addresses Element 8 and the related Risk Assessment component.

Points of focus	Questions
• Considers various types of fraud • Assesses incentives and pressures • Assesses opportunities • Assesses attitudes and rationalizations and responsibilities	• Does the entity have a process for a continuous comprehensive fraud risk assessment that can identify various types of fraud (including fraudulent financial reporting, material safeguarding of assets and management override of controls) that could affect the entity? • Does the entity consider in its fraud risk assessment process the various 'fraud risk triangle' factors that may affect or create fraud risks, namely: - incentives and pressures; - opportunities; and - attitudes or rationalizations? • Does the entity involve appropriate personnel at various levels across the organization in its fraud risk assessment, including interviews with employees to assess the incentives and pressures to manipulate earnings, misappropriate assets or alter records? • Does the entity consider, assess and reassess compensation programs, if necessary? • How does the entity manage fraud risk across the organization and at all levels (including its segments and subsidiary, division, operating unit and functional levels) related to the financial statement accounts and assertions? • How do those charged with governance oversee the identification, assessment and evaluation of fraud risks, including opportunities for, and occurrences of, management override of controls? • Do management and those charged with governance maintain adequate oversight, an appropriate level of skepticism and allow for proper reporting of actual or suspected fraud by implementing a whistleblower program? • Has the entity identified controls that respond to the identified fraud risks, including the risk of bias and management override of controls?

What else do we consider when understanding how the entity addresses this principle/element? [ISA | 1320.11909]

We consider the entity's process for considering the potential for fraud in accounting estimates, including the susceptibility of accounting estimates to management bias. We also consider how management communicates to those charged with governance its process for identifying and responding to risks of fraud.

What else do we consider when understanding how the entity addresses this principle/element? [ISA | 1320.11910]

We consider the entity's process for considering the potential for fraud in accounting estimates, including the susceptibility of accounting estimates to management bias. We also consider how management communicates to those charged with governance its process for identifying and responding to risks of fraud.

What types of misstatements are relevant to our consideration of fraud risks? [ISA | 1320.1700]

Two basic types of misstatements are relevant when we consider fraud risks.

Type	Description	How it's accomplished
Fraudulent financial reporting	Intentional misstatements or omissions of amounts or disclosures designed to deceive financial statement users	• Manipulating, falsifying or altering accounting records or supporting documentation • Misrepresenting or intentionally omitting events, transactions or other significant information from the financial statements • Intentionally misapplying accounting policies or principles
Misappropriation of assets	Theft of an entity's assets, causing the financial statements to be misstated	• Embezzling receipts • Stealing assets • Causing an entity to pay for goods or services that have not been received and may be accompanied by false or misleading records or documents, possibly created by circumventing controls

How is management's fraud risk assessment different from our independent fraud risk assessment? [ISA | 1320.1600]

The process used by management to identify and assess fraud risks is likely to be similar to the way we do it. It is likely to include identifying and evaluating fraud risk factors to identify fraud risks that are relevant to the entity.

What are fraud risk factors? [ISA | 1320.11964]

Fraud risk factors can cover a broad range of events and conditions. They are specific events and conditions we observe or identify that promote or foster an environment where fraud could occur.

Understanding these factors helps us consider where fraud risks may exist that call for a specific audit response.

Identifying fraud risk factors does not necessarily mean that fraud exists or will eventually occur. But these factors are often present in circumstances in which fraud exists.

Category of fraud risk factor	Description	Example
Incentive or pressure	Why someone might commit fraud	An employee may be in financial distress (internal incentive), or management may be under extreme pressure to meet financial targets (external incentive). These situations can be a catalyst for committing the fraud, and could be internal or external to the entity or the person committing the fraud.
Opportunity	The 'setting' that helps someone commit fraud	Deficiencies in CERAMIC or poorly designed control activities can make it easier for an individual to carry out fraud.
Attitude or rationalization	The state of mind that helps justify committing fraud	Management's attitude that the entity will meet its targets at all costs, or a justification claiming that the fraud doesn't really harm anybody.

These three categories of fraud risk factors form the fraud triangle.

How does an entity consider fraud risk factors in the identification of fraud risks? [ISA | 1320.1800]

Once an entity identifies fraud risk factors, it evaluates whether the identified fraud risk factors, individually or in combination, indicate that a fraud risk is present.

How is materiality considered in an entity's fraud risk assessment? [ISA | 1320.1900]

Both management and we consider:

- the quantitative materiality of any potential misstatements; and
- the qualitative impacts the fraud would have

when identifying and evaluating risks of fraud in the entity's financial reporting process, and designing and evaluating relevant anti-fraud controls.

Risks of fraud generally demand careful consideration and response, even if the misstatements that could arise as a result of those fraud risks are lower than the quantitative measure of planning materiality.

Qualitative considerations that an entity may consider as part of its fraud risk assessment include:

- intent to achieve a particular outcome (e.g. meet analysts' expectations, which in some cases could be achieved through manipulation in an amount that is lower than planning materiality);
- involvement in the fraud by members of senior management; and
- questions about the pervasiveness of the fraud and its impact on the reliability of the entire financial statements, etc.

How are those charged with governance involved in an entity's fraud risk assessment? [ISA | 1320.2000]

Those charged with governance may play an important role in the entity's risk assessment process, particularly when it comes to the risk of management override of controls. The standards say that one of the roles of those charged by governance is to counterbalance the pressures on management in relation to financial reporting that may arise from market demands or remuneration schemes, which may be achieved by challenging management, depending on the circumstances, when performing their oversight responsibilities.

For example, based on the results of the entity's risk assessment process, those charged with governance might exercise its oversight role by selecting a sample of significant accounting estimates in the financial statements and reviewing and challenging management's key judgments about these estimates on a periodic basis.

The board might perform similar oversight for the accounting and financial reporting of significant unusual transactions and other matters that may be prone to management bias and override of controls.

Examples

1.4 Understand how the entity identifies and assesses changes that impact internal control [ISA | 1321]

What do we do?

Obtain an understanding of how the organization identifies and assesses changes that could significantly impact the system of internal control.

Why do we do this?

If an entity does not appropriately identify and assess changes that could significantly impact the system of internal control, it may lead to unidentified / unaddressed risks relevant to its financial reporting objectives, ineffectively designed control activities and an increase in the possibility of a material misstatement in the financial statements.

Our understanding and evaluation of the entity's risk assessment process assists us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

What is Element 9 of the Risk Assessment component? [ISA | 1321.1300]

Element 9:

The organization identifies and assesses changes that could significantly impact the system of internal control.

This includes the entity's process for assessing changes that could impact the entity's process for making accounting estimates.

What are the points of focus related to Element 9? [ISA | 1321.1400]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us obtain an understanding of the process that is intended to address the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus related to Element 9, along with questions that may help us obtain an understanding of how the entity addresses Element 9 and the related Risk Assessment component.

Points of focus	Questions
• Assesses changes in the external environment • Assesses changes in the business model • Assesses changes in leadership	• Does the entity have a process to identify and assess internal and external changes in operations that could impact the risks relevant to financial reporting and system of internal controls? • Does this process include monitoring external information sources (e.g. news channels, trade publications, and websites) to identify changes in the marketplace and other external factors that could directly or indirectly affect their business operations and, therefore, the risks relevant to financial reporting and system of internal controls? • Does the entity consider the effect of changes in the organization (e.g. acquisitions, business model changes, personnel changes) on the risks relevant to financial reporting and system of internal controls?

When obtaining an understanding of the entity's risk assessment process, we consider the frequency of entity's assessments of business risks relevant to the preparation of financial statements. Obtaining an understanding of the entity's process to address Element 9 assists us in understanding whether the frequency of the entity's assessments is appropriate.

What are some examples of changes that could affect ICFR? [ISA | 1321.1500]

The following are examples of changes that could significantly affect an entity's system of internal control for each of the points of focus related to Element 9.

Point of focus	Examples
Assesses changes in the external environment	*Changing external environment* A changing regulatory or economic environment can result in increased competitive pressures, changes in operating requirements and significantly different risks. Large-scale operations, or reporting or compliance failures by one entity may result in the rapid introduction of broad new regulations. *Changing physical environment*

	Natural disasters directly affecting the entity, supply chain and other business partners may result in elevated risks that an entity needs to consider to sustain its business. For example, the entity may need to find alternative sources of raw material, or move production.
Assesses changes in the business model	*Changing business model* When an entity has new accounts or transactions, enters new business lines, alters the delivery of its services through new outsourced relationships, or alters the composition of existing business lines, new risks may emerge. The composition of the risks initially assessed as the basis for establishing internal controls may have changed, or the potential effect of those risks may have increased so that prior internal controls are no longer sufficient. Some financial services organizations, for example, may have expanded into new products and concentrations without focusing on how to respond to changes in the associated risks of their products. *Significant acquisitions and divestitures* When an entity acquires a new business operation, it may need to review and standardize internal controls across the expanded entity. Controls in place in the pre-acquisition operation may not be well developed, suitable for the newly combined entity or scalable to the new business. Similarly, when an entity disposes of a business operation, the level of acceptable variation may change in operations, and materiality may decrease. In addition, certain entity-level controls at the divested operation may no longer be present. Acquisitions and divestitures may require the entity to review and possibly revise its internal controls to support the achievement of objectives as appropriate to the restructured entity. *Foreign operations* Expanding or acquiring foreign operations carries new and often unique risks. Developing business in new geographies, or outsourcing operations to foreign locations, may help the business to grow and/or reduce costs, but it may also present new challenges and alter the type and extent of the risks.

	Operating in unfamiliar markets poses risk because there are different customs and practices. For example, the control environment in a new environment is likely to be influenced by the local culture and customs. Business risks may result from factors unique to the local economy, regulatory environment and channels of communication. *Rapid growth* When operations expand significantly and quickly, existing structures, business processes, information systems and resources may be strained to the point that internal controls break down. For example, adding manufacturing shifts to meet demand, or increasing back-office personnel may result in supervisors being unable to adapt to the higher activity levels and maintain adequate control. *New technology* When new technology is incorporated into production, service delivery processes or supporting information systems, internal controls will likely need to be modified. For example, introducing sales capabilities through mobile devices may require access controls specific to that technology, as well as changes in controls over shipping processes.
Assesses changes in leadership	*Significant personnel changes* A new member of senior management at an entity may not understand the entity's culture and reflect a different philosophy, or may focus solely on performance to the exclusion of control-related activities. For example, a newly hired CEO focusing on revenue growth may send a message that a prior focus on effective internal control is now less important. Further, high turnover of personnel, in the absence of effective training and supervision, can result in breakdowns. For instance, a company that reduces its staffing levels by 25% in an attempt to reduce costs may erode the overall internal control structure.

Examples

1.5 Not Integrated Audit | Perform procedures to obtain an understanding of the CERAMIC components [ISA | 7843]

What do we do?

Perform procedures to obtain an understanding of the CERAMIC components

Why do we do this?

We perform procedures to obtain an understanding of the CERAMIC components as part of our risk assessment to support our identification and assessment of risks of material misstatement (RMMs).

Execute the audit

What type of procedures do we perform to obtain an understanding of the CERAMIC components? [ISA | 7843.8495]

We begin by performing inquiries to obtain an understanding of the CERAMIC components. However, inquiry alone may not be sufficient to obtain the necessary understanding of the components when certain factors exist. We consider whether certain factors apply to determine whether to perform more than inquiry.

What factors do we consider when determining whether to perform more than inquiry in order to obtain an understanding of CERAMIC? [ISA | 7843.8496]

We consider the factors in the table below. When certain circumstances exist, there is a rebuttable presumption that we will perform more than inquiry in order to obtain an understanding over one or more of the CERAMIC components.

Factor	Impact on nature, timing, and extent of procedures
Size and complexity of the entity	The larger and more complex an entity, the more robust and comprehensive its set of controls, processes, structures, and communications necessary to address the elements/principles within each CERAMIC component. As such, for a large and/or complex entity, it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Conversely, less complex entities require simpler set of controls, processes, structures, and communications to achieve their objectives. For example, the entity may develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication rather than have a written code of code. Due the simplicity of their processes, inquiry alone may be sufficient to obtain an understanding of the entity's CERAMIC.

	The size of an entity (e.g. number of employees) may be an indicator of its complexity. However, some smaller entities may be complex, and some larger entities may be less complex. Refer to 'What characteristics of the entity do we think about to assess its complexity?' for additional information.
Our existing knowledge of the entity's system of internal control	When we have less knowledge of the entity's system of internal control (e.g. we are performing an initial audit), it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC.
Reliance on the entity's control activities	It is presumed that inquiry alone is not sufficient to obtain an understanding of CERAMIC when we plan to place reliance on the entity's control activities to reduce our control risk.
Nature and extent of changes in entity's systems and operations	Where there have been extensive changes in the entity's systems (e.g. new IT system implementation) and/or operations (e.g. product line or geographic expansion, significant changes in management or personnel) from the prior year, the entity's system of internal control may have significantly changed such that it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Inquiry alone may also not be sufficient when changes to the entity's CERAMIC have occurred to remediate prior year deficiencies.

What if we conclude that it is appropriate to rebut the presumption that 'inquiry alone is not sufficient'? [ISA | 7843.8497]

When we conclude that rebutting the presumption that 'inquiry alone is not sufficient' is appropriate in the circumstances of the engagement, and accordingly have only obtained an understanding of CERAMIC through inquiry, we document the reasons for that conclusion.

What characteristics influence the complexity of an entity? [ISA | 7843.8498]

The characteristics below influence the complexity of an entity. No one characteristic is more indicative than another of an entity's complexity. The presence of one characteristic that indicates 'more complexity' does not necessarily indicate a 'more complex' entity. We collectively think about all the characteristics when considering the factor 'size and complexity of the entity.'

Factor	Impact on nature, timing, and extent of procedures
Size and complexity of the entity	More robust and comprehensive sets of controls, processes, structures, and communications are necessary at larger and

	more complex entities to address the elements/principles within each CERAMIC component. As such, for a large and/or complex entity, it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Conversely, less complex entities require a simpler set of controls, processes, structures, and communications to achieve their objectives. For example, the entity may develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication rather than have a written code of code. Due the simplicity of their processes, inquiry alone may be sufficient to obtain an understanding of the entity's CERAMIC. The size of an entity (e.g. number of employees) may be an indicator of its complexity. However, some smaller entities may be complex, and some larger entities may be less complex. Refer to 'What characteristics influence the complexity of an entity ?' for additional information.
Our existing knowledge of the entity's system of internal control	When we have less knowledge of the entity's system of internal control (e.g. we are performing an initial audit), it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC.
Reliance on the entity's control activities	It is presumed that inquiry alone is not sufficient to obtain an understanding of CERAMIC when we plan to place reliance on the entity's control activities to reduce our control risk.
Nature and extent of changes in entity's systems and operations	Where there have been extensive changes in the entity's systems (e.g. new IT system implementation) and/or operations (e.g. product line or geographic expansion, significant changes in management or personnel) from the prior year, the entity's system of internal control may have significantly changed such that it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Inquiry alone may also not be sufficient when changes to the entity's CERAMIC have occurred to remediate prior year deficiencies.

Characteristics	Examples of less complexity	Examples of more complexity

Organizational structure and management personnel	An entity has few business segments or lines of business with a small management team and no internal audit.	An entity has several business segments or lines of business with multiple levels of management and a sophisticated internal audit department.
Ownership and governance structure	An owner-manager is responsible for the governance and direct oversight of the operations and accounting / financial reporting for the entity.	The entity is publicly traded, and those charged with governance operate independently of management.
Operating characteristics	The entity is a single legal entity with operations in only a few geographic locations.	The entity is a group that has many components that operate in several markets and geographic locations and are decentralized.
Nature of assets, liabilities and transactions	The entity processes routine transactions and the accounts do not require complex accounting or significant judgments.	The entity processes non-routine or unusual transactions, including in controversial or emerging areas, and the accounts require complex accounting or significant judgments.
Nature of the accounting processes and controls	The entity has simple record-keeping with few accounting processes with primarily manual control activities performed by a few people.	The entity has many IT systems (or many instances of a single system) and customizes the systems for the entity's specific needs.
IT systems	The entity has few IT systems and the entity uses pre-packaged purchased applications that are not able to be customized by the entity.	The entity has many IT systems (or many instances of a single system) and customizes the systems for the entity's specific needs.

1.6 Evaluate the entity's risk assessment process

[ISA | 7844]

What do we do?

Based on our understanding of the entity's risk assessment process, evaluate whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity.

Why do we do this?

If an entity does not have a risk assessment process that is appropriate for its nature and complexity, it may lead to unidentified / unaddressed risks relevant to its financial reporting objectives, ineffectively designed control activities and an increase in the possibility of a misstatement in the financial statements.

Our understanding and evaluation of the entity's risk assessment process assists us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the audit

Not Integrated Audit | How do we evaluate whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity? [ISA | 7844.8501]

Based on our understanding of the entity's risk assessment process, we identify a CERAMIC control deficiency (refer to 'Evaluate the severity and assess the impact of CERAMIC control deficiencies' for additional information) if:

- there are unaddressed principles/elements or
- the entity's set of controls, processes and structures do not appropriately address the principle/element considering the nature and complexity of the entity

When there is at least one principle/element that is unaddressed or not appropriately addressed, we conclude that the entity's risk assessment process is not appropriate to the entity's circumstances considering the nature and complexity of the entity.

How may the Risk Assessment Process component for smaller, less complex entities be different? [ISA | 7844.2200]

In some less complex, smaller entities, and particularly owner-managed entities, an appropriate risk assessment may be performed through the direct involvement of management or the owner-manager (for example, the manager or owner-manager may routinely devote time to monitoring the activities of competitors and other developments in the market place to identify emerging business risks). The evidence of this risk assessment occurring in these types of entities is often not formally documented. However, discussions we have with management, corroborated, when appropriate, by e-mails or other correspondence between management and other personnel, may provide evidence that management is, in fact, performing risk assessment procedures appropriate to the nature and complexity of the entity.

What if we conclude that the entity's risk assessment process is not appropriate to the entity's circumstances considering the nature and complexity of the entity? [ISA | 7844.8504]

When we conclude that the entity's risk assessment process is not appropriate to the entity's circumstances considering the nature and complexity of the entity, we identify a financial statement level risk (see activity 'Evaluate RMs at the financial statement level' for additional information) and respond to the risk in line with activity'Design and implement overall responses'.

1.7 Not Integrated Audit | Understand the results of the entity's risk assessment process [ISA | 7845]

What do we do?

Obtain an understanding of the business risks relevant to financial reporting objectives identified and assessed by management and the actions taken to address those risks. IF we identify RMMs that arise from business risks that management failed to identify, THEN obtain an understanding of why the entity's risk assessment process failed to identify the business risk and determine whether this indicates a control deficiency(ies) within the entity's risk assessment process.

Why do we do this?

When we obtain an understanding of the Risk Assessment component of ICFR, we understand the results of the entity's risk assessment process, including the business risks relevant to financial reporting objectives identified and assessed by management and the actions taken to address those risks.

Identification by us of a business risk that management failed to identify may highlight possible deficiencies in the entity's Risk Assessment component.

Execute the audit

How do we understand the risks identified by management? [ISA | 7845.8525]

We consider the results of the procedures performed to obtain an understanding of the Risk Assessment component of ICFR, including:

- our understanding of the entity's processes that address the elements/principles in the Risk Assessment component; and
- our understanding of the results of the entity's risk assessment process.

This includes inquiries of management and those charged with governance and understanding the business risks identified as a result of the entity's risk assessment process.

What if we identify risks of material misstatement that arise from business risks that were not identified by the entity's risk assessment process? [ISA | 7845.8526]

If we identify risks of material misstatement that arise from business risks that were not identified by the entity, we perform the following:

- obtain an understanding of why the business risk was not identified by the entity's risk assessment process; and

- based on our understanding, determine whether this indicates a control deficiency(ies) within the entity's risk assessment process and consider the implications for our evaluation of the entity's risk assessment process.

What do we think about when determining whether the difference in our risk assessment and the entity's risk assessment is appropriate or an indication of a control deficiency? [ISA | 7845.8527]

As part of obtaining an understanding of why the business risk was not identified by the entity's risk assessment process, we think about whether there are differences or inconsistencies in the items below and the reasons for the difference:.

Materiality	If management have determined an overall financial statement materiality that is not equal to or lower than the materiality we have determined, this difference may indicate a deficiency in the entity's risk assessment process - particularly when management have determined materiality that is significantly higher than ours. We expect that the materiality determined by management will not be higher than materiality we determine. Since management's purpose for establishing materiality is similar to ours, we expect the amounts we each determine to also be similar.
Significant accounts, disclosures, assertions, RMMs or significant risks	Management assessment of a business risk relevant to financial reporting may differ from our assessment of a related risk of material misstatement. Potential differences in the assessment of business risks and the related risks of material misstatement includes: • the likelihood and potential magnitude of the risk (i.e., whether the RM is a RMM); • the significant accounts / disclosures and relevant assertions associated with the risk; and/or • the inherent risk for the risk. In these circumstances, we consider the reasons for the differences in management's assessment and ours and determine whether the inconsistency is indicative of a deficiency in the entity's risk assessment process.

Process risk points	When we are evaluating the design and implementation of process control activities or taking a controls approach, we may identify differences in process risk points identified by us as compared to management. If we have identified process risk points related to a risk of material misstatement that management have not, we think about whether this is an indication that there is a deficiency in the entity's risk assessment process. On the other hand, if management have identified process risk points that we have not identified as part of our risk assessment, we consider whether to identify these process risk points when we are taking a controls approach.

The items above may assist us in understanding why a risk was not identified by the entity and whether there is a deficiency in the entity's risk assessment process.

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

International Standards on Auditing: ISA 315.24

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

24.The auditor shall obtain an understanding of the entity's process for monitoring the system of internal control relevant to the preparation of the financial statements, through performing risk assessment procedures, by: (Ref: Para. A114-A115)	
(a) Understanding those aspects of the entity's process that address: (i) Ongoing and separate evaluations for monitoring the effectiveness of controls, and the identification and remediation of control deficiencies identified; (Ref: Para. A116.A117) and (ii) The entity's internal audit function, if any, including its nature, responsibilities and activities; (Ref: Para. A118)	and (c) Evaluating whether the entity's process for monitoring the system of internal control is appropriate to the entity's circumstances considering the nature and complexity of the entity. (Ref: Para. A121.A122)

(b) Understanding the sources of the information used in the entity's process to monitor the system of internal control, and the basis upon which management considers the information to be sufficiently reliable for the purpose; (Ref: Para. A119.A120)	

ISA Application and Other Explanatory Material: ISA 315.A96-A98 | ISA 315.A114-A122

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

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

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

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

A98. Because these components are foundational to the entity's system of internal control, any deficiencies in their operation could have pervasive effects on the preparation of the financial statements. Therefore, the auditor's understanding and evaluations of these components affect the auditor's identification and assessment of risks of material misstatement at the financial statement level, and may also affect the identification and assessment of risks of material misstatement at the assertion level. Risks of material misstatement at the financial statement level affect the auditor's design of overall responses, including, as explained in ISA 330, an influence on the nature, timing and extent of the auditor's further procedures.[35]

---

35 ISA 330, paragraphs A1-A3

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

Scalability

A114. In less complex entities, and in particular owner-manager entities, the auditor's understanding of the entity's process to monitor the system of internal control is often focused on how management or the owner-manager is directly involved in operations, as there may not be any other monitoring activities.

> **Example:**
>
> Management may receive complaints from customers about inaccuracies in their monthly statement that alerts the owner-manager to issues with the timing of when customer payments are being recognized in the accounting records.

A115. For entities where there is no formal process for monitoring the system of internal control, understanding the process to monitor the system of internal control may include understanding periodic reviews of management accounting information that are designed to contribute to how the entity prevents or detects misstatements.

Understanding the entity's process to monitor the system of internal control (Ref: Para. 24(a))

A116. Matters that may be relevant for the auditor to consider when understanding how the entity monitors its system of internal control include:

- The design of the monitoring activities, for example whether it is periodic or ongoing monitoring;
- The performance and frequency of the monitoring activities;
- The evaluation of the results of the monitoring activities, on a timely basis, to determine whether the controls have been effective; and
- How identified deficiencies have been addressed through appropriate remedial actions, including timely communication of such deficiencies to those responsible for taking remedial action.

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

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

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

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

A118. The auditor's inquiries of appropriate individuals within the internal audit function help the auditor obtain an understanding of the nature of the internal audit function's responsibilities. If the auditor determines that the function's responsibilities are related to the entity's financial reporting, the auditor may obtain further understanding of the activities performed, or to be performed, by the internal audit function by reviewing the internal audit function's audit plan for the period, if any, and discussing that plan with the appropriate individuals within the function. This understanding, together with the information obtained from the auditor's inquiries, may also provide information that is directly relevant to the auditor's identification and assessment of the risks of material misstatement. If, based on the

auditor's preliminary understanding of the internal audit function, the auditor expects to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed, ISA 610 (Revised 2013)[37] applies.

_____

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

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

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

A119. Management's monitoring activities may use information in communications from external parties such as customer complaints or regulator comments that may indicate problems or highlight areas in need of improvement.

Why the auditor is required to understand the sources of information used for the entity's monitoring of the system of internal control

A120. The auditor's understanding of the sources of information used by the entity in monitoring the entity's system of internal control, including whether the information used is relevant and reliable, assists the auditor in evaluating whether the entity's process to monitor the entity's system of internal control is appropriate. If management assumes that information used for monitoring is relevant and reliable without having a basis for that assumption, errors that may exist in the information could potentially lead management to draw incorrect conclusions from its monitoring activities.

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

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

A121. The auditor's evaluation about how the entity undertakes ongoing and separate evaluations for monitoring the effectiveness of controls assists the auditor in understanding whether the other components of the entity's system of internal control are present and functioning, and therefore assists with understanding the other components of the entity's system of internal control. This evaluation may also assist the auditor with identifying and assessing financial statement level and assertion level risks of material misstatement (see paragraph A86).

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

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

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Understand and evaluate monitoring activities [ISA | 1336]

What do we do?

Obtain an understanding of and evaluate the entity's monitoring activities.

Why do we do this?

Our understanding and evaluation of how the entity monitors the system of internal control relevant to the preparation of the financial statements assists us in understanding whether the other components of the entity's system of internal control are present and functioning, and therefore assists with understanding the other components of the entity's system of internal control. Our understanding and evaluation may also assist us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

What is a monitoring activity? [ISA | 1336.1300]

Monitoring activities help ascertain whether each of the components of internal control, including controls within each component, is present and functioning as intended.

Management's monitoring activities over internal controls involves assessing the effectiveness of internal control performance over time through ongoing activities, separate evaluations, or a combination of the two and taking necessary remedial actions.

Why are monitoring activities an important component of ICFR? [ISA | 1336.1400]

Using our house example, monitoring activities are similar to the roof of the house. They oversee and protect the other components.

Management's monitoring processes and controls continually check the other ICFR components to identify issues and determine what needs attention. Effective monitoring helps management identify necessary changes to the ICFR system to prevent or detect, on a timely basis, future errors in the financial statements.

The goal of monitoring is to determine both that the system of internal control operated and that it operated effectively.

Monitoring also includes evaluating the severity of identified deficiencies and communicating deficiencies to the appropriate parties.

Without effective monitoring, management do not have a basis to rely on their own ICFR.

Not Integrated Audit | How do we obtain an understanding of the entity's monitoring activities? [ISA | 1336.1700]

We obtain an understanding of the entity's process to monitor internal controls relevant to financial reporting by:

- understanding, through inquiry, the processes that address the following elements/principles:
  - how the entity selects, develops, and performs monitoring activities
  - how the entity addresses internal control deficiencies
- performing procedures to obtain an understanding of the CERAMIC components:
  - begin by performing inquiries
  - consider whether certain factors apply to determine whether to perform more than inquiry
  - If at least one of the factors apply, design additional procedures to obtain an understanding (i.e. observation and/or inspection)

- based on our understanding obtained, evaluating whether the entity's process for monitoring the system of internal control is appropriate to the entity's circumstances, considering the nature and complexity of the entity.

We also consider how information is being used in our procedures and determine the appropriate audit procedures to evaluate the reliability of the information used to obtain an understanding.

In addition, if the entity has an internal audit function, we obtain an understanding of the internal audit function as part of understanding the entity's monitoring activities (refer to the activity 'Obtain an understanding of the IA function'.)

If we identify a control deficiency in a CERAMIC component(s), we evaluate the severity of the control deficiency and assess the impact on our evaluation.

What do we do if there are unaddressed elements after we obtain an understanding of CERAMIC? [ISA | 1336.8653]

When those charged with governance are not separate from management, it is appropriate for the following elements to be unaddressed:

- Element 2 - Those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Element 11 - The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

In all other circumstances, if there are unaddressed elements after we have obtained an understanding of the CERAMIC component, we identify a control deficiency in the related CERAMIC component.

What are the two elements of the Monitoring component? [ISA | 1336.1800]

We consider the two elements outlined in the table below when obtaining an understanding of the Monitoring component of ICFR.

Elements of the Monitoring Component	Element 13: The organization selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Element 14: The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action.

How may the Monitoring component for less complex entities be different? [ISA | 1336.1900]

Although the same principles / elements underlying the Monitoring component apply for both small and large organizations; the entity's process to address the CERAMIC component is likely to differ.

In less complex entities, the entity's process to monitor the system of internal control may be accomplished by management's close involvement in the entity's operations and accounting / financial reporting. In these circumstances, monitoring activities are likely to include more ongoing activities that are built into the normal recurring activities of an entity, as opposed to separate evaluations or formal testing of controls by Internal Audit or a similar function.

> For example, management's close involvement in the entity's operations may involve regular and supervisory activities such as periodic reviews of the financial statement and related accounting information and/or a review of bank reconciliations, exception reports, or other information which has a role in monitoring the effectiveness of the underlying controls.

Through this close involvement, management may identify variances from expectations or inaccuracies in financial data, leading to the control being corrected. Further, management's actions and follow-up may also evidence how remedial actions are implemented.

Examples

1.1 Understand how the entity selects, develops, and performs monitoring activities [ISA | 1337]

Obtain an understanding of how the entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Our understanding about how the entity undertakes ongoing and separate evaluations for monitoring the effectiveness of controls assists us in understanding whether the other components of the entity's system of internal control are present and functioning, and therefore assists with understanding the other components of the entity's system of internal control. Our evaluation may also assist us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

What is Element 13 of the Monitoring component? [ISA | 1337.1300]

Element 13:

The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

This includes 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.

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

What are the points of focus related to Element 13? [ISA | 1337.1400]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us obtain an understanding of how they entity addresses the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus related to Element 13, along with questions that may help us obtain an understanding of how the entity addresses Element 13 and the related Monitoring component.

Points of focus	Questions
• Considers a mix of ongoing and separate evaluations • Considers rate of change • Establishes baseline understanding • Uses knowledgeable personnel • Integrates with business processes • Adjusts scope and frequency • Evaluates objectively	• Does the entity have a documented monitoring plan for all five components of ICFR? • Do the entity's monitoring activities consider a mix of ongoing and separate evaluations? • Is the appropriateness of that mix re-evaluated every year? • Do the monitoring procedures determine only that the control was performed, or that it was performed *effectively*? • How does the entity monitor the continuing effectiveness of controls in other CERAMIC components? • Does the entity use metrics or dashboards to monitor results/key control indicators within the organization? • Does management monitor the results of service providers? • How does the entity monitor controls over non-routine transactions? • How does management consider the information used in monitoring activities to be sufficiently reliable?

What might we think about when considering the entity's monitoring activities (Element 13)? [ISA | 1337.1500]

Management's monitoring activities involves assessing the effectiveness of internal control performance. When considering the monitoring activities that the entity uses to monitor internal controls, we think about:

- the design of the monitoring activities - i.e., whether ongoing activities, separate evaluations, or a combination of both are used
- the performance and frequency of the monitoring activities
- the points of focus related to this element.

In addition, management's monitoring activity may include using information from communications with external parties (e.g., customer complaints) and regulator comments (e.g., governing bodies, external

auditors, consultants) that may indicate problems or highlight areas where control deficiencies may exist.

In order to meet the objective of Element 13 and the related Monitoring component of ICFR, management's monitoring activities assess whether a control has been performed *effectively* (not just that a control has been performed). This concept helps us understand the monitoring activities that the entity uses to monitor internal controls relevant to financial reporting.

What are ongoing evaluations? [ISA | 1337.11873]

Ongoing evaluations are generally defined routine operations built into processes and performed in real time. Ongoing monitoring activities are often built into management's normal recurring activities (including regular management and supervisory activities) and provide information about the operation of controls.

Ongoing evaluations either monitor business performance or the effective operation of other controls to identify unusual trends that may indicate control deficiencies.

For example, an entity authorizes its accounts payable clerks to process contractor invoices with up to a 5% variance from amounts specified for services pursuant to executed contracts without seeking supervisory approval. The accounts payable manager monitors this control activity at the end of each month by reviewing disbursement activity and focusing specifically on two trends: the volume of disbursements where there are variances from contracts, and the frequency with which a particular clerk processes any variance payments. The accounts payable manager investigates any instance of an excessive variance or abnormal frequency or trend from both an operational and potential fraud perspective and takes action to assess and resolve root causes.

What are the benefits of ongoing evaluations? [ISA | 1337.11875]

There are a number of benefits associated with ongoing evaluations, including in particular:

- routine conduct and continuous operation of the ongoing evaluations as part of the entity's everyday business processes;
- focus on relationships and inconsistencies that are most important to management and other stakeholders; and
- real-time identification of issues allowing for a more timely response by management.

How do ongoing activities that monitor business performance provide information about the operation of controls? [ISA | 1337.12984]

Ongoing activities that monitor business performance establishes whether the entity's business performance (or that of its components) is meeting the objectives or expectations set by management or third parties. Such objectives or expectations can be expressed in the form of forecasts, budgets or prior-period normal results that serve as a benchmark for evaluating the current-period actual results.

Unexpected trends or outliers may be identified as a result of ongoing activities that monitor business performance that trigger management to investigate further. This may identify breakdowns in related controls

> An example of monitoring trends in business performance is observing key performance indicators - such as the allowance for doubtful accounts as a percentage of accounts receivable - and following up on unexpected trends.

While an unexpected trend in the allowance percentage may not be a result of a breakdown in internal controls, it represents a trigger for management to look more closely at their processes for:

- credit sales;
- accounts receivable collection; and
- allowance calculation.

Their investigation may identify breakdowns in relevant control activities in one or more of the processes above.

What are separate evaluations? [ISA | 1337.11876]

Objective management personnel, internal audit and/or external parties (and others) that periodically conduct separate evaluations to monitor the effectiveness of internal controls.

The techniques they use to perform separate evaluations are often similar to the techniques we use to independently evaluate the design and implementation of internal controls and test their operating effectiveness (when taking a controls reliance approach).

What are some different approaches to separate evaluations? [ISA | 1337.11877]

The different approaches for separate evaluations are set out below, each with differing degrees of objectivity and independence.

Approach	Description
Internal audit evaluations	Internal auditors are often objective and competent resources, whether in-house or outsourced, and perform separate evaluations either as part of their regular duties or at the specific request of senior management or those charged with governance.
Other objective evaluations	Such evaluations may be performed by other internal or external objective reviewers -e.g. compliance team, IT security specialists or consultants.
Cross-functional evaluations	This type of monitoring may be performed by personnel from different functions or departments that are independent of the process and controls being evaluated.
Benchmarking/peer evaluations	These evaluations compare or benchmark a component of internal control against the corresponding component within another entity or group of entities.

Self-assessments	Evaluations of the presence and functioning of controls performed by personnel responsible.

When might the different types of evaluations be more appropriate? [ISA | 1337.11878]

Different types of evaluations may be more appropriate in certain circumstances, for example:

Ongoing evaluation	Separate evaluation
Low risk in the execution of the control or in the related account or disclosure	Moderate or significant risk in the execution of the control or in the related account
Low judgment in executing the control	Moderate or significant judgment in executing the control
No history of errors in the related account	History of errors in the related account
No changes to the process or design of the control	Changes that may affect the way information is processed or the design of the control (e.g. an acquisition or changes in economic conditions)
No expectation from management for us to rely on the work of others relative to the control	An expectation for us to rely on the work of others relative to this control

Does an entity have monitoring activities over processes and controls performed by external service providers? [ISA | 1337.11882]

Yes. As a general rule, although management may outsource a process to an external service provider, they may *not* outsource their responsibility for the results of the service provider's work.

When the entity uses external service providers, management still monitors whether control activities performed by those service providers have been appropriately designed and implemented and are operating effectively.

Such monitoring may be accomplished by performing:

- periodic evaluations (e.g. by reviewing a Service Organization Control (SOC) 1 - Type II report if such a report is available for the service provider or by directly testing controls in place at the service organization); or
- ongoing evaluations (e.g. reviewing output provided by the service organization for outliers that may indicate its controls have not been appropriately designed or are not operating effectively).

How are monitoring activities different from process control activities? [ISA | 1337.1800]

The key difference between process control activities and monitoring activities relates to their objective and their relationship to the risk of material misstatement of an entity's financial statements.

With process control activities, that relationship is direct: each process control activity's objective is to mitigate a specific risk within a business process that could lead to a material misstatement of the entity's financial statements. We call that risk a process risk point (PRP).

Accordingly, process control activities are designed and operated with a level of precision that allows both management and external auditors to be confident that they would prevent or detect, in a timely manner, a material misstatement to the entity's financial statements.

On the other hand, monitoring activities have only an indirect relationship to the risk of misstatement (RM) of an entity's financial statements. They do not themselves mitigate risks to specific financial statement assertions. Instead, they monitor the continuing appropriateness of the design and operating effectiveness of control activities and controls within other components of ICFR (Control Environment, Risk Assessment, Control Activities, and Information and Communication).

The objective of monitoring activities is to:

- timely identify deficiencies in controls;
- analyze their root causes; and
- design and implement effective remediation plans.

For example, the intent of a monthly completeness control activity would be to detect and correct errors; whereas a monitoring activity would ask why there were errors in the first place and assign management the responsibility of fixing the process to prevent future errors.

Monitoring activities *could* identify a misstatement in the entity's financial statements. But they're more likely to identify instances where control activities did not operate effectively, and where further investigation as to the propriety of financial reporting may be necessary.

When it comes to mitigating the RMMs of an entity's financial statements, the difference in the level of assurance provided by process control activities ('would' level) and monitoring activities ('could' level) has implications for how we rely on their assessment of the entity's ICFR.

Process Control activities	Monitoring activities
• Respond to specific risks (PRPs) at the process level	• Monitor the effective operation of control activities and other components of ICFR • Monitor operations to identify unusual trends or anomalies that may warrant investigation
• Designed with sufficient precision to prevent, or detect and correct errors in financial statement assertions at the 'would' level of assurance	• Could identify errors themselves, but that is not the objective of their design • Designed to identify the cause of errors • Monitor the remediation of deficiencies

What is 'would' level? [ISA | 1337.11885]

We have coined the phrase 'would-level' because the standards require reasonable assurance that a control *would* prevent, or detect and correct, a material misstatement on a timely basis.

'Would' in this context means 'probable'. For a control to function properly as a process control activity, it needs to operate in a manner that allows us to confidently say it would - i.e. probably will - prevent or detect a material misstatement.

What is 'could' level? [ISA | 1337.11886]

We have coined the phrase 'could-level' to refer to an activity that doesn't meet the 'would' level of assurance. The activity *could* or *may* or *might* prevent or detect a material misstatement in the entity's financial statements, but it doesn't meet the 'would' or probable level.

Monitoring activities typically function at the 'could' level. They are often reviews of consolidated information at the culmination of the process. So they are appropriate to help determine whether further investigation may be warranted, but do not directly address the assertion-level risks (and therefore are not likely to mitigate the severity of a deficiency unless it is combined with a process control activity that is operating effectively-i.e., while the original process control activity is found deficient, the monitoring activity identified that it was not operating as intended, communicated it to management timely, and management put in place an additional process control activity that addressed the same risk that the deficient control intended to mitigate).

What is a flux analysis? [ISA | 1337.11887]

A flux analysis is a monitoring activity whereby management understand and investigate changes in account balances within the balance sheet and income statement across two periods.

A flux analysis may compare:

- actual account balances for the current period to actual account balances from the prior period (e.g. actual results from the current month to the previous month); or
- account balances for the current period to a budget or forecast (e.g. actual results from the current month to the budget for the month).

Can a flux analysis be a process control activity? [ISA | 1337.11888]

Typically, a flux analysis is a monitoring activity as it usually has a different objective and is not designed at a sufficient level of precision necessary to be a process control activity.

If the flux analysis directly addresses a process risk point and is designed at a level of precision that would prevent or detect a material misstatement, it is a process control activity - but it could also be a monitoring activity if it monitors the effectiveness of other controls. This is rare as it is difficult to design a flux analysis to be a process control activity and we take caution when management asserts that it does.

Can a control be both a monitoring activity and a control activity? [ISA | 1337.11891]

Yes. A monitoring activity may be designed to serve as an ongoing evaluation that identifies other process control activities within an entity's business processes that did not operate effectively, and where further investigation may be necessary and also designed to address a PRP with sufficient precision to prevent, or detect and correct errors in financial statement assertions at the 'would' level of assurance.

In these instances, we treat the monitoring activity as a process control activity and link it to the PRPs that it addresses.

1.2 Understand how the entity addresses internal control deficiencies [ISA | 1338]

What do we do?

Obtain an understanding of how the entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action

Why do we do this?

Our understanding and evaluation about how the entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action assists us in understanding whether the other components of the entity's system of internal control are present and functioning, and therefore assists with understanding the other components of the entity's system of internal control. Our understanding and evaluation may also assist us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

What is Element 14 of the Monitoring component? [ISA | 1338.1300]

Element 14:

The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

What are the points of focus related to Element 14? [ISA | 1338.1400]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us obtain an understanding of how the entity addresses the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus related to Element 14, along with the questions that may help us obtain an understanding of how the entity addresses Element 14 and the related Monitoring component.

Points of focus	Questions
• Monitors corrective actions	• Does the entity have a process to develop, monitor and report corrective actions taken in response to the identified deficiencies? • How does management assess the results of the monitoring activities, including the identification and evaluation of control deficiencies? • How are appropriate remedial actions developed to address identified deficiencies?

	• How are the deficiencies and remedial actions communicated to those responsible for taking remedial actions and whether those communications are made timely? • How does management monitor whether the remedial actions take place?

What is a control deficiency? [ISA | 1338.1500]

A deficiency in internal control exists when the design or operation of that control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements in a timely manner.

When a control deficiency exists, a control is:

(1) missing;
(2) designed inappropriately; or
(3) operating ineffectively.

In the context of our audit, we may identify control deficiencies when:

(1) obtaining an understanding of the entity's ICFR as part of our risk assessment;
(2) testing the operating effectiveness of control activities as part of our response to an RMM or in an audit of ICFR; or
(3) evaluating whether misstatements that been detected through our substantive procedures indicate that controls are not operating effectively.

Additionally, management may bring other deficiencies to our attention as a result of the entity's monitoring activities.

How does an entity identify and evaluate a control deficiency? [ISA | 1338.1600]

An entity typically has a process to identify and evaluate a control deficiency as part of assessing the results of its monitoring activities. This process will vary depending on the entity's circumstances; however, it will probably contain a variation of the following steps:

- Determine whether a deficiency in ICFR exist
- Perform a root cause analysis of the deficiency
- Determine whether the deficiency is indicative of other deficiencies
- Evaluate the severity of the deficiency individually
- Evaluate the effect of compensating controls, if applicable
- Evaluate the severity of similar deficiencies in aggregate

The results of the entity's process of identifying and evaluating a control deficiency assists in the development and initiation of remedial actions.

How does an entity initiate corrective actions necessary to remediate control deficiencies? [ISA | 1338.1800]

Once an entity has identified a control deficiency, they put processes in place to initiate remedial actions, including:

(1) determine what corrective actions are necessary to remediate the control deficiency (considering the results of its evaluation of the control deficiency);
(2) communicate the deficiency and corrective actions to those responsible for the remediation; and

(3) monitor whether the corrective actions have taken place in a timely manner.

Typically, the individuals responsible for monitoring whether corrective actions have taken place in a timely manner will be different from the individuals responsible for determining the corrective actions and/or implementing them.

What if corrective actions don't take place in a timely manner? [ISA | 1338.1601]

We expect entities to have activities, policies, procedures and processes in place to escalate corrective actions that have not taken place in a timely manner at least one level above the individual responsible for implementing those actions. Management also discusses the remediation status of significant deficiencies with those charged with governance.

When corrective actions have not taken place in a timely manner, the entity may put additional monitoring activities in place until the corrective actions have been implemented.

Further, Element 5 of the Control Environment component of ICFR includes that the entity holds individuals accountable for their internal control responsibilities, which includes responsibilities related to corrective actions necessary to remediate control deficiencies.

Examples

1.3 Not Integrated Audit | Perform procedures to obtain an understanding of the CERAMIC components [ISA | 7843]

What do we do?

Perform procedures to obtain an understanding of the CERAMIC components

Why do we do this?

We perform procedures to obtain an understanding of the CERAMIC components as part of our risk assessment to support our identification and assessment of risks of material misstatement (RMMs).

Execute the audit

What type of procedures do we perform to obtain an understanding of the CERAMIC components? [ISA | 7843.8495]

We begin by performing inquiries to obtain an understanding of the CERAMIC components. However, inquiry alone may not be sufficient to obtain the necessary understanding of the components when certain factors exist. We consider whether certain factors apply to determine whether to perform more than inquiry.

What factors do we consider when determining whether to perform more than inquiry in order to obtain an understanding of CERAMIC? [ISA | 7843.8496]

We consider the factors in the table below. When certain circumstances exist, there is a rebuttable presumption that we will perform more than inquiry in order to obtain an understanding over one or more of the CERAMIC components.

Factor	Impact on nature, timing, and extent of procedures
Size and complexity of the entity	The larger and more complex an entity, the more robust and comprehensive its set of controls, processes, structures, and communications necessary to address the elements/principles within each CERAMIC component. As such, for a large and/or complex entity, it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Conversely, less complex entities require simpler set of controls, processes, structures, and communications to achieve their objectives. For example, the entity may develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication rather than have a written code of code. Due the simplicity of their processes, inquiry alone may be sufficient to obtain an understanding of the entity's CERAMIC. The size of an entity (e.g. number of employees) may be an indicator of its complexity. However, some smaller entities may be complex, and some larger entities may be less complex. Refer to 'What characteristics of the entity do we think about to assess its complexity?' for additional information.
Our existing knowledge of the entity's system of internal control	When we have less knowledge of the entity's system of internal control (e.g. we are performing an initial audit), it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC.
Reliance on the entity's control activities	It is presumed that inquiry alone is not sufficient to obtain an understanding of CERAMIC when we plan to place reliance on the entity's control activities to reduce our control risk.
Nature and extent of changes in entity's systems and operations	Where there have been extensive changes in the entity's systems (e.g. new IT system implementation) and/or operations (e.g. product line or geographic expansion, significant changes in management or personnel) from the prior year, the entity's system of internal control may have significantly changed such that it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC.

	Inquiry alone may also not be sufficient when changes to the entity's CERAMIC have occurred to remediate prior year deficiencies.

What if we conclude that it is appropriate to rebut the presumption that 'inquiry alone is not sufficient'? [ISA | 7843.8497]

When we conclude that rebutting the presumption that 'inquiry alone is not sufficient' is appropriate in the circumstances of the engagement, and accordingly have only obtained an understanding of CERAMIC through inquiry, we document the reasons for that conclusion.

What characteristics influence the complexity of an entity? [ISA | 7843.8498]

The characteristics below influence the complexity of an entity. No one characteristic is more indicative than another of an entity's complexity. The presence of one characteristic that indicates 'more complexity' does not necessarily indicate a 'more complex' entity. We collectively think about all the characteristics when considering the factor 'size and complexity of the entity.'

Factor	Impact on nature, timing, and extent of procedures
Size and complexity of the entity	More robust and comprehensive sets of controls, processes, structures, and communications are necessary at larger and more complex entities to address the elements/principles within each CERAMIC component. As such, for a large and/or complex entity, it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Conversely, less complex entities require a simpler set of controls, processes, structures, and communications to achieve their objectives. For example, the entity may develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication rather than have a written code of code. Due the simplicity of their processes, inquiry alone may be sufficient to obtain an understanding of the entity's CERAMIC. The size of an entity (e.g. number of employees) may be an indicator of its complexity. However, some smaller entities may be complex, and some larger entities may be less complex. Refer to 'What characteristics influence the complexity of an entity ?' for additional information.
Our existing knowledge of the entity's system of internal control	When we have less knowledge of the entity's system of internal control (e.g. we are performing an initial audit), it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC.

Reliance on the entity's control activities	It is presumed that inquiry alone is not sufficient to obtain an understanding of CERAMIC when we plan to place reliance on the entity's control activities to reduce our control risk.	
Nature and extent of changes in entity's systems and operations	Where there have been extensive changes in the entity's systems (e.g. new IT system implementation) and/or operations (e.g. product line or geographic expansion, significant changes in management or personnel) from the prior year, the entity's system of internal control may have significantly changed such that it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Inquiry alone may also not be sufficient when changes to the entity's CERAMIC have occurred to remediate prior year deficiencies.	
Characteristics	Examples of less complexity	Examples of more complexity
Organizational structure and management personnel	An entity has few business segments or lines of business with a small management team and no internal audit.	An entity has several business segments or lines of business with multiple levels of management and a sophisticated internal audit department.
Ownership and governance structure	An owner-manager is responsible for the governance and direct oversight of the operations and accounting / financial reporting for the entity.	The entity is publicly traded, and those charged with governance operate independently of management.
Operating characteristics	The entity is a single legal entity with operations in only a few geographic locations.	The entity is a group that has many components that operate in several markets and geographic locations and are decentralized.
Nature of assets, liabilities and transactions	The entity processes routine transactions and the accounts do not require	The entity processes non-routine or unusual transactions, including in

	complex accounting or significant judgments.	controversial or emerging areas, and the accounts require complex accounting or significant judgments.
Nature of the accounting processes and controls	The entity has simple record-keeping with few accounting processes with primarily manual control activities performed by a few people.	The entity has many IT systems (or many instances of a single system) and customizes the systems for the entity's specific needs.
IT systems	The entity has few IT systems and the entity uses pre-packaged purchased applications that are not able to be customized by the entity.	The entity has many IT systems (or many instances of a single system) and customizes the systems for the entity's specific needs.

1.4 Evaluate the entity's monitoring activities [ISA | 7880]

What do we do?

Evaluate whether the entity's process for monitoring the system of internal control is appropriate to the entity's circumstances considering the nature and complexity of the entity based on our understanding of the entity's monitoring activities

Why do we do this?

Our evaluation about how the entity monitoring the effectiveness of controls assists us in understanding whether the other components of the entity's system of internal control are present and functioning, and therefore assists with understanding the other components of the entity's system of internal control. Our evaluation may also assist us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the audit

Not Integrated Audit | How do we evaluate whether the entity's circumstances considering the nature and complexity of the entity? [ISA | 7880.8556]

Based on our understanding of the entity's monitoring activities, we identify a CERAMIC control deficiency (refer to 'Evaluate the severity and assess the impact of CERAMIC control deficiencies' for additional information) if:

- there are unaddressed principles/elements or
- the entity's set of controls, processes and structures do not appropriately address the principle/element considering the nature and complexity of the entity

When there is at least one principle/element that is unaddressed or not appropriately addressed, we conclude that the entity's monitoring activities is not appropriate to the entity's circumstances considering the nature and complexity of the entity.

How may the Monitoring component for less complex entities be different? [ISA | 7880.1900]

Although the same principles / elements underlying the Monitoring component apply for both small and large organizations; the entity's process to address the CERAMIC component is likely to differ.

In less complex entities, the entity's process to monitor the system of internal control may be accomplished by management's close involvement in the entity's operations and accounting / financial reporting. In these circumstances, monitoring activities are likely to include more ongoing activities that are built into the normal recurring activities of an entity, as opposed to separate evaluations or formal testing of controls by Internal Audit or a similar function.

> For example, management's close involvement in the entity's operations may involve regular and supervisory activities such as periodic reviews of the financial statement and related accounting information and/or a review of bank reconciliations, exception reports, or other information which has a role in monitoring the effectiveness of the underlying controls.

Through this close involvement, management may identify variances from expectations or inaccuracies in financial data, leading to the control being corrected. Further, management's actions and follow-up may also evidence how remedial actions are implemented.

What if we conclude that the entity's process for monitoring the system of internal control is not appropriate to the entity's circumstances considering the nature and complexity of the entity? [ISA | 7880.8559]

When we conclude that the entity's process for monitoring the system of internal control is not appropriate to the entity's circumstances considering the nature and complexity of the entity, we identify a financial statement level risk (see activity 'Evaluate RMs at the financial statement level' for additional information) and respond to the risk in line with activity 'Design and implement overall responses'.

1.5 Not Integrated Audit | Internal Audit | Obtain an understanding of the IA function [ISA | 1126]

What do we do?

IF the entity has an internal audit function THEN obtain an understanding of the function, including by performing inquiries and other procedures

Why do we do this?

When an entity has an internal audit (IA) function, we obtain an understanding of the function and its activities. This understanding helps us:

- identify those activities that are relevant to planning the audit; and

- conclude whether we will use the IA function's work.

Understanding the function's role in monitoring of internal control over financial reporting (ICFR) in particular helps us understand the entity's monitoring activities. It may also provide information that is directly relevant to our identification and assessment of the risks of material misstatement (RMMs).

Execute the Audit

What is an IA function? [ISA | 1126.1300]

An entity's IA function performs assurance and consulting activities to management and those charged with governance that are designed to evaluate and improve the effectiveness of the entity's governance, risk management and internal control processes.

Many public entities have an IA function, often comprising one or more people who perform internal auditing activities within an entity. In some cases, other functions within an entity perform these or similar activities. In other cases, employees may be called 'internal auditors' but do not perform the internal auditing activities described in this chapter. These others are acting in the capacity of the IA function and are assessed in the similar fashion.

Do we obtain an understanding of the IA function, when the function is outsourced to a third-party service provider? [ISA | 1126.1400]

Yes. The function's title and whether the activities are performed by the entity or a third-party service provider do not solely determine whether we can use the function's work. Rather, we consider the nature of the activities and the IA function's competence, objectivity, and whether they apply a systematic and disciplined approach.

In this chapter, references to the work of the IA function include relevant activities of other functions or third-party service providers.

What IA responsibilities and activities are 'relevant to planning the audit'? [ISA | 1126.1500]

The IA responsibilities and activities are relevant to planning the audit when they relate to the entity's financial reporting. When their responsibilities and activities are relevant, we may be able to use the IA function's work to modify the nature or timing of audit procedures we will perform directly, or to reduce their extent.

The IA function can have several responsibilities, some that are relevant to our audit and some that are not. As we obtain our understanding of the IA function, it is helpful for us to focus on those activities that are relevant to our audit.

The table below sets out examples of common IA function responsibilities and activities that may be relevant to our audit.

Work performed by the IA function	Description
Evaluation of internal control	Evaluate the design and implementation of controls, their operation and recommend improvements.

	For example, the IA function may plan and perform tests or other procedures to provide assurance to management and those charged with governance regarding the design, implementation and operating effectiveness of internal control, including those that are relevant to the audit (i.e. ICFR).
Examination of financial and operating information	Review the means used to identify, recognize, measure, classify and report financial and operating information, and to make specific inquiries into individual items, including detailed testing of transactions, balances and procedures.
Review of compliance with laws and regulations	Review compliance with laws, regulations and other external requirements, and with management policies and directives and other internal requirements.
Perform risk management procedures	Identify and evaluate significant exposures to risk and contribute to the improvement of risk management and internal control. Perform procedures to help the entity to detect fraud.
Assess the governance process	Assess whether the governance process meets the entity's objectives for: • ethics and values; • performance management and accountability; • effectively communicating risk and control information to appropriate areas of the entity; and • effective communication among those charged with governance, external and internal auditors, and management.

How do we assess whether IA activities are relevant to planning the audit? [ISA | 1126.1600]

Examples of procedures that may help with our assessment include:

- considering knowledge from prior-year audits;
- reviewing how the internal auditors allocate their audit resources to financial or operating areas in response to their risk-assessment process; and
- obtaining detailed information about the scope of IA activities by reading IA reports, the IA function's charter and the IA function's organizational chart.

How do we obtain our understanding of the IA function? [ISA | 1126.1700]

We obtain our understanding of the IA function by performing inquiries. To supplement the inquiries, we may also obtain our understanding by performing other procedures, such as:

- reading the internal audit charter or terms of reference;

- reviewing the internal audit function's audit plan for the period and discussing that plan with appropriate individuals;
- reading internal audit reports or other documents outlining the work performed; and
- reading other documents outlining the work performed by the IA function.

Do we perform inquiries even when we don't intend to use the IA function's work? [ISA | 1126.10469]

Yes. The IA function has likely obtained insight into the entity's operations and risks, and may have findings based on its work -- e.g. control deficiencies, identified risks. These findings may help us understand the entity, assess risk or perform other aspects of the audit. So we make our inquiries whether or not we intend to use the IA function's work.

Do we read IA reports when obtaining an understanding of the IA function? [ISA | 1126.10470]

We may decide to read internal audit reports when:

- our inquiries reveal findings that may be relevant to the entity's financial reporting and our audit, or
- they may provide us more information about the IA function.

Reading reports prepared for management or those charged with governance may help us conduct several areas of our audit, including:

- obtaining detailed information about the scope of IA activities;
- uncovering matters that may inform our risk assessment;
- identifying previously unknown control deficiencies;
- identifying instances of non-compliance with laws and regulations;
- detecting instances of fraud; and
- providing evidence that helps us evaluate the results of the IA function's work.

Who do we inquire of when obtaining an understanding of the IA function? [ISA | 1126.1800]

We inquire of individuals who have appropriate knowledge, experience and authority - e.g. the head of the IA function, appropriate management and other IA staff. When the entity's governance structure includes an audit committee, we may also inquire of its chair and/or members.

What do we inquire about when obtaining an understanding of the IA function? [ISA | 1126.1900]

The table below sets out areas we inquire about as we obtain our understanding of the IA function and highlights the purpose of these inquiries.

Area of inquiry	Purpose
The organizational status of the IA function within the entity	Depending on the organizational status of the IA function, the function may be more or less effective. For example, the function may be considered as less effective or even ineffective if it reports to management because this may affect the IA function's objectivity.

The IA function's nature of responsibilities	Learning about the nature of the IA function's responsibilities helps us determine whether the IA function's work is relevant to the audit. For example, the IA function may focus on economic efficiency and operational effectiveness. These responsibilities do not necessarily relate to the entity's financial reporting and so they may not be relevant to the audit.
The IA function's application of internal audit professional standards	Internal audit professional standards (e.g. standards issued by the International Internal Audit Standards Board, Institute of Internal Auditors and General Accounting Office) aim to: • impart an understanding of the role and responsibilities of the IA function; • permit measurement of the IA function's performance; and • improve the practice and quality of internal audit's work.
The IA function's audit plan, including the nature, timing and extent of their work	An IA plan may provide insights about, among other things, the IA function's areas of focus, how much time was allocated to the work, and who performed it. This helps us to understand whether the work may be relevant to our audit and form initial views about how it could be used to modify our audit procedures.
The IA function's access to records and whether there are limits on the scope for their activities	Limits imposed by management or those charged with governance on the IA function's access to documents and other sources of information relevant to its activities and/or on the function's scope may indicate that the function is less effective.

When do we make inquiries to gain an understanding of the IA function? [ISA | 1126.2000]

We make inquiries to gain an understanding of the IA function during risk assessment and audit planning. We update this understanding throughout the audit.

How can the IA function's work help us in our audit? [ISA | 1126.2100]

The IA function's work can provide information about the entity that is helpful during risk assessment and audit planning. In some cases, their work may allow us to modify the nature or timing of audit procedures we perform, or reduce their extent.

The table below sets out examples of how the work of the IA function may affect our audit approach.

IA function's work	Impact on our approach

Preparation of reports detailing work they have performed	Reviewing these reports may help us identify matters that could influence our risk assessment and audit plan
Review, assess and monitor controls	When we use the procedures performed by the internal auditors in this area, we may gain useful information about the entity's internal controls and possibly reduce the nature, timing, and/or extent of the procedures necessarily to test controls
Flowcharting procedures performed by entity	Reviewing these flowcharts may provide us with information about the entity's business processes and the design of relevant controls
Work performed over a number of locations	We may be able to reduce the number of locations where we perform audit procedures

The information system and communication

International Standards on Auditing: ISA 315.25

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

The information system and communication

25. The auditor shall obtain an understanding of the entity's information system and communication relevant to the preparation of the financial statements, through performing risk assessment procedures, by: (Ref: Para. A131)	
(a) Understanding the entity's information processing activities, including its data and information, the resources to be used in such activities and the policies that define, for significant classes of transactions, account balances and disclosures: (Ref: Para. A132.A143) (i) How information flows through the entity's information system, including how: a. Transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger and	and (c) Evaluating whether the entity's information system and communication appropriately support the preparation of the entity's financial statements in accordance with the applicable financial reporting framework. (Ref: Para. A146)

reported in the financial statements; and b. Information about events and conditions, other than transactions, is captured, processed and disclosed in the financial statements; (ii) The accounting records, specific accounts in the financial statements and other supporting records relating to the flows of information in the information system; (iii) The financial reporting process used to prepare the entity's financial statements, including disclosures; and (iv) The entity's resources, including the IT environment, relevant to (a)(i) to (a)(iii) above; (b) Understanding how the entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control: (Ref: Para. A144.A145) (i) Between people within the entity, including how financial reporting roles and responsibilities are communicated; (ii) Between management and those charged with governance; and (iii) With external parties, such as those with regulatory authorities;	

ISA Application and Other Explanatory Material: ISA 315.A123-A146

Information System and Communication, and Control Activities (Ref: Para. 25.26)

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

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

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

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

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

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

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

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

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

accordance with paragraph 33) may also only be identifiable once the auditor's inherent risk assessments have been undertaken.

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

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

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

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

Scalability

A131. The information system, and related business processes, in less complex entities are likely to be less sophisticated than in larger entities, and are likely to involve a less complex IT environment; however, the role of the information system is just as important. Less complex entities with direct management involvement may not need extensive descriptions of accounting procedures, sophisticated accounting records, or written policies. Understanding the relevant aspects of the entity's information system may therefore require less effort in an audit of a less complex entity, and may involve a greater amount of inquiry than observation or inspection of documentation. The need to obtain an understanding, however, remains important to provide a basis for the design of further audit procedures in accordance with ISA 330 and may further assist the auditor in identifying or assessing risks of material misstatement (see paragraph A86).

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

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

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

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

A134. Matters the auditor may consider when understanding the policies that define the flows of information relating to the entity's significant classes of transactions, account balances, and disclosures in the information system and communication component include the nature of:

(a) The data or information relating to transactions, other events and conditions to be processed;

(b) The information processing to maintain the integrity of that data or information; and

(c) The information processes, personnel and other resources used in the information processing process.

A135. Obtaining an understanding of the entity's business processes, which include how transactions are originated, assists the auditor in obtaining an understanding of the entity's information system in a manner that is appropriate to the entity's circumstances.

A136. The auditor's understanding of the information system may be obtained in various ways and may include:

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

Automated tools and techniques

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

Information obtained from outside of the general and subsidiary ledgers

A138. Financial statements may contain information that is obtained from outside of the general and subsidiary ledgers. Examples of such information that the auditor may consider include:

- Information obtained from lease agreements relevant to disclosures in the financial statements.
- Information disclosed in the financial statements that is produced by an entity's risk management system.
- Fair value information produced by management's experts and disclosed in the financial statements.
- Information disclosed in the financial statements that has been obtained from models, or from other calculations used to develop accounting estimates recognized or disclosed in the financial statements, including information relating to the underlying data and assumptions used in those models, such as:
  - Assumptions developed internally that may affect an asset's useful life; or

  - Data such as interest rates that are affected by factors outside the control of the entity.

- Information disclosed in the financial statements about sensitivity analyses derived from financial models that demonstrates that management has considered alternative assumptions.
- Information recognized or disclosed in the financial statements that has been obtained from an entity's tax returns and records.
- Information disclosed in the financial statements that has been obtained from analyses prepared to support management's assessment of the entity's ability to continue as a going concern, such as disclosures, if any, related to events or conditions that have been identified that may cast significant doubt on the entity's ability to continue as a going concern.[38]

38 ISA 570 (Revised), paragraphs 19.20

A139. Certain amounts or disclosures in the entity's financial statements (such as disclosures about credit risk, liquidity risk, and market risk) may be based on information obtained from the entity's risk management system. However, the auditor is not required to understand all aspects of the risk management system, and uses professional judgment in determining the necessary understanding.

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

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

A140. The auditor's understanding of the information system includes the IT environment relevant to the flows of transactions and processing of information in the entity's information system because the entity's use of IT applications or other aspects in the IT environment may give rise to risks arising from the use of IT.

A141. The understanding of the entity's business model and how it integrates the use of IT may also provide useful context to the nature and extent of IT expected in the information system.

Understanding the entity's use of IT

A142. The auditor's understanding of the IT environment may focus on identifying, and understanding the nature and number of, the specific IT applications and other aspects of the IT environment that are relevant to the flows of transactions and processing of information in the information system. Changes in the flow of transactions, or information within the information system may result from program changes to IT applications, or direct changes to data in databases involved in processing, or storing those transactions or information.

A143. The auditor may identify the IT applications and supporting IT infrastructure concurrently with the auditor's understanding of how information relating to significant classes of transactions, account balances and disclosures flows into, through and out the entity's information system.

Obtaining an understanding of the entity's communication (Ref: Para. 25(b))

Scalability

A144. In larger, more complex entities, information the auditor may consider when understanding the entity's communication may come from policy manuals and financial reporting manuals.

A145. In less complex entities, communication may be less structured (e.g., formal manuals may not be used) due to fewer levels of responsibility and management's greater visibility and availability. Regardless of the size of the entity, open communication channels facilitate the reporting of exceptions and acting on them.

Evaluating whether the relevant aspects of the information system support the preparation of the entity's financial statements (Ref: Para. 25(c))

A146. The auditor's evaluation of whether the entity's information system and communication appropriately supports the preparation of the financial statements is based on the understanding obtained in paragraphs 25(a).(b).

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Understand and evaluate information and communication [ISA | 1323]

What do we do?

Obtain an understanding of the information system relevant to financial reporting and how the entity communicates roles and responsibilities and significant matters relating to financial reporting and evaluate whether the entity's information system and communication appropriately support the preparation of the entity's financial statements in accordance with the applicable financial reporting framework.

Why do we do this?

We understand the entity's information system and communication because understanding the entity's policies that define the flows of transactions and other aspects of the entity's information processing activities relevant to the preparation of the financial statements, and evaluating whether the component appropriately supports the preparation of the entity's financial statements, supports our identification and assessment of risks of material misstatement at the assertion level.

This understanding and evaluation may also result in the identification of risks of material misstatement at the financial statement level when the results of our 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.

Execute the Audit

What is information and communication? [ISA | 1323.1300]

> The scope of the Information and Communication component of ICFR is broad. It generally comprises people, business processes, activities, transactions, information/data elements and IT.
>
> The information system may be located at the entity, its service organizations or both. It is used to generate relevant, quality information to execute the entity's business objectives - e.g. to produce and sell its products and services and measure its performance - and financial reporting objectives.

Communication, both internal and external, delivers the information the entity needs to carry out day-to-day controls. Communication also helps staff understand their internal control responsibilities and how they help achieve the entity's objectives.

Our understanding of information focuses on the aspects of an entity's information system relevant to financial reporting and ICFR. Even with that narrow focus, this often includes obtaining an understanding of how information flows from:

- the initiation and authorization of individual transactions;
- the occurrence of other events and conditions relevant to financial reporting; and
- how those transactions and other events and conditions are reported in the financial statements and related disclosures within the financial statements.

How do we obtain an understanding of the Information and Communication component? [ISA | 1323.1500]

We obtain an understanding of the information and communication component by:

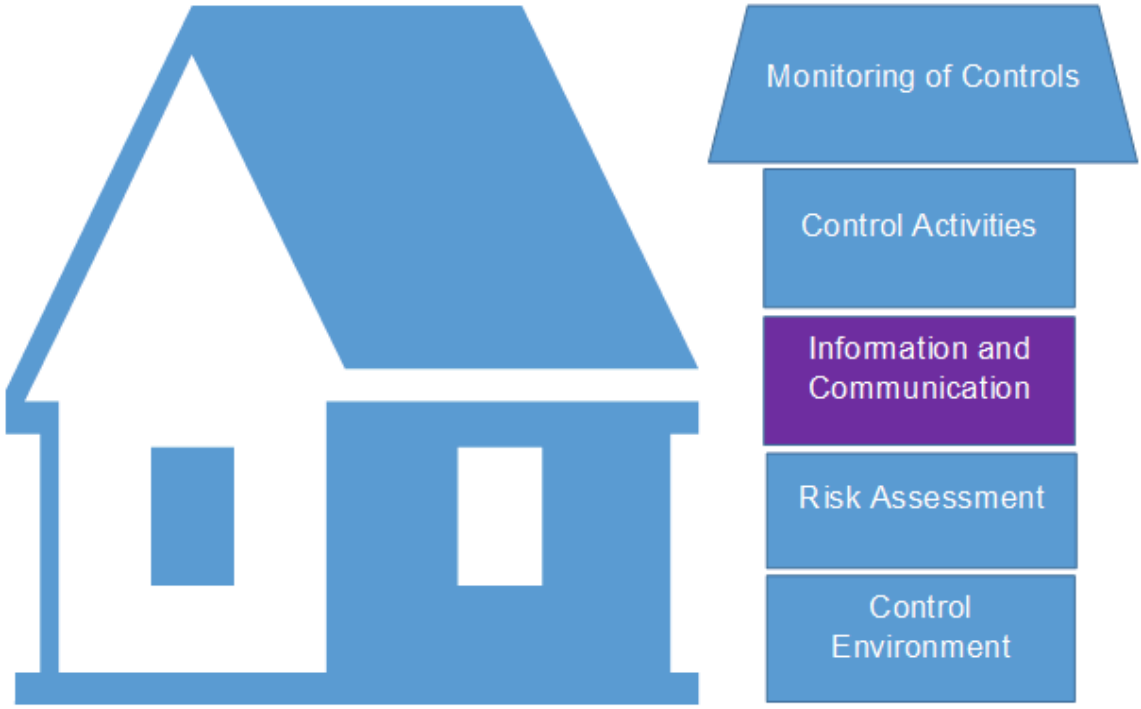
- understanding and evaluating information; and
- understanding and evaluating communication

We also consider how information is being used in our procedures and determine the appropriate audit procedures to evaluate the reliability of the informationused to obtain an understanding.

Why is the Information and Communication component important to ICFR? [ISA | 1323.1400]

An entity's ICFR uses information and communication to achieve its ICFR objectives across all of the ICFR components. If we recall our house example, information and communication are the walls and pipes of the house. Information and communication touch all of the components and act as a conduit for interaction between the components and throughout the entity.

The entity's ICFR could be ineffective if control operators don't receive complete, accurate, appropriate and timely information from both external and internal sources.



Because communication is so pervasive to the entity's overall ICFR, deficiencies can also have implications for our audit approach. For example, if an entity has written accounting policies but does not communicate them consistently across employees, individuals responsible for financial reporting may not appropriately account for transactions in accordance with the applicable financial reporting framework.

As auditors, if we are aware of this deficiency, it is likely to affect our risk assessment - especially as it relates to our identification of RMMs.

Similarly, if the entity does not have processes and controls in place to facilitate communication between its legal and accounting departments about a legal contingency, a higher risk of material misstatement might exist in this area. So, we may plan to respond to it.

Without obtaining an understanding of the entity's communication processes and controls, we may not have all the information we need to appropriately plan and execute our audit.

What are the three elements for the communications portion of the Information and Communications component? [ISA | 1323.1600]

We consider the three elements outlined in the table below when obtaining an understanding and evaluating the communications portion of the Information and Communication component of ICFR.

Elements for communication	Element 10: The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between people within the entity, including how financial reporting roles and responsibilities are communicated.

Element 11:

The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

Element 12:

The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control to external parties, such as regulatory bodies.

Examples

1.1 Understand and evaluate the information system [ISA | 7846]

What do we do?

Obtain an understanding of the information systems relevant to financial reporting and evaluate whether the entity's information system appropriately support the preparation of the entity's financial statements in accordance with the applicable financial reporting framework.

Why do we do this?

We obtain an understanding and evaluate the entity's information systems relevant to financial reporting, which is part of the Information and Communication component of ICFR, to support our identification and assessment of risks of material misstatement (RMMs). Information systems support informed decision making and the functioning of the internal control by processing relevant, timely, and quality information from internal and external sources.

Execute the audit

How do we obtain an understanding of the entity's information systems relevant to financial reporting? [ISA | 7846.8529]

We obtain an understanding of the entity's information systems relevant to financial reporting by:

- obtaining an understanding of the entity's business processes and its financial reporting process. This includes:
  - obtaining an understanding of the entity's business processes
  - understanding the process by which accounting estimates are developed;
  - obtaining an understanding of the entity's financial reporting process;
  - obtaining an understanding of the processes and procedures to enter transaction totals into the general ledger;

  - obtaining an understanding of processes and procedures for journal entries and other adjustments; and
  - preparing or using the entity's flowcharts to document our understanding of the entity's processes.

- evaluating the entity's information systems
- obtaining an understanding of the entity's overall IT environment. An entity's overall IT environment includes its IT organization, the IT processes, and the IT systems (and underlying layers of technology) used in the entity's financial reporting and business processes.

What is the role of IT systems in the entity's information systems relevant to financial reporting? [ISA | 7846.11949]

In today's technology-focused economy, using IT systems, including enterprise resource planning (ERP) systems, has become commonplace. Entities often use IT systems extensively within their information systems and in business processes to help them:

- manage and operate their business;
- maintain their financial records; and
- report financial results both internally and externally.

Entities may choose to automate certain functions using IT systems within business processes - including process control activities to address risks - to enhance efficiency and effectiveness.

Automation may be particularly common when processing and reporting larger volumes of transactions, or when processing and aggregating information or data elements is not feasible without using IT systems.

Are general IT controls part of the Information and Communication component or Control Activities? [ISA | 7846.11951]

General IT controls are control activities.

Are service organizations part of the Information and Communication component of ICFR? [ISA | 7846.11952]

Because an entity's information system is not limited by legal boundaries, service organizations contracted by that entity may be part of its information system - depending on the nature of the processes and activities the service organization performs.

Many entities routinely contract with service organizations to assist them with certain business processes or aspects of business processes.

In turn, many service organizations further contract with other service organizations - i.e. sub-service organizations - to help them provide their services to an entity. For example, a payroll service organization may engage another service organization to provide it with an IT data center.

The service organization is part of the entity's information system when the processes and activities they perform:

- are part of the entity's accounting and reporting processes; or
- have an indirect effect on those processes (e.g. when a service organization performs IT processes and activities that mitigate risks arising from IT).

How may the Information component for smaller, less complex entities be different? [ISA | 7846.1800]

A smaller, less complex entity's approach to addressing the CERAMIC component is likely different than that of a larger, more complex entity. For example, the information system(s) relevant to financial reporting in small, less complex entities are likely to be less sophisticated than in larger, more complex entities and smaller, less complex entities will likely have simpler accounting and financial reporting processes. This includes relevant aspects of the system that relate to information disclosed in the financial statements that comes from within or outside of the general and subsidiary ledgers. As such, a smaller, less complex entity may not need extensive descriptions of accounting procedures, sophisticated accounting records, or written policies.

1.1.1 Understand how the entity uses IT as part of financial reporting [ISA | 1325]

What do we do?

Obtain an understanding of how the entity uses IT and how IT affects the entity's flow of transactions and the financial statements by understanding the IT environment.

Why do we do this?

Understanding how the entity uses IT as part of financial reporting provides information that's useful when:

- determining whether the entity highly depends on IT processing,
- identifying and assessing risks of material misstatement (RMMs),
- obtaining an understanding of business processes, including process risk points (PRPs) and relevant automated process control activities,
- identifying the relevant IT layers, risks arising from IT (RAFITs) and relevant general IT controls (GITCs),
- identifying information we plan to use in the audit, and
- designing substantive audit procedures.

Execute the Audit

How do entities use IT systems? [ISA | 1325.1400]

Entities often use IT systems extensively within their information systems and in business processes to help them:

- manage and operate their business;
- maintain their financial records;
- and report financial results both internally and externally.

Entities may choose to automate certain processes using IT systems - including control activities to mitigate risks - to enhance efficiency and effectiveness. Automation may be particularly common when processing and reporting larger volumes of transactions, or when processing and aggregating information or data elements is not feasible without using IT systems.

A wide range of software may be part of an entity's financial reporting IT systems, including ERP systems that integrate multiple layers of technology. Common ERP software vendors include

Microsoft, Oracle and SAP. In addition, many entities develop custom software to meet their specific needs or outsource IT services to service organizations, such as cloud computing (see question "What additional considerations are there if the entity outsources cloud computing?" and sub-questions for more information).

How might service-organization-managed services affect business processes? [ISA | 1325.10452]

Using service-organization-managed services may have a pervasive effect on the flow of an entity's transactions in one or many business processes. Some of these service organizations may not produce service auditor reports, which can make obtaining an understanding of the entity's information system challenging.

Using service organizations may also result in unique risks because the entity has given up control of some or all of its IT systems, while retaining responsibility for its information systems and ICFR.

In view of the wide variety of outsourced services offered and potential structures, understanding how the entity uses IT and its effect on the financial statements, and identifying and testing general IT controls, can be difficult. Using specific team members (STMs) with expertise in IT (IT Audit STMs) to help us obtain an understanding can be beneficial.

Who do we involve in obtaining an understanding of an entity's use of IT? [ISA | 1325.2100]

When obtaining an understanding of the entity's use of IT, we determine whether to involve specific team members (STMs) with expertise in IT (IT Audit STMs). See activity 'Involve specific team members with expertise in Tax and IT as appropriate' for information on:

- when we involve IT Audit depending on the type of entity we are auditing,
- when we may involve IT Audit, and
- how we involve IT Audit in our audit, including what are some common areas where IT Audit is involved.

Even if we involve IT Audit, we remain responsible for obtaining an understanding of the entity's use of IT as part of financial reporting.

How do we obtain an understanding of how the entity uses IT as part of financial reporting? [ISA | 1325.2200]

Obtaining an understanding of how the entity uses IT as part of financial reporting involves obtaining an understanding of an entity's overall IT environment, which includes:

- understanding the IT systems the entity uses as part of its financial reporting and business processes relevant to the preparation of the financial statements, including the various layers of technology that make up the IT system (applications, databases, operating systems and networks);
- understanding the entity's IT processes to manage the IT environment;
- understanding the entity's IT organization; and
- understanding cybersecurity risks and incidents.

Additionally, as part of obtaining an understanding of the entity's business processes and financial reporting process relevant to the preparation of the financial statements, we also obtain and/or confirm our understanding of how IT affects the entity's flow of transactions, accounting records and disclosures related to each process (see activity "Understand business processes" and sub-activities for further information).

How may the complexity of the entity's IT environment impact our understanding of the entity's use of IT? [ISA | 1325.8676]

While the use of IT may be significant in entities with less complex IT environments, extensive descriptions of accounting and IT procedures, sophisticated accounting records, or written policies may not be available. Understanding the entity's IT environment may be easier and it may be more dependent on inquiry than on review of documentation.

When an entity has greater complexity in its IT environment, it is likely that we involve specific team members with expertise in IT in identifying the IT systems and other aspects of the IT environment, determining the related risks arising from IT, and identifying general IT controls. Such involvement is likely to be essential and may be more extensive for complex IT environments. Refer to the activity "Involve specific team members with expertise in Tax and IT as appropriate" for further information on when to involve IT Audit.

The extent of our understanding of the IT processes varies with the nature and the circumstances of the entity and its IT environment. The complexity of the IT environment may also impact the extent to which the entity has general IT controls in place, as well as the number of IT system layers that are subject to risks arising from IT.

What do we document when we obtain an understanding of how the entity uses IT as part of financial reporting? [ISA | 1325.10455]

We document:

- the key elements of our understanding,
- the risk assessment procedures performed, and
- the sources of information from which our understanding was obtained.

Examples

What procedures might we perform to obtain an understanding of how the entity uses IT as part of financial reporting? [ISA | 1325.3000]

Fact pattern:

When obtaining an understanding of how the entity uses IT as part of financial reporting, the engagement team decides to perform a combination of inquiry and inspection procedures.

Analysis

Example procedures that the engagement team may perform to obtain an understanding of the entity's IT systems IT processes and IT organization include:

- Inquiry of management (CIO/ IT director/ Head of IT/ IT manager) to obtain an understanding of matters such as:
  - the structure of IT governance;
  - an overview of the entity's IT infrastructure;
  - how IT is used to support financial reporting/ business processes that impact financial reporting;

- relevant IT systems used for financial and business operations, including the various layers of technology that make up the IT system (applications, databases, operating systems and networks);
- how systems interface/transfer data;
- the extent of end-user computing in financial reporting;
- recently implemented and new or upcoming IT projects;
- significant upgrades or changes to relevant layers of technology;
- management's assessment of significant IT risks;
- the extent of reliance on centralized services, including shared service centers, and/or third-party service providers;
- the use of any report writers, data warehouses, utility tools or ticketing tools in the processing of financial data or implementation/operation of automated controls;
- the use of any Robotic Process Automation (RPA) and if used, its level of sophistication; and
- the entity's IT processes to manage:
    - access to programs and data
    - program changes
    - program acquisition and development (e.g. Agile development or a more traditional approach)
    - computer operations.

- Inspection of documentation, when available, such as:
    - IT organization chart;
    - Description of IT processes to manage:
        - access to programs and data
        - program changes
        - program acquisition & development
        - computer operations;
    - Cybersecurity risk assessment;
    - IT governance / steering group meeting minutes;
    - service organization contract(s) relating to IT;
    - recent internal audit report(s) relating to IT ; and
    - evaluation report(s) (or other relevant documentation) describing the outcome of IT system(s) implemented or upgraded/ changed in the period.
- Inquiry of management (CEO/ COO/ CFO/ Head of Accounting) to obtain an understanding of matters such as:
    - the dependency of financial reporting/ business processes that impact financial reporting on the use of IT;
    - the extent of end-user computing in financial reporting;
    - recently completed and currently ongoing IT projects and known/ expected impact on the financial reporting process/ business operations;
    - any recent or ongoing IT issues that impact the financial reporting process/ business operations; and
    - any envisioned changes to IT that impact business processes and financial reporting.

What matters might we consider when obtaining an understanding of a less complex IT environment? [ISA | 1325.8677]

Fact pattern:

An entity's use of IT as part of financial reporting consists of a single commercial accounting software.

Analysis

Obtaining an understanding of an entity's use of IT may be more easily accomplished in a less complex IT environment that uses an "off-the-shelf" single commercial accounting software (e.g. QuickBooks). Matters that the engagement team may consider in understanding the nature of a single commercial accounting software may include:

- The nature and extent of modifications that have been made to the software (e.g., setting or amending reporting parameters);
- The extent to which it is possible for the entity to modify the source code of the software to include additional modules (i.e., add-ons) to the base software, or to make direct changes to data;
- The extent to which data related to the preparation of the financial statements can be directly accessed (i.e., direct access to the database without using the IT application) and the volume of data that is processed; and
- The extent to which the software is well established and has a reputation for reliability.

1.1.1.1 Understand the entity's IT systems [ISA | 7589]

What do we do?

Obtain an understanding of the IT systems the entity uses as part of its financial reporting and business processes relevant to the preparation of the financial statements.

Why do we do this?

We obtain an understanding of the IT systems the entity uses as part of its financial reporting and business processes relevant to the preparation of the financial statements in order to understand how the entity uses IT and how IT affects the entity's flow of transactions and the financial statements.

Execute the audit

How do we obtain an understanding of the IT systems used by the entity? [ISA | 7589.10383]

For each IT system used by the entity as part of its financial reporting and business processes relevant to the preparation of the financial statements, we obtain at a minimum an understanding of the elements that are set out in the table below.

Element	Description
Name of IT system	The name of the IT system the entity uses, including: • whether it was purchased from an outside vendor or developed internally; and

	• the name of the vendor (if applicable).
Purpose of the IT system	A description of how the entity uses the IT system as part of its financial reporting and business processes.
Processes using the IT system	A list of the accounting and financial reporting processes that use the IT system.
Components using the IT system	If applicable, a list of the entity's components (subsidiaries, divisions or locations) that use the IT system.
Layers of technology within the IT system	For each layer of technology that comprise the IT system - i.e. application layer, database layer, operating system layer and network layer: • Title and version • Significant upgrades Description of any significant upgrades to the IT layer/ system during the period. For example: - the implementation of a new IT layer/system; - upgrades to the existing IT layer/system; - upgrades to layers of the IT system, such as the underlying database for the application; or - upgrades to the operating system that the database runs on. • Extent of customization and/or changes Whether the IT layer/system has been customized and the nature of the customization, and whether significant changes have been made. • Extent of outsourcing Whether the IT layer/system has been outsourced, and the nature of the outsourcing - e.g. an outsourced data center that hosts the entity's IT system, or an outsourced Cloud-based IT system. Note: The same database layer may support more than one IT application and, therefore, be part of more than one IT system. Also, the operating system may support more than one IT application and database.

We may also prepare or include an IT systems diagram (ISD) or other documentation as part of our understanding.

Additionally, the entity may use emerging technologies (e.g., robotic process automation (RPA), blockchain, or artificial intelligence) because such technologies may present specific opportunities to increase operational efficiencies or enhance financial reporting. When emerging technologies are used in the entity's information system relevant to the preparation of the financial statements, we may include such technologies in our understanding of the entity's IT systems and the layers of technology.

What are IT systems diagrams? [ISA | 7589.10384]

An IT systems diagram (ISD) is a graphical depiction of the IT systems an entity uses- including the layers of technology within those systems.

Why are ISDs useful when obtaining an understanding of an entity's use of IT systems? [ISA | 7589.10385]

An ISD helps us to simplify our understanding of the entity's IT systems and the layers of technology within those systems. Understanding the layers of technology that make up an IT system can become complex - especially when the entity uses multiple IT systems that comprise many different layers of technology.

This simplified understanding may help us:

- evaluate whether we have a sufficient understanding of the entity's use of IT systems; and
- identify risk arising from the entity's use of IT that could affect the continued effective operation of automated controls or the integrity of data and information residing within those systems.

Can an ISD be used to document our understanding of the flow of data and information through IT systems? [ISA | 7589.10386]

No, because ISDs show the relationships between layers of IT, not the flow of data or transactions through the IT system or through a business process.

While the ISD helps us understand the IT systems and the layers of technology within those IT systems, we capture and document the flow of data and information as part of our understanding of the business processes (see activity 'Understand business processes' for more information).

What are the layers of technology that comprise an IT system? [ISA | 7589.10387]

IT systems are comprised of four types of layers of technology (also referred to as IT system layers or IT layers), which are the application, database, operating system and network layers (the last three layers may be collectively referred to as IT infrastructure). Each of these layers of technology may present risks arising from IT (RAFITs) to be controlled by management so that:

- automated controls operate and function effectively; or
- the integrity of data and information sourced from an entity's IT system is maintained.

The table below provides a description of each of the layers of technology.

Layer	Description
Application	Applications are the layers of IT systems designed to perform one or many functions, tasks or activities - often to capture, process or extract data. Applications often include an interface accessed by an end-user.

	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. Examples of the application layer of an IT system include: • ERP systems, such as SAP and Oracle; • report writers, • emerging technologies, such as robotic process automation (RPA), artificial intelligence; and • transaction-processing systems, such as a CRM or billing system.
Database	Databases are the layers of IT systems that organize a collection of data or information so that it can be easily accessed, managed and updated. This includes data warehouses, which are separate applications that we consider as a database layer. SQL Server and Oracle DB, as well as stand-alone data repositories and data warehouses, are examples of the database layer of an IT system. Technologies such as MS SQL Server may be used by an entity for multiple IT systems to access information in the database.
Operating system	Operating systems are the layers of IT systems that control the basic operation of a computer and provide a software platform on which to run other software, such as applications and databases. The operating system generally works behind the scenes and is usually not manipulated directly by the end user. UNIX, LINUX, Microsoft Windows and MacOS are examples of the operating system layer of an IT system.
Network	Networks are the layers of IT systems that transport information or data between computers, either within an organization or between organizations. Access to IT applications may be restricted to users on a particular network - e.g. users cannot access an IT application outside of a local area network (LAN) or virtual private network (VPN). Wide area networks (WANs), LANs and VPNs are examples of the network layer of an IT system.

Why do we understand the layers of technology that comprise an IT system? [ISA | 7589.10388]

We understand the layers of technology that comprise an IT system because:

- Data and information related to transactions and other events and conditions relevant to an entity's financial reporting may flow through multiple IT systems and the layers of technology within those systems.

- An entity may also design and implement automated controls within any layer of technology in an IT system. Thus, risks arising from IT (RAFITs) may exist in some or all of the layers of technology that make up an IT system.
- Not all layers of technology may be relevant to our audit, so understanding the layers helps us determine the specific layers that impact our audit approach.

What are report writers? [ISA | 7589.10389]

Report writers are a specific type of application whose function is to extract information or data, often from a database or data warehouse, and present that information or data in a specified format such as a report.

Entities often use these application layers as part of their financial reporting and business processes to produce data and information used in the operation of controls.

Report writers include:

- separate report writer applications;
- report writer functionality integrated into another IT application (e.g. within an ERP system); or
- report writer functionality integrated into an end-user computing environment (e.g. within Microsoft Excel).

What is robotic process automation (RPA)? [ISA | 7589.10390]

Robotic process automation (RPA), also referred to as 'robotics' or 'bots', is an emerging type of application used to automate manual tasks within a workflow. These tasks are generally repetitive, low judgment, and high-volume in nature and are often associated with processes that follow explicit or predictable rules and prescriptive steps. Bots may rely on end-users to trigger the activity (i.e. attended bots) or run independently, enabling work to be scheduled or completed continuously (i.e. unattended bots).

What is a data warehouse? [ISA | 7589.10391]

Data warehouses are separate applications that are database layers used as a central repository to accumulate and integrate data and information from a wide range of sources, e.g. multiple databases or other IT systems used in financial reporting and business processes, from which reports may be generated or that may be used by the entity for other data analysis activities. Data warehouses are often the source of data and information used in the operation of controls.

How do we identify report writers, RPA and data warehouses used in an entity's financial reporting and business processes? [ISA | 7589.10392]

We identify report writers, RPA and data warehouses when we obtain an understanding of the business processes - specifically, when we carefully consider and understand how the data is transferred to the report writer/data warehouse, where it is stored and how it is manipulated, extracted and reported.

Examples

What is included in our understanding of an entity's IT systems? [ISA | 7589.10393]

Fact pattern:

Consider an entity (Daisy Inc.) that uses:

- Hyperion for the consolidation process;
- Oracle Financials for the general ledger and sales and purchases processes; and
- Oracle HR for the HR/payroll process.

Each application is hosted in the entity's Boston data center.

Oracle Financials and Oracle HR run on a Unix A|X operating system and Oracle Database and are supported by the local IT group in Boston.

Hyperion runs on a Windows 10 operating system and SQL Server 2019 database and is supported by the IT group in the entity's corporate office in New York.

The consolidation application, Hyperion, was upgraded from Hyperion Enterprise to Hyperion Financial Management (HFM) in February of the current period. This was a major upgrade, which required replacing hardware, converting data, and installing and configuring new servers - including upgrading the operating systems to Windows 10 and upgrading the databases to SQL Server 2019.

Analysis:

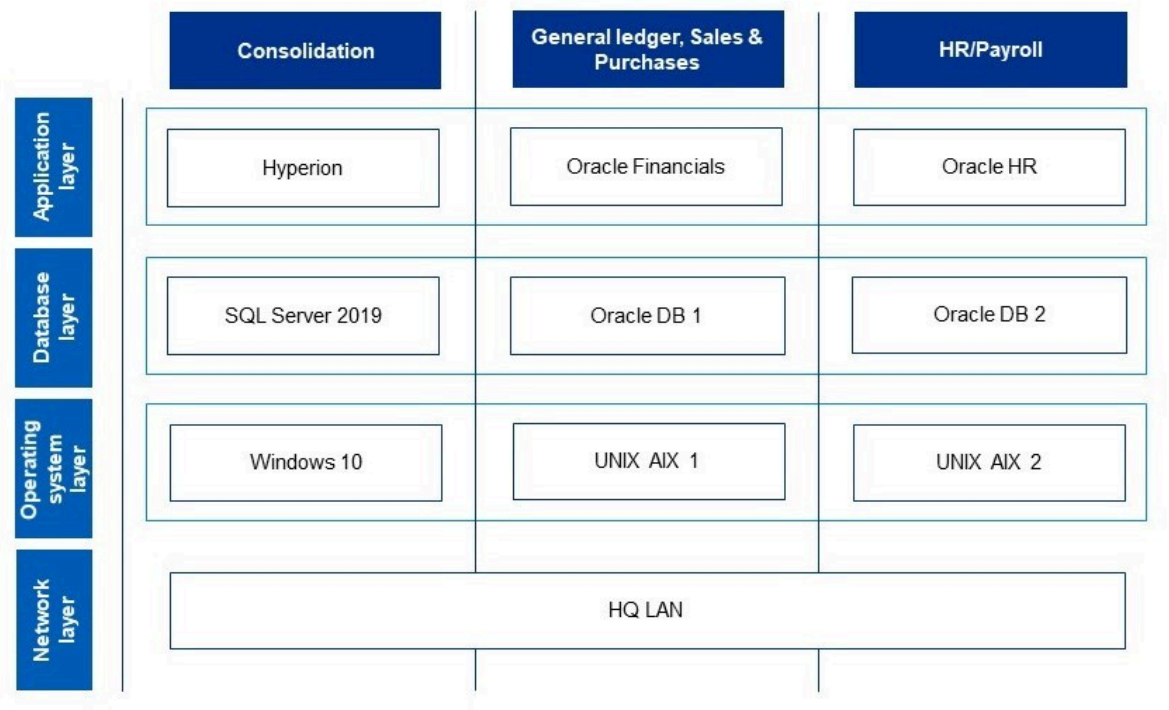
The engagement team identified three IT systems the entity uses as part of its financial reporting and business processes relevant to the preparation of the financial statements: Hyperion, Oracle Financials and Oracle HR.

The engagement team's understanding of the entity's IT systems included the following for the Hyperion system (Note: the engagement team also obtained an understanding of the Oracle Financials and Oracle HR systems, but this is not shown in this example):

Name of IT system	Hyperion
Purpose of the IT system	Used for the entity's financial reporting from components and for the entity's consolidated financial information
Processes using the IT system	Consolidation
Components using the IT system	All components
Layers of technology within the IT system	Application layer • Title and version: Hyperion Financial Management (HFM) • Significant upgrades: upgraded from Hyperion Enterprise to Hyperion Financial Management (HFM) in February of the current period. This was a major upgrade, which required replacing hardware, converting data, and installing and configuring new servers. • Extent of customization and/or changes: None • Extent of outsourcing: None

	• Other relevant information: None
	Database layer • Title and version: SQL Server 2019 (15.0.2000.5) • Significant upgrades: as part of upgrading Hyperion, the database was upgraded from SQL Server 2014 to SQL Server 2019 in February of the current period • Extent of customization and/or changes: None • Extent of outsourcing: None • Other relevant information: None
	Operating system layer • Title and version: Windows 10 • Significant upgrades: as part of upgrading Hyperion, the operating system was upgraded from Windows 2003 to Windows 10 in February of the current period • Extent of customization and/or changes: None • Extent of outsourcing: None • Other relevant information: None
	Network layer • Title and version: HQ LAN • Significant upgrades: N/A • Extent of customization and/or changes: None • Extent of outsourcing: None • Other relevant information: None

They also include the following ISD, capturing certain key elements of all three IT systems:



1.1.1.2 Understand the entity's IT processes [ISA | 7842]

What do we do?

Obtain an understanding of the entity's IT processes to manage access to programs and data, program changes, program acquisition and development and computer operations.

Why do we do this?

We obtain an understanding of the entity's IT processes in order to understand how the entity uses IT and how IT affects the entity's flow of transactions and the financial statements. Our understanding may help us to identify relevant risks arising from IT (RAFITs) and the general IT controls (GITCs) that address them.

Execute the audit

What does our understanding of the entity's IT processes include? [ISA | 7842.8689]

Obtaining an understanding of the entity's IT processes includes understanding the process to:

- manage access to programs and data;
- manage program changes or changes to IT systems;
- acquire or develop new IT systems; and
- manage computer operations.

The table below provides example considerations that may be applicable when obtaining an understanding of the entity's IT processes.

IT process	Example considerations
Access to programs and data	• The process to manage access to programs and data (authentication/ authorization, provisioning, de-provisioning, privileged access, user access reviews, physical access) • The complexity of the process to manage access rights • Whether the entity uses any tools to support the process (e.g. identity access management (IAM), workflow tools to support the approval process, password vaults to secure shared passwords, etc.)
Program changes	• The process to manage program changes or changes to IT systems (authorization, development, testing, and approval, migration to the production environment including configuration and emergency changes) • The complexity and formalization of the change process • Whether the entity uses any tools to support the change management process (e.g. workflow tools, code migration tools, etc.)
Program acquisition and development	• The process to acquire or develop new IT systems (design, development, testing, approval, implementation, and data migration) • The development methodology (e.g. agile or traditional) • The complexity and formalization of the acquisition and development process • The nature and significance of major data conversion, if one occurred, and how the conversion was undertaken (e.g. software upgrade provided by vendor, major version upgrade, new release, platform change, etc.)
Computer operations	• The process to manage computer operations (job scheduling, job monitoring, backup and recovery, and incident/problem management) • Whether the entity uses any tools to backup data related to relevant financial systems, tools used for incident and problem management, and/or tools used to manage job scheduling activities.

Understanding the nature and complexity of IT processes in place may assist in determining which IT systems the entity is relying upon to process and maintain the integrity of information in the entity's IT environment.

What might we consider when assessing the complexity of IT processes? [ISA | 7842.8690]

The table below sets out example considerations when assessing the complexity of IT processes.

IT process	Example complexity considerations

Access to programs and data	The complexity of the process to manage access rights may vary from a less complex IT process with informal policies and procedures, centralized security administration function, and/or a single individual dedicated to supporting security administration to a more complex IT process with formally documented policies and procedures, a decentralized security administration function and a larger number of individuals dedicated to supporting security administration and monitoring.
Program changes	The complexity of the program change process may vary from a less complex IT process over changes to a commercial application with little or no customization to a more complex program change process over highly customized or highly integrated applications.
Program acquisition and development	The complexity of the program acquisition and development process may vary from a less complex IT process over the acquisition of purchased commercial applications with no ability to customize to a more complex process over entity-developed applications with significant customizations and conversions of system data from legacy systems to new systems.
Computer operations	The complexity of the computer operations process may vary from a less complex IT process over informal computer operations with few scheduled jobs and no policies or procedures to a formal computer operations function with many scheduled jobs with varying frequency and formal policies and procedures.

Examples

What is included in our understanding of an entity's IT processes? [ISA | 7842.8691]

Fact pattern 1:

Consider an entity that:

- Has a moderately complex IT environment
- Uses Hyperion for consolidation and part of the period-end financial reporting process; Oracle Financials for the general ledger and sales and purchases processes; and Oracle HR for the HR/payroll process
- Uses ServiceNow to support the access to programs and data and program change processes

Analysis:

The engagement team's understanding of the entity's IT processes included the following:

IT process	Description

Access to programs and data	The entity adopted a formal security policy that provides guidance for information security within the organization. The security policy includes aspects of the IT environment relevant to financial reporting applications such as password policies, procedures to request and revoke access, etc. Passwords are used for authentication to the entity's financial systems based on the entity's information security policy. The entity established password rules including minimum length, password change interval, complexity, use of recycled password, etc. The process to provision access, including privileged access, to the entity's financial systems is initiated when a user's manager submits an online access request form via ServiceNow. The user's manager completes the form to indicate the user's role/responsibilities and the system(s) and access permissions requested for the new user. The form is submitted to the IT department, where a designated IT security administrator will review the form and process the request. The process to de-provision access to the entity's financial systems is initiated when the HR department changes the employee status to 'terminated' in the Oracle HR system. Once the status is changed, the terminated employee's Oracle user account is automatically disabled. Changing the employee status to 'terminated' also triggers the automatic creation of a ServiceNow ticket. The ticket is assigned to the IT security administrator to confirm that access to all systems is disabled. On a quarterly basis, the entity performs a user access review. The IT security administrator generates system security reports showing the access permissions of users and submit the reports to the business owners for review. The business owners review the users access rights and submit requests for access changes as necessary. The IT security administrator will then process the requests. The entity uses electronic key cards to restrict physical access to the data center. The process to obtain physical access to the data center requires that the employee complete and submit a request form to Operations Management personnel for approval. Upon approval, a designated security administrator will grant the employee physical access to the data center.
Program changes	The entity has a formal change management policy. All changes, including configuration changes, require approval and testing. Prior to migration to production, changes are reviewed and approved by both business and IT managers. The entity uses an automated workflow to capture the change request and approval process. The process to migrate changes to production is initiated when the final approvals for testing indicate the change was successfully tested in the quality assurance (QA) environment and is ready for migration into the production

	(PROD) environment. Designated system administrators responsible for migrating changes, which are separate from developers, will then migrate the change from the QA environment to the PROD environment. Emergency changes follows a similar process, however emergency changes are flagged as high priority and the request, approval, testing are expedited.
Program acquisition and development	Requests for new system acquisitions or development are forwarded to Steering Committee for review and approval. Major system acquisitions require the approval of the Board of Directors. Once approved, the entity follows the established policies and procedures over new system acquisitions/developments including defining requirements, design, development, testing, and data conversion/migration. *Note: When there are significant program acquisitions or developments, additional documentation of the specific aspects of those processes would be included here.
Computer operations	The entity uses utility tools to support batch job scheduling, processing, and monitoring. The Computer Operations team is responsible for monitoring batch jobs and notifying relevant teams as necessary to resolve any job failures. The entity uses a cloud backup service to back up their business-critical data and applications on cloud servers. Data backups are restored periodically and tested for data recoverability.

Fact pattern 2:

Consider an entity that:

- Has a less complex IT environment
- Uses ABC system, a single commercial accounting software application

Analysis:

The engagement team's understanding of the entity's IT processes included the following:

IT process	Description
Access to programs and data	The entity has informal process and procedures in place to manage access to ABC system. The IT Manager has security administrative responsibility to administer access to the system. The process to provision access is initiated when HR notifies the IT Manager of a new hire. HR completes an access request form to request access based on the new hire's job responsibility. The IT Manager will then provision access as requested and email the new hire the new user ID and password. The user is required to change the password upon initial logon. The entity also

	has password rules in place including minimum password length, password expiration, and complexity requirements. The process to de-provision access is initiated when HR notifies the IT Manager of an employee termination. Upon notification of termination, the IT Manager will revoke the terminated employees' access. The server room that houses ABC system is secured through use of a key fob. The entity uses a physical security software to program the key fobs to unlock entry to doors based on employee need. The process to obtain access to the server room is initiated when an employee fills out a physical access request form and submits it to the IT Manager for review and approval. Upon approval, the IT Manager will program the employee's key fob to access the server room.
Program changes	The entity does not perform any programming/development nor does the entity have access to ABC system source code. The entity has an informal and less complex change management process in place whereby changes are limited to software patches, releases, and updates. These types of changes are generally initiated by the vendor. If the vendor has an update, they notify the entity that a new update is available. The entity is then responsible for reviewing the release notes and determining whether they want to apply the update. If the entity determines that they will apply the update, they will download the update from the vendor's website to the entity's test environment and perform end user testing. Once testing is completed and the change is approved for production, entity management with system administrative privileges will install the software update in the production environment.
Program acquisition and development	The entity does not develop any new IT systems. It has an informal process to acquire new systems. If the business determines a need to acquire a new system, it is discussed during the weekly Senior Management meetings. If Senior Management agrees to acquire a new system, they will coordinate with the IT Manager to perform research and identify potential vendors. Once a system is identified, they will then coordinate with the vendor to implement the new IT system. The vendor assisting with the implementation has a project plan in place that includes data migration. The entity validates data migrated from the legacy system to the new system.
Computer operations	Job scheduling, job processing, and job monitoring are not applicable given the entity's use of a single commercial accounting software. All transactions are updated in real-time. The entity has an informal process in place to backup data. The entity runs backup jobs to perform incremental daily and weekly backups. Full backups run

	monthly. The backed-up data is stored at an offsite secured location. The entity performs periodic data restorations as requested by end users.

What is included in our understanding of an entity's IT processes when we determine GITCs are ineffective and we do not test automated controls? [ISA | 7842.8907]

Fact pattern:

Consider an entity that:

- Has a less complex IT environment
- Uses System A, a single commercial accounting software application
- GITCs are not always formalized and documented
- The engagement team identified GITC deficiencies in the previous audit

The engagement team's understanding of the entity's IT processes included the following:

IT process	Description
Access to programs and data	The IT Manager and the Accounting Manager (as a backup) have security administrative responsibility to administer access to the system. The prior year deficiency related to the privileged access GITC was not remediated in the current year[1]. The process to provision access is initiated when the Accounting department identifies a new user that needs access. Generally, the Accounting Manager sends a request either verbally or via email to the IT Manager requesting a new user account. The emails are not always retained[2]. The user is required to change the password upon initial logon. The entity has password rules in place for minimum password length password expiration, and complexity requirements. The process to de-provision access occurs when the IT Manager is notified of an employee resignation or termination. Upon notification of termination, the IT Manager will revoke the terminated employees' access. The IT Manager indicated that he does not always retain documentation to evidence the timely removal of access[2]. There is no data processing Center, as the system is maintained on the cloud.

Footnotes

[1] KPMG identifies this as a deficiency

[2] Since the entity has a less complex IT environment and uses a single commercial accounting software application, GITCs may not always be formalized and documented, which in this case is considered appropriate for the size and complexity of the entity and its IT environment.

Remember: When documenting our understanding of IT processes, we obtain an understanding for all four IT processes even if we identify a deficiency in one process. In this example, only one row was completed to illustrate example documentation when a deficiency is identified.

Analysis

As a result of the GITC deficiencies identified during the engagement team's understanding of the IT Processes, the engagement team concluded that they cannot rely on the related automated control(s). The engagement team decided to test manual controls related to the same assertion and risk of material misstatement.

1.1.1.3 Understand the entity's IT organization [ISA | 7591]

What do we do?

Obtain an understanding of the entity's IT organization.

Why do we do this?

We obtain an understanding of the entity's IT organization in order to understand how the entity uses IT and how IT affects the entity's flow of transactions and the financial statements.

Execute the audit

How do we obtain an understanding of the entity's IT organization? [ISA | 7591.10426]

Obtaining an understanding of the entity's IT organization includes understanding:

- key members of the IT organization, including their names, titles, and locations where they are based. We may also obtain an understanding of the number and skill level of the IT personnel;
- whether certain key functions of the IT organization have been outsourced, including the functions outsourced to external parties and service organizations; and
- the use of any centralized IT services, including shared services centers, to perform IT related processes for multiple IT systems and/or their related layers of technology.

1.1.1.4 Understand cybersecurity risks and incidents [ISA | 7592]

What do we do?

Obtain an understanding of management's cybersecurity risk assessment process when obtaining an understanding of how the entity uses IT as part of financial reporting AND consider whether cybersecurity risks or incidents lead us to identifying a risk of material misstatement (RMM) AND, if applicable, involve specific team members with expertise in IT.

Why do we do this?

The risk of a cybersecurity incident is faced by any company. Cybersecurity incidents often have negative consequences for the entity, including:

- lost revenues;
- litigation costs and potential regulatory fines;
- remediation costs related to stolen information, intellectual property, system repairs and incentives given to maintain relationships with customers or business partners;
- increased cybersecurity protection costs, e.g. insurance premiums;
- diminished investor confidence; and
- reputational or brand damage.

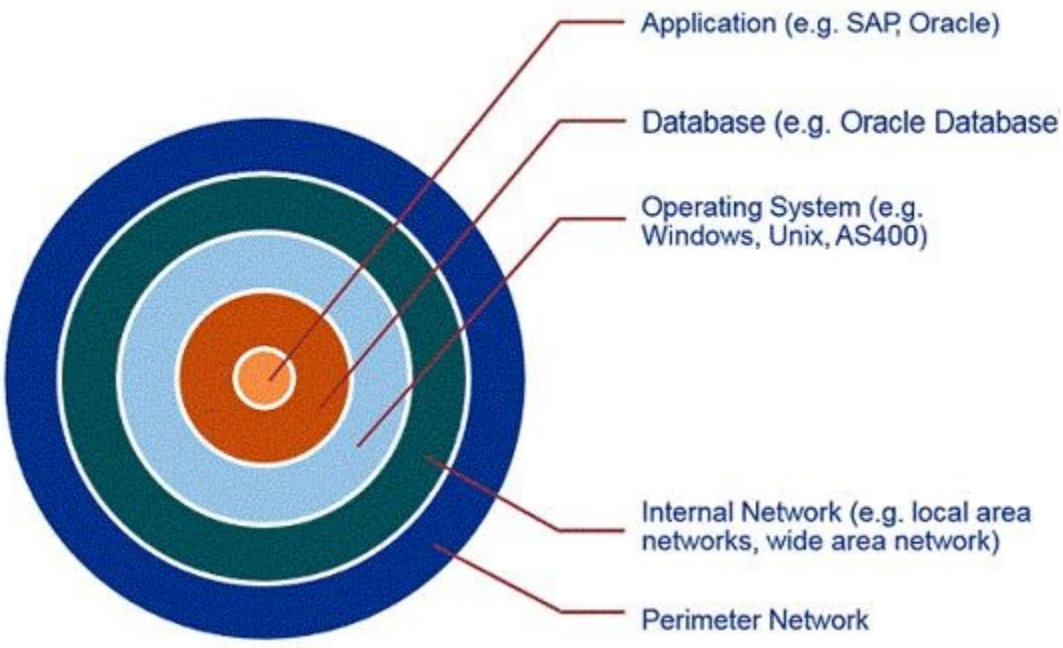
Consequently, when we obtain an understanding of how the entity uses IT and how IT affects the financial statements, we also consider cybersecurity risks and incidents because they may lead us to identifying RMMs, either at the financial statement level or at the assertion level, and may impact our audit approach.

Execute the audit

What are cybersecurity risks and incidents? [ISA | 7592.10437]

Cybersecurity risks relate to unauthorized access to IT systems. Cybersecurity incidents are intentional attacks or unintentional events whereby unauthorized users gain access to IT systems to disrupt operations, corrupt data, steal sensitive information or cause denial of service on websites.

The following diagram depicts the typical access path to an IT system.



Cybersecurity incidents usually first occur through the perimeter and internal networks. Depending on the entity's business environment, security around the internal and perimeter network may not pose risks to financial and non-financial data relevant to the audit. However, network access may or may not be relevant to the audit for entities that permit access to operating systems, databases, and applications through single sign-on protocols at the operating system layer. An example of a cybersecurity incident at the internal or perimeter network is when a computer virus sent as an email attachment or downloaded from a website infects systems on an entity's network.

Do we obtain an understanding of how management responds to cybersecurity risks for all entities? [ISA | 7592.10438]

Yes, we obtain an understanding of how management responds to cybersecurity risks and consider the occurrence of cybersecurity incident(s) for all audits, taking into consideration the nature of the entity's business, customer and vendor base, reliance on automated business processes and other relevant factors.

For example, cybersecurity risks may be more relevant to entities:

- with significant consumer focus and interaction, such as those with high volumes of credit card transactions;
- that retain large amounts of personally identifiable information (PII) (e.g. financial services, insurance, healthcare and retail organizations);
- that have significant intellectual property, such as software developers or pharmaceutical companies;
- with high volumes of transactional data, such as telecommunication providers or financial institutions; or
- with highly automated business processes which may become disrupted during a cybersecurity incident.

Are cybersecurity risks also relevant for third-party service organizations used by the entity? [ISA | 7592.10439]

Yes. When we obtain an understanding of how management responds to cybersecurity risks, we also consider risks related to third-party service organizations that are relevant to the audit.

We may consider the business environment and the nature of services provided by the third-party service organization in determining whether we perform additional procedures to address any cybersecurity risks arising from the third party.

What does obtaining an understanding of management's cybersecurity risk assessment include? [ISA | 7592.10440]

Management is responsible for evaluating the risk of cybersecurity incidents and cyber-related frauds (e.g. business email compromise (BEC) scams and other spoofing techniques) across all aspects of the entity's business operations, including financial reporting and compliance with relevant laws and regulations, and establishing processes, structures, and safeguards to mitigate those risks.

We are not responsible for evaluating cybersecurity risks across an entity's entire IT environment or providing assurances on the adequacy of safeguards and controls established to address cybersecurity risks or the entity's ability to withstand a cybersecurity incident. We are also not responsible for concluding on the appropriateness of the entity's actions in response to cybersecurity risks or to actual cybersecurity incidents. Care should be taken to avoid overstating our responsibilities and the scope of our work when discussing the results of the audit with management and audit committees.

However, we obtain an understanding of management's cybersecurity risk assessment process, which includes:

- evaluating the risks of material misstatement (RMMs) to an entity's financial statements resulting from, among other things, unauthorized access to financial reporting systems, including IT applications, databases, and operating systems.
- obtaining an understanding of a cybersecurity incident if one occurs and evaluating its effect on our audit approach. We evaluate management's assessment of the incident's effect on the amounts and disclosures in the financial statements and the entity's ICFR (see question ' What procedures may we perform if a cybersecurity incident comes to our attention during the course of the audit?').

In obtaining an understanding of management's cybersecurity risk assessment, we inquire of those within the entity that are primarily responsible and knowledgeable about cybersecurity matters and risks about management's risk assessment process related to cybersecurity risks and incidents.

Inquiries we make include:

- How does the entity's risk assessment process evaluate cybersecurity risks across the entity? How does the entity analyze and assess the significance of the risks to financial reporting? How do they manage the risk across the entity?
- How has the entity assessed its internal accounting controls in light of risks arising from cyber-related frauds (e.g. BEC scams, spoofing, phishing etc.)?
- How does the entity identify, assess and respond to risks related to attacks perpetrated through BEC scams or spoofing or phishing routines?
- How would the entity be aware, on a timely basis, if its IT applications, databases, operating systems and/or network had been subject to a cybersecurity incident that could impact the integrity of information used in the financial reporting process?
- Has a cybersecurity incident occurred within the entity during the period or in prior periods that impacts the current period?

What are BEC scams, spoofing or phishing? [ISA | 7592.8655]

In a "business email compromise" (BEC), also known as "email account compromise" (EAC), scams or spoofing/phishing routines, bad actors send an email message that appears to come from a known source, making it appear as if it's a legitimate request in the course of the business, with the aim of getting otherwise confidential or proprietary information from the entity, or getting personal information to perpetuate fraud for financial gain.

What are some of the entity's processes we may consider when understanding management's cybersecurity risk assessment? [ISA | 7592.8656]

Examples of the processes being employed by the entity as part of management's cybersecurity risk assessment that we may consider are:

Process	Description
Security evaluations	IT performs periodic network vulnerability assessments to: • scan, investigate, analyze, and report on any security vulnerabilities discovered on public, internet-facing devices; and

	• give the entity's management appropriate mitigation strategies to address those discovered vulnerabilities.
Security software	The entity installs security software to help protect it from web-based threats - including spyware, viruses, and phishing attacks. In addition, the entity uses virtual private networks and email encryption to prevent unauthorized disclosure of information.
Personnel training	Personnel are required to complete security training upon hire, which focuses on IT security and access communications. Security policies and procedures are available throughout the year via the Employee Handbook, located on the HR portal. All employees are required to complete an annual security 'refresh' training.
Network monitoring	The entity uses various software tools across the organization to monitor network access. These include vulnerability scanners, packet sniffers, intrusion detection systems (IDS), vulnerability exploitation devices, packet crafting tools, and firewall monitoring devices.
Corporate cybersecurity incident response team (CIRT)	The entity sets up a CIRT as part of its cyber intrusion protection program (CIPP), which monitors threats and/or breaches of data on a real-time basis. In particular, the CIRT identifies, assesses, evaluates, and takes actions to mitigate data breaches or other types of unauthorized cyber intrusion. Often management would organize their cybersecurity activities in a Security Operations Center.
Cyber governance	The entity incorporates cyber governance in its corporate governance regime - e.g. to receive reports on cybersecurity activities regularly. Alternatively, on a quarterly basis, the Board of Directors is briefed on findings and concerns relating to the entity's CIPP, as well as other measures taken by management to mitigate cybersecurity risks.
Business continuity plan	The business continuity plan includes a documented and tested plan to deal with cybersecurity incidents if the organization does not have a separate cybersecurity incident response plan that is tested by the CIRT.
Service organizations	The entity has a process to consider the impact of cybersecurity risks on service organizations relied upon in connection with their internal control over financial reporting and depending on the nature of the services provided.

Verification controls	The entity has various controls that verify changes to bank account information or vendor payment information (e.g. routing numbers, vendor names, etc.) to authenticate the validity of the changes.

Under what circumstances do we involve specific team members with expertise in IT? [ISA | 7592.10441]

If a cybersecurity incident at any layer comes to our attention during the course of our audit, or if we identify cybersecurity risks that lead us to the identification of an RMM, we involve specific team members with expertise in IT to help us with our response to the incident and/or RMM, including the identification of process risk points (PRPs) and process control activities and related general IT controls when applicable.

Further guidance may be sought from the firm's cybersecurity specialists, or DPP, if deemed appropriate.

What if a cybersecurity incident and/or cybersecurity risk gives rise to an RMM? [ISA | 7592.8659]

If we determine that a cybersecurity incident and/or cybersecurity risk gives rise to an RMM, we:

- Identify the RMM,
- Revise our approach to testing relevant control activities, including relevant automated process control activities and GITCs, as a result of the identified RMM, and/or
- Determine the additional substantive procedures to be performed to address the potential financial statement implications (as a result of the cybersecurity incident and/or risk), such as contingent or known liabilities related to possible noncompliance with laws and regulations.

Under what circumstances may a cybersecurity risk give rise to an RMM? [ISA | 7592.8658]

Although it is more likely that we identify an RMM as a result of a cybersecurity incident since the incident can have a significant impact on our audit approach and on the entity's financial statements, in certain circumstances we may identify an RMM as a result of a cybersecurity risk without a cybersecurity incident having occurred. For example, if, as a result of our inquiries to management about their risk assessment process related to cybersecurity risks and incidents, it becomes clear to us that management does not have a risk assessment process or controls in place to prevent and/or detect cybersecurity incidents on a timely basis, such that there is a reasonable possibility of an undetected cybersecurity incident that would have a material effect on the financial statements, including those that may occur at a service organization relevant to the audit.

What procedures may we perform if a cybersecurity incident comes to our attention during the course of the audit? [ISA | 7592.8661]

If a cybersecurity incident, including cyber-related frauds perpetrated through BEC scams, spoofing or phishing techniques, occurs, we evaluate the impact of the incident on our audit and on the entity's financial statements. When evaluating the impact on our audit approach, we may consider taking the following actions:

- Obtain an understanding of the nature, magnitude, and duration of the cybersecurity incident, including what internal and perimeter networks or IT applications, databases, and operating systems were compromised, and any impact on the financial information.

- Determine whether any control deficiencies have been identified as a result of a cybersecurity incident and evaluate them in accordance with the activity 'Identify and evaluate control deficiencies'.
- Reassess whether continued reliance on automated control activities is warranted and if so, whether to test additional process control activities or GITCs. Consider the layers of technology that may have been impacted by the cybersecurity incident and its impact to the RAFITs that are relevant to the effective operation of automated controls or the integrity of information.
- Reassess the risk of material misstatement. Consider whether additional substantive testing is necessary, e.g. over liabilities for compensation and remediation, litigation costs, and regulatory fines/penalties.
- Consider the financial accounting and reporting implications related to a cybersecurity incident. For example:
  - An entity that has experienced a cybersecurity incident may incur both direct and indirect losses that require recognition and/or disclosure in the financial statements, such as those derived from claims asserted against the entity, fines or penalties levied by governmental agencies, incentives to affected customers to maintain the business relationship, or a decline in expected future cash flows as a result of reputational and brand damage that may impact the fair value of assets.
  - Financial statement disclosures related to cybersecurity risks and incidents required by the applicable financial reporting framework or other laws and regulations.
  - Evaluate management's assessment of the incident's effect on the amounts and disclosures in the financial statements - e.g. related contingent liabilities and claims suffered as a result of the actual incident, the impact on cash flows (which may trigger impairment), and the adequacy of disclosures.

1.1.2 Understand processes [ISA | 8117]

What do we do?

Obtain an understanding of processes

Why do we do this?

Obtaining an understanding of processes gives us important evidence that we use in identifying and assessing RMMs and designing further audit procedures.

Execute the audit

For which business processes do we obtain an understanding? [ISA | 8117.159401]

We obtain an understanding for:

- business processes, and
- the period-end financial reporting process.

1.1.2.1 Understand business processes [ISA | 1327]

What do we do?

Obtain an understanding of business processes

Why do we do this?

Obtaining an understanding of business processes gives us important evidence that we use in identifying and assessing RMMs and designing further audit procedures.

For example, a thorough understanding of the revenue process will help us understand:

- each type of revenue stream;
- where systems are used to alert us to situations in which we might inadvertently rely on the IT system;
- how complex the process is to account for revenue;
- how the revenue process is reported in the financial statements, etc.

Execute the Audit

What is a business process? [ISA | 1327.11218]

An entity's business processes are the activities designed to:

- Develop, purchase, produce, sell and distribute an entity's products and services;
- Record information, including accounting and financial reporting information; and
- Comply with laws and regulations relevant to the financial statements.

Business processes result in transactions that are:

- initiated, authorized, recorded, processed, and corrected when necessary,
- transferred and reconciled to the general ledger,
- reported by the information system within both automated and manual systems, and
- reported in the financial statements and related disclosures.

Why do we say 'financial statements and related disclosures'? [ISA | 1327.159427]

Financial statements are a structured representation of historical financial information and include disclosures in accordance with a financial reporting framework. Disclosures comprise explanatory or descriptive information set out as required, expressly permitted or otherwise allowed by the applicable financial reporting framework on the face of a financial statement or in the notes, or incorporated therein by reference when expressly permitted.

While the term 'financial statements' includes disclosures, the phrase 'financial statements and related disclosures' is used to emphasize it means the primary financial statements and disclosures.

Enhanced | How do we obtain an understanding of business processes? [ISA | 1327.157103]

We obtain an understanding of business processes based on the applicable International-Enhanced methodology as follows:

Applicable International-Enhanced methodology	Processes	Obtain an understanding of the process by:

International-Enhanced PIE methodology	All processes and sub-processes	Performing a walkthrough
International-Enhanced Non-PIE methodology	Processes, or sub-processes, where we evaluate D&I of process control activities that address RMMs	Performing a walkthrough
	Processes, or sub-processes, where we do not evaluate D&I of process control activities that address RMMs	Either performing (i) a walkthrough or (ii) through inquiry and observation or inspection. Walkthroughs are encouraged.

See question "Which control activities do we obtain an understanding of and are relevant to the audit?" for guidance on when we evaluate D&I of process control activities that address RMMs.

Performing either (i) walkthroughs or (ii) inquiries and observations or inspections provide information about the entity's transactions, balances, disclosures and accounting policies or principles. This helps us identify and assess RMMs.

Enhanced | Which business processes do we walkthrough and why? [ISA | 1327.6370]

We perform a walkthrough for business processes that may have an RMM within the process based on the applicable International-Enhanced methodology as follows:

Applicable International-Enhanced methodology	Processes
International-Enhanced PIE methodology	All processes and sub-processes
International-Enhanced Non-PIE methodology	Processes, or sub-processes, where we evaluate D&I of process control activities that address RMMs

Additionally, when we apply the International-Enhanced Non-PIE methodology in processes or sub-processes where we do not evaluate D&I of process control activities that address RMMs, we perform either (i) a walkthrough or (ii) inquiry and observation and/or inspection for business processes that may have an RMM within the process. Walkthroughs are encouraged.

See question "Which control activities do we obtain an understanding of and are relevant to the audit?" for guidance on when we evaluate D&I of process control activities that address RMMs.

See activity "Understand business processes" for guidance when obtaining an understanding of a business process through inquiry and observation or inspection.

At this point in the risk assessment process, we have not yet identified RMMs, so we initially perform a walkthrough for each process (as noted in the table above) associated with accounts, disclosures, relevant transactions, events and conditions that has a 'reasonable possibility' of having an RMM within the process. 'Reasonable possibility' means a more than remote possibility, and is therefore a low threshold. We assess both risks due to error and risks due to fraud. This includes those processes where the entity did not have any relevant transactions, but events and conditions exist that indicate there is a 'reasonable possibility" of having RMMs within the process. An RMM is a risk that could result in a material misstatement to the financial statements.

Since we use walkthroughs as an input to determine whether an RMM exists and whether an account is a significant account or whether a disclosure is a significant disclosure, understanding when to do a walkthrough can be tricky to explain.

We may also exclude certain processes if we are reasonably certain that no RMM exists, either individually or in the aggregate (e.g. based on size and nature of the account). That may leave a remaining population where we do not know enough about the process to determine if there are associated RMMs. In those cases, we obtain further information about the process until we have sufficient knowledge to determine whether an RMM exists, this may include performing a walkthrough.

Walkthroughs allow us to gather information to identify and assess risk, so we are careful about when we decide not to perform them. We may end up performing walkthroughs over business processes that ultimately do not contain an RMM, but the walkthrough is one of the risk assessment procedures that allows us to make an informed decision about whether an RMM exists.

As we progress through the remainder of the risk assessment process and audit, we may identify RMMs where we have not yet performed a walkthrough of the processes associated with them. For example, we may identify RMMs related to the completeness of liability accounts that we originally did not have a 'reasonable possibility' of having an RMM associated with them. When we identify these new RMMs, we perform a walkthrough of the associated processes.

Enhanced | Do we walkthrough business processes related to significant unusual transactions? [ISA | 1327.11295]

Yes. We always perform walkthroughs for understanding business processes related to significant unusual transactions, which may include transactions such as business combinations or impairment of goodwill. We perform walkthroughs even when applying the International-Enhanced Non-PIE methodology because for processes related to significant unusual transactions we always evaluate D&I of process control activities that address RMMs.

Core and Less Complex | How do we obtain an understanding of business processes? [ISA | 1327.6357]

We obtain an understanding of business processes by either performing (i) a walkthrough or (ii) through inquiry and observation or inspection. Walkthroughs may be the most effective way to obtain our understanding.

Performing either (i) walkthroughs or (ii) inquiries and observations or inspections provide information about the entity's transactions, balances, disclosures and accounting policies or principles. This helps us identify and assess RMMs.

Core and Less Complex | For which business processes do we obtain an understanding and why? [ISA | 1327.2401]

We perform either (i) a walkthrough or (ii) inquiry and observation or inspection for all business processes that may have an RMM associated with them.

At this point in the risk assessment process, we have not yet identified RMMs, so we initially perform either (i) a walkthrough or (ii) inquiry and observation or inspection for each process associated with accounts, disclosures, relevant transactions, events and conditions that has a 'reasonable possibility' of having an RMM within the process. 'Reasonable possibility' means a more than remote possibility, and is therefore a low threshold. We assess both risks due to error and risks due to fraud. This includes those processes where the entity did not have any relevant transactions, but events and conditions exist that indicate there is a 'reasonable possibility" of having RMMs within the process. An RMM is a risk that could result in a material misstatement to the financial statements.

Since we either perform (i) walkthroughs or (ii) inquiries and observations or inspections as an input to determine whether an RMM exists and whether an account is a significant account or whether a disclosure is a significant disclosure, explaining when to obtain an understanding can be tricky.

We may exclude certain processes if we are reasonably certain that no RMM exists, either individually or in the aggregate (e.g. based on size and nature of the account). That may leave a remaining population where we do not know enough about the process to determine if there are associated RMMs. In those cases, we obtain further information about the process until we have sufficient knowledge to determine whether an RMM exists, this may include performing (i) a walkthrough or (ii) inquiry and observation or inspection.

Performing (i) walkthroughs or (ii) inquiries and observations or inspections allow us to gather information to identify and assess risk, so we are careful about when we decide not to perform them. We may end up performing (i) walkthroughs or (ii) inquiries and observations or inspections over business processes that ultimately do not contain an RMM, but these are procedures that allows us to make an informed decision about whether an RMM exists.

As we progress through the remainder of the risk assessment process and audit, we may identify RMMs where we have not yet performed either (i) a walkthrough or (ii) inquiry and observation or inspection of the processes associated with them. For example, we may identify RMMs related to the completeness of liability accounts that we originally did not have a 'reasonable possibility' of having an RMM associated with them. When we identify these new RMMs, we perform either a (i) walkthrough or (ii) inquiry and observation or inspection of the associated processes.

What are some examples when we may not identify any relevant transactions just events and conditions? [ISA | 1327.8699]

We may identify relevant events and conditions without transactions which may indicate that RMMs exist in a process.

For example:

- we identify that the entity lost significant customers during the financial year but have not recognized impairment losses on the relevant PPEs. This event indicates that there may be an RMM in the valuation of PPEs and may also impact the entity's ability to continue as a going concern and may cause liquidity issues.
- the entity has a loan from the prior year but there is no obligation for payment of instalments in the current year in accordance with the loan agreement. However, if the entity does not comply with the covenant requirements they have to repay the loan.

- the entity has a provision for a pending litigation from the prior year which remains unchanged in the current year. The development of the litigation in the current year may indicate necessary changes in the amount of the provision.

Core and Less Complex | Do we perform either (i) walkthroughs or (ii) inquiries and observations or inspections for business processes related to significant unusual transactions? [ISA | 1327.11236]

Yes. We perform either (i) walkthroughs or (ii) inquiries and observations or inspections for both routine processes, such as sales or procurement, and for significant unusual transactions, which may include transactions such as business combinations or impairment of goodwill.

When a business process uses a relevant service organization or sub-service organization, do we perform a walkthrough of the activities at the service organization or sub-service organization? [ISA | 1327.8616]

No. We do not walkthrough the processes at a relevant service organization or a sub-service organization when obtaining an understanding of the related business process. We do however identify PRPs around the relevant handoffs of data between the service organization and the entity (e.g., inputs and outputs), as well as any complementary user entity controls (CUEC). We also understand how the user entity uses service organization or sub-service organization (see activities 'Understand how the user entity uses service and sub-service organizations' and 'Understand the service organization's activities and internal controls')

What specifically do we understand when obtaining our understanding of a process? [ISA | 1327.8696]

When we obtain an understanding of a business process, we specifically understand each of the following items:

- how the application of accounting principles or policies is determined and implemented;
- how transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger and reported in the financial statements and related disclosures;
- how information about events and conditions, other than transactions, is captured, processed and included in the financial statements and related disclosures;
- the accounting records, specific accounts and disclosures in the financial statements and other supporting records relating to the flows of information in the information system;
- the entity's resources, including the IT environment, relevant to the business process.

We may not include parts of a business process that do not relate to financial reporting or that may not result in risks of material misstatement of the financial statements (e.g. parts of the business process only related to operational matters).

Refer to activity 'Understand the period-end financial reporting process' for additional information.

What are transactions? [ISA | 1327.1700]

Transactions are the entity's day-to-day contractual and transactional activities.

Why do we not refer to the "classes of transactions"? [ISA | 1327.1701]

KPMG methodology does not refer to the term "classes of transactions"; only "accounts." The auditing standards use the term "classes of transactions" to refer to groups of transactions with common characteristics that occurred during the period under audit (generally income statement accounts)

and "account balances" to refer to accounts balances at the period end (generally balance sheet accounts). The term "account" is intended to include both "classes of transactions" and "account balances".

What are accounting policies or principles? [ISA | 1327.1400]

Accounting policies or principles are standards and guidelines an entity selects and applies when preparing and presenting financial statements in accordance with a financial reporting framework.

For example, when US GAAP is the financial reporting framework, the FASB's Accounting Standards Codification is the authoritative source of accounting principles. US GAAP entities that are SEC registrants also follow SEC rules and interpretive releases.

Many accounting policies or principles set out in financial reporting frameworks are complex or call for considerable judgment. This is because the underlying economics of a business transaction may be complex or difficult to present without applying judgment or providing detailed disclosures.

In some cases, the financial reporting framework allows an entity to select an accounting principle from a number of alternatives. For example, the entity may have alternatives such as first-in-first-out (FIFO) or average cost for measuring its inventory costs. In other cases, the entity has no choice.

What else, other than relevant transactions, do we consider when obtaining our understanding of a process? [ISA | 1327.1900]

In addition to relevant transactions, we also consider how the information system captures relevant events and conditions.

Events and conditions are specific circumstances which are relevant to the entity when preparing its financial statements and related disclosures and may indicate that RMMs exist in a process or can influence our assessment of the inherent risk.

> For example, breach of loan covenants occurred (event) may affect the presentation of the loans in the financial statements and require additional disclosures or changes in income tax laws or rates that affect the recognition of income or deductibility of expenses (condition) may indicate that RMMs exist when the entity applies the new tax laws or rates.

As a result we also gain an understanding of those processes where the entity did not have any relevant transactions, but events and conditions exist that indicate there is a 'reasonable possibility' of having RMMs within the process.

What transactions, events and conditions might be relevant to processes? [ISA | 1327.11225]

The following are examples of transactions, events and conditions that may indicate the existence of RMM in the financial statements, at the financial statement level or the assertion level. The examples provided cover a broad range of transactions, events and conditions; however, not all transactions, events and conditions are relevant to every audit engagement and the list of examples is not necessarily complete.

Examples of transactions, events and conditions that may indicate the existence of RMM at the assertion level for accounts and/or disclosures:

Applicable financial reporting framework:

- Accounting measurements that involve complex processes.
- Application of new accounting pronouncements.
- 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.

Business model:

- Changes in the supply chain.
- Developing or offering new products or services, or moving into new lines of business.
- Commitments to make future payments under operating lease agreements.
- Compliance with debt covenants, or the entity's intent and ability to refinance current obligations on a long-term basis.

Capital:

- New constraints on the availability of capital and credit.

Customer loss:

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

Economic conditions:

- Operations in regions that are economically unstable, for example, countries with significant currency devaluation or highly inflationary economies.
- Changes in income tax laws or regulations that affect the entity's tax provision, such as changes in tax rates, or changes affecting the recognition of income or deductibility of expenses.

Entity structure:

- Changes in the entity such as large acquisitions or reorganizations or other unusual events.
- Entities or business segments likely to be sold.
- The existence of complex alliances and joint ventures.

Geography:

- Expanding into new locations.

Human resources competence:

- Changes in key personnel including departure of key executives.

Industry model:

- Changes in the industry in which the entity operates.

IT:

- Changes in the IT environment.
- Installation of significant new IT systems related to financial reporting.

Markets:

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

- External events and conditions that may affect the recoverability of an entity's long-lived assets, such as increases in competition, decreases in customer demand, or changes in the regulatory environment.

Regulatory:

- Operations that are subject to a high degree of complex regulation.
- Inception of investigations into the entity's operations or financial results by regulatory or government bodies.
- Impact of new legislation related to environmental protection.

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.
- Changes in litigation and contingency matters that affect the likelihood of an adverse outcome.
- Events or conditions that affect whether substantial doubt exists that the entity can continue as a going concern, and management's plans to alleviate such doubt.
- Opportunities for management and employees to engage in fraudulent financial reporting, including omission, or obscuring, of significant information in disclosures.

Transactions:

- Use of off-balance sheet finance, special-purpose entities, and other complex financing arrangements.
- Significant transactions with related parties.
- Significant amount of non-routine or non-systematic transactions including intercompany transactions and large revenue transactions at period end.
- Transactions that are recorded based on management's intent, for example, debt refinancing, assets to be sold and classification of marketable securities.

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

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

What if an entity's processes do not capture relevant events and conditions other than transactions? [ISA | 1327.11226]

If an entity's processes do not appropriately identify and capture relevant events and conditions, we may identify one or more control deficiencies in the Risk Assessment or Information and Communication component of ICFR.

We then consider the reasons for the assessed RMM when determining the nature, timing and extent of our audit procedures to respond to that RMM

What kind of resources are relevant to business processes? [ISA | 1327.8697]

Understanding the entity's information system also includes an understanding of the resources including the IT environment to be used in the entity's information processing activities.

Information about the human resources involved that may be relevant to understanding risks to the integrity of the information system include:

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

How do we obtain an understanding of the IT environment relevant to business processes?" [ISA | 1327.8698]

We obtain an understanding of the overall IT environment (refer to the activity "Understand how the entity uses IT as part of financial reporting"). We enhance this understanding as we understand business processes when we focus on understanding how data flows through the IT systems that are relevant to the business process.

Core and Less Complex | Do we obtain our understanding for just one transaction per business process? [ISA | 1327.2500]

It depends on whether there are different classes of transactions that flow through a business process. A single business process may relate to several significant accounts and disclosures. For example, a sales transaction for a commercial enterprise may impact not only sales and accounts receivable and related cash and cash equivalents accounts and disclosures, but possibly deferred revenue, sales returns, customer allowances, or other accounts and disclosures.

The table below shows more scenarios and how we might respond.

Scenario	How we might respond
Online and store sales: A retailer sells a product on its website and also through several physical locations. It is unclear whether both transaction types go through the same process.	It may be appropriate to select both an internet sales transaction and a retail store sales transaction, then trace each transaction until the processes they follow merge.
Opening an account online, at a branch or by post: A commercial bank offers a customer multiple options for initiating a transaction, such as opening a customer deposit (CD) account. A CD can be opened through the website, at a branch, or by post. Regardless of the option the customer chooses, the bank receives the same information and processes that information in the same manner.	If there are no unique process risk points related to the different ways a customer opens a CD, we may be able to follow a single transaction for the CD/account-origination process.

Sales and warranty reserve process: An entity's warranty reserve and sales process are closely linked. Information relevant to accounting for the warranty reserve is extracted from the same transactions that are part of the sales process. Both processes rely on quantity of units sold. However, each also relies on distinct information - e.g. accounting for the warranty reserve relies on the make and model of a part -i.e. a part number- while accounting for revenue relies on price per unit.	Because distinct information exists within the warranty reserve and sales process, we understand the flow of information related to each. It may be helpful to start with the previous year's disclosure in the financial statements, amounts recorded in the general ledger or input to the warranty reserve model, and follow the flow of information back to initiation.
New share-based payments awards: During our risk assessment procedures, we identified that management started issuing share-based payments to non-employees, with the resulting liability balance recorded in the accrued liability account.	These awards present a new RM that was not present in the prior year. We understand how these awards are initiated, authorized, processed, recorded and reported in the financial statements and related disclosures to be able to identify financial reporting risks and related controls.

When a transaction is processed at multiple locations, we may obtain an understanding of the entire information flow by understanding the input and output controls regarding how the entity manages the transmission of information to and from the other locations, and may use at least one transaction processed at each stage in the overall process. We may not necessarily use the same transaction to walkthrough, observe or inspect the related documentation.

For example, assume that a particular transaction:

- originates and undergoes initial transaction processing in an entity's Delhi, India office (initial processing),
- is batched with other transactions for further processing in the entity's Singapore office (intermediate processing), and
- is further batched with other intermediate processed transactions for final processing and, ultimately, reflected in the financial records in the entity's Atlanta corporate offices (final processing).

In this case, we do not necessarily use the same specific transaction that is initially processed in the Delhi office during our procedures in the Singapore or Atlanta locations. Rather we may select, at each processing location, an originating or input transaction for that location and trace it through the entity's information systems for each location until it is reflected in the output for that location.

Are there additional details we may obtain in understanding an entity's cash management or treasury process? [ISA | 1327.7953]

Yes. Obtaining a detailed understanding of an entity's bank accounts when conducting our risk assessment over the cash management or treasury process may be beneficial before performing substantive procedures. Additional details we may obtain in understanding an entity's cash management or treasury process may include the nature and purpose of the bank accounts held by the entity and specifically understanding:

- Whether there were bank accounts newly opened or closed during the period and the rationale for either;
- Where bank accounts are located and how such locations align with the entity's operational structure or strategic initiatives;
- What the purpose of the bank accounts are and how they link to other relevant business processes (e.g. revenue, payroll, accounts payable, etc.) or specific transactions (e.g. significant unusual transactions or related party transactions);
- Whether any bank accounts are managed by a third party (e.g., a trustee) and the reason why;
- Whether there are withdrawal restrictions and the reasons why;
- Whether any of the cash is held as collateral and the reasons why.

Does the group auditor obtain detailed understanding of an entity's bank accounts at all components? [ISA | 1327.7954]

Not necessarily. The group engagement team thinks about obtaining an understanding of a component's cash management or treasury process to assist them in assessing whether a risk of material misstatement exist related to existence of cash at components that have large cash positions or may have specific risks related to existence of cash.

> For example, the group engagement team may obtain an understanding of a component's cash management or treasury process to support our conclusions about whether RMMs exist if it is established as a central cash clearing house for a set of components in a particular region or it is used as the counterparty for the entity's debt and holds cash balances that are material to the group financial statements.

The component auditor may obtain detailed understanding of a component's bank accounts as part of understanding a component's cash management or treasury process at the components where the component engagement team have concluded that there is a reasonable possibility of a material misstatement, either individually or in the aggregate, related to cash and cash equivalents in the group financial statements.

Why do we obtain a detailed understanding of the bank accounts? [ISA | 1327.7955]

A detailed understanding of an entity's bank accounts enables us to identify situations when it is appropriate to disaggregate an RMM over cash and cash equivalents between different bank accounts when those accounts have different risk profiles.

> For example, management may use bank accounts in varying ways in different locations for different purposes (e.g. payroll, accounts payable and expense disbursement, treasury function

for interest and dividend receipts, or revenue receipts). In these situations, the related inherent risks may vary based on account/location/component because of differing risk profiles and our detailed understanding of the bank accounts and treasury process enables us to properly assess the risks present within cash and cash equivalents.

Core and Less Complex | Do we obtain an understanding of every type of transaction, events and conditions in a business process? [ISA | 1327.6420]

No, we only obtain an understanding of those transactions, events and conditions that have a 'reasonable possibility' of giving rise to a RMM within the process.

If we are obtaining an understanding of a business process through inquiry and observation or inspection, what questions may we ask? [ISA | 1327.6366]

We may ask questions similar to those when we perform a walkthrough. Refer to the question 'What questions do we ask during a walkthrough?'.

If the engagement is not an initial audit, supplementing our comprehensive understanding obtained in the prior years with inquiry in connection with other procedures may be sufficient. However, simply asking management to review prior year documentation of the process and requesting they confirm the documentation continues to properly reflect the process or that they update the documentation for changes is not sufficient as those procedures consist of inquiry alone.

If we are obtaining an understanding of a business process through inquiry and observation or inspection, what documents or items do we observe or inspect? [ISA | 1327.6368]

The documents or items we observe or inspect supports our inquiries. Because our inquiries primarily cover the initiation, processing, authorization, recording and reporting in the financial statements and related disclosures, the documents or items we observe or inspect evidence those aspects. Note that because we are not performing a walkthrough, we may not observe or inspect documents or items related to the same transaction all the way through the process. In many cases, the documents or items we observe or inspect in a process will also be documents or items we request and obtain as audit evidence to respond to an RMM in that process.

For example, in obtaining an understanding of an entity's revenue process, in addition to the inquiries, we may inspect documents that evidences the entity's revenue transactions through the process, such as purchase orders, invoices, shipping documents, and the related journal entries. We document our inspection of such documents as part of the narrative or flowchart.

Core and Less Complex | How might we involve others in obtaining an understanding of business processes? [ISA | 1327.63612]

We may ask others - for example, specific team members with expertise in tax and IT or employed KPMG valuation specialists - to assist with certain procedures when we obtain an understanding of business processes.

We may ask them to:

- participate in 'whiteboarding' sessions;

- participate in a walkthrough where applicable or inquiring of entity personnel and observation or inspection procedures;
- help prepare narrative documentation or flowchart data and transactions; and
- review narrative or flowchart documentation prepared by the entity or other members of the engagement team.

Core and Less Complex | When might we involve IT Audit in obtaining an understanding of business processes? [ISA | 1327.157461]

IT Audit may be particularly helpful when we perform procedures to obtain an understanding of business processes that involve IT systems, such as:

- obtaining an understanding of how IT affects the flow of data and information related to relevant transactions, events and conditions; and
- inspecting IT systems and other relevant documentation showing how IT systems are used to process data and transactions.

Core and Less Complex | When obtaining an understanding of business processes, what is the extent of IT Audit's involvement? [ISA | 1327.11241]

When we involve IT Audit throughout risk assessment, we are likely to obtain a better understanding of the process.

If we limit IT Audit's involvement, they may not adequately understand the IT environment, IT's impact on business processes or the related risks.

Even so, the nature and extent of their involvement in our (i) walkthroughs or (ii) inquiries and observations or inspections may depend on the extent to which a process relies on IT and the level of IT knowledge held by non-IT Audit team members.

Enhanced | How might we involve others in obtaining an understanding of business processes? [ISA | 1327.6361]

We may ask others - for example, specific team members with expertise in tax and IT or employed KPMG valuation specialists - to assist with certain procedures when we obtain an understanding of business processes.

We may ask them to:

- participate in 'whiteboarding' session;
- participate in a walkthrough where applicable or inquiring of entity personnel and observation or inspection procedures
- help prepare narrative documentation or flowchart data and transactions; and
- review narrative or flowchart documentation prepared by the entity or other members of the engagement team.

See question "How do we obtain an understanding of business processes?" for guidance on when to perform (i) a walkthrough or (ii) inquiry and observation or inspection based on the applicable International-Enhanced methodology.

When might we involve IT Audit in obtaining an understanding of business processes? [ISA | 1327.11230]

IT Audit may be particularly helpful when we perform procedures to obtain an understanding of business processes that involve IT systems, such as:

- obtaining an understanding of how IT affects the flow of data and information related to relevant transactions, events and conditions; and
- inspecting IT systems and other relevant documentation showing how IT systems are used to process data and transactions.

Enhanced | When obtaining an understanding of business processes, what is the extent of IT Audit's involvement? [ISA | 1327.11231]

When we involve IT Audit throughout risk assessment, we are likely to obtain a better understanding of the process. If we limit IT Audit's involvement, they may not adequately understand the IT environment, IT's impact on business processes or the related risks.

Even so, the nature and extent of their involvement in our (i) walkthroughs or (ii) inquiries and observations or inspections may depend on the extent to which a process relies on IT and the level of IT knowledge held by non-IT Audit team members.

See question "How do we obtain an understanding of business processes?" for guidance on when to perform a (i) walkthrough or (ii) inquiry and observation or inspection based on the applicable International-Enhanced methodology.

Core and Less Complex | How do we evidence our understanding of business processes? [ISA | 1327.2302]

As the engagement team, we evidence our understanding of the business processes through the preparation of a narrative or flowchart.

If we decide to use flowcharts to document our understanding of processes, we do so in accordance with the activity 'Prepare or use the entity's flowcharts to document our understanding of processes'.

When we decide to use narratives, we document our understanding of processes in accordance with the question 'How do we prepare a narrative?'.

Enhanced | How do we evidence our understanding of business processes? [ISA | 1327.2301]

As the engagement team, we evidence our understanding of the business processes based on the applicable International-Enhanced methodology as follows:

Applicable International-Enhanced methodology	Processes	Evidence our understanding of the process through a:
International-Enhanced PIE methodology	All processes and sub-processes	Flowchart
International-Enhanced Non-PIE methodology	Processes, or sub-processes, where we evaluate D&I of process control activities that address RMMs	Flowchart

	Processes, or sub-processes, where we do not evaluate D&I of process control activities that address RMMs	Either (i) flowchart or (ii) narrative

See question "Which control activities do we obtain an understanding of and are relevant to the audit?"for guidance on when we evaluate D&I of process control activities that address RMMs.

If we use flowcharts to document our understanding of processes, we do so in accordance with the activity 'Prepare or use the entity's flowcharts to document our understanding of processes'.

When we decide to use narratives, we document our understanding of processes in accordance with the question 'How do we prepare a narrative?".

What is a narrative? [ISA | 1327.6364]

A narrative is a written detailed description of our understanding of the process.

How do we prepare a narrative? [ISA | 1327.6365]

To prepare a narrative, we:

(1) Identify the business or accounting process we will gain an understanding of;
(2) Perform inquiry and observation or inspection to obtain an understanding of the process (refer to question 'What specifically do we understand when obtaining our understanding of a process?'); and
(3) Document our understanding in a narrative format.

1.1.2.1.1 Perform a walkthrough to understand the business processes [ISA | 1328]

What do we do?

Perform a walkthrough of business processes where there is a reasonable possibility that an RMM exists within the process.

Why do we do this?

A walkthrough is a risk assessment procedure that gives us an understanding of business processes, including information systems. We use the information we gather to identify and assess RMMs.

Execute the Audit

What is a walkthrough? [ISA | 1328.1300]

A walkthrough is an audit procedure in which we follow, or 'trace', a transaction from origination, through the entity's processes and information systems, until it is reflected in the financial records. We also understand how information about transactions are reported in the financial statements and related disclosures.

For an event or condition, we walkthrough how information about the event or condition captured, processed and included in the financial statements and related disclosures.

We use the same documents and IT that the entity's personnel use.

What are the objectives of a walkthrough? [ISA | 1328.1400]

The objective of a walkthrough is to understand the process and flow of transactions as a risk assessment procedure to identify and assess RMMs.

When we evaluate the design and implementation of control activities as part of our risk assessment process, a walkthrough can also meet the objective of identifying process risk points (PRPs).

Once we've identified PRPs[(the 'where' and the 'how' a misstatement could occur), we then identify the relevant process control activities which address the PRPs and evaluate the design and implementation of these control activities management relies on to mitigate PRPs in audits when there are relevant process control activities (see activity 'Determine which control activities are relevant to the audit')

How do these objectives affect how we perform the walkthrough? [ISA | 1328.11301]

A walkthrough is primarily about *understanding* the process. This is not the same as, but will lead to, identifying process risk points and process control activities relevant to the audit and ultimately to evaluating the design and implementation of those process control activities when we evaluate the design and implementation of process control activities.

Misunderstandings in the objectives of a walkthrough can lead to deficiencies in the procedures or extent of evidence we gather. If we perform walkthroughs with a narrow focus on one objective, we run the risk of not meeting each of the others.

For example, if we execute our walkthroughs principally to evaluate the design and implementation of control activities, we may fail to gather an understanding of the whole process. We might not have a basis for our identified or assessed RMMs, or we might not identify a complete set of process risk points.

Such failures have downstream effects. For example, we may not identify and evaluate a complete set of relevant control activities or identify that a control is not designed properly.

How do we conduct a walkthrough? [ISA | 1328.11302]

To conduct an effective walkthrough, we complete the following steps.

(1) Identify the business processes we will walkthrough
(2) Prepare for the walkthrough, which may include holding pre-walkthrough risk assessment sessions
(3) Conduct a walkthrough of the identified business process, including asking probing questions

What do we consider when holding a pre-walkthrough risk assessment session? [ISA | 1328.11304]

In preparing for a walkthrough we may hold a pre-walkthrough risk assessment session. This collaborative team-based session provides an opportunity to:

- articulate the engagement team's preliminary understanding of the flow of information by using whiteboarding techniques;

- discuss or revisit initial walkthrough planning decisions to confirm they are appropriate (e.g. engagement team member assignments, entity's personnel that will be involved in walkthrough procedures, involvement of others, walkthrough schedule etc.);
- prepare for walkthrough procedures, including discussion of the importance of probing questions and identification of areas where follow-up questions and more detailed understandings to be addressed during the walkthrough;
- make a preliminarily identification of the relevant RMs.

We may also use prior year financial statements, including related disclosures, to prepare for walkthrough procedures.

What is 'whiteboarding'? [ISA | 1328.11305]

Whiteboarding is a brainstorming session where we, as an engagement team, visually draw out our preliminary understanding of the process.

A whiteboarding session can help us plan for a walkthrough, including identifying parts of the process we may not understand well and outlining questions we plan to ask during the walkthrough.

Who performs walkthroughs? [ISA | 1328.1700]

Walkthroughs are performed by members of our engagement team with sufficient experience to perform them appropriately, including asking the right probing questions. Depending on the process, we may involve more than one member of the engagement team in each walkthrough.

Because each business process or information system may pose a different level of risk, the extent of our audit procedures - i.e. inquiry, inspection or observation - and who performs the walkthrough procedures may differ. For example, specific team members with expertise in IT may be involved in walkthroughs when the engagement team believes IT applications will be relevant to our process understanding. For business processes that relate to more complex or subjective accounting topics or areas of the audit that are expected to have a higher volume of RMMs, involvement of more experienced team members may be necessary.

Can we use the work of internal audit in performing our walkthroughs? [ISA | 1328.157289]

Remember: the primary purpose of a walkthrough is for us to obtain an understanding of the information system and business processes relevant to financial reporting. To do this properly, we walkthrough the processes ourselves, which includes supervising the work of internal auditors if we use them to provide direct assistance. We do not use the work of the internal audit function.

What is the starting point of a walkthrough? [ISA | 1328.11306]

When we perform a walkthrough, we start the walkthrough where the transaction first originates (e.g. the 'boundary' of the business process) rather than at the earliest process control activity identified.

As we prepare to perform a walkthrough, we think of whether we've appropriately identified the boundary or boundaries. Identifying the boundary of a business process can help us to set the scope of the business process and start our walkthrough and process documentation where the process actually starts. Where multiple boundaries are identified (e.g. customer can initiate transactions online, using a mobile phone, EDI, in store, etc.), we determine if we need to walkthrough at each boundary.

Enhanced | Do we walkthrough just one transaction per business process? [ISA | 1328.11298]

Not necessarily. As we perform our risk assessment procedures, we may become aware that there are different classes of transactions that flow through the business process. To sufficiently understand the business process, we may perform a walkthrough of a transaction in several sub-processes where there is a reasonable possibility that an RMM exists or we do not know enough about the sub-process to determine if there are associated RMMs.

A single transaction may relate to several significant accounts and disclosures. For example, a sales transaction for a commercial enterprise may impact not only sales and accounts receivable, but possibly deferred revenue, sales returns, customer allowances, or other accounts. We may perform a walkthrough of multiple transactions in order to understand each part of the business process.

The table below shows more scenarios and how we might respond.

Scenario	How we might respond
Online and store sales: A retailer sells a product on its website and also through several physical locations. It is unclear whether both transaction types go through the same process.	It may be appropriate to select both an internet sales transaction and a retail store sales transaction, then trace each transaction until the processes they follow merge.
Opening an account online, at a branch or by post: A commercial bank offers a customer multiple options for initiating a transaction, such as opening a customer deposit (CD) account. A CD can be opened through the website, at a branch, or by post. Regardless of the option the customer chooses, the bank receives the same information and processes that information in the same manner.	If there are no unique process risk points related to the different ways a customer opens a CD, we may be able to follow a single transaction for the CD/account-origination process.
Sales and warranty reserve process: An entity's warranty reserve and sales process are closely linked. Information relevant to accounting for the warranty reserve is extracted from the same transactions that are part of the sales process. Both processes rely on quantity of units sold. However, each also relies on distinct information - e.g. accounting for the warranty reserve relies on the make and model of a	Because distinct information exists within the warranty reserve and sales process, we understand the flow of information related to each. It may be helpful to start with the previous year's disclosure in the financial statements, amounts recorded in the general ledger or input to the warranty reserve model, and follow the flow of information back to initiation.

part -i.e. a part number- while accounting for revenue relies on price per unit.	
New share-based payments awards: During our risk assessment procedures, we identified that management started issuing share-based payments to non-employees, with the resulting liability balance recorded in the accrued liability account.	These awards present a new RM that was not present in the prior year. We understand how these awards are initiated, authorized, processed, recorded and reported in the financial statements and related disclosures to be able to identify financial reporting risks and related controls.

When a transaction is processed at multiple locations, we may obtain an understanding of the entire information flow by understanding the input and output controls regarding how the entity manages the transmission of information to and from the other locations, and may use at least one transaction processed at each stage in the overall process. We may not necessarily use the same transaction to walkthrough.

For example, assume that a particular transaction:

- originates and undergoes initial transaction processing in an entity's Delhi, India office (initial processing),
- is batched with other transactions for further processing in the entity's Singapore office (intermediate processing), and
- is further batched with other intermediate processed transactions for final processing and, ultimately, reflected in the financial records in the entity's Atlanta corporate offices (final processing).

In this case, we do not necessarily use the same specific transaction that is initially processed in the Delhi office during our walkthrough procedures in the Singapore or Atlanta locations. Rather we may select, at each processing location, an originating or input transaction for that location and trace it through the entity's information systems for each location until it is reflected in the output for that location.

How do we follow a transaction through the process? [ISA | 1328.11299]

In a walkthrough, we follow:

- how transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger and reported in the financial statements and related disclosures; and
- how information about events and conditions, other than transactions, is captured, processed and included in the financial statements and related disclosures.

We use the same documents and information technology that management use when performing the process.

We follow the flow of information (or transaction data) by inspecting key documents, reports and third-party deliverables within the process.

Do we walkthrough the whole process or just the process control activities? [ISA | 1328.11300]

We walkthrough the parts of an entity's process that relate to financial reporting or that may result in risks of material misstatement of the financial statements and related disclosures, not the process control activities. While performing a walkthrough of the process, we will likely discuss different process risk points and process control activities. However, our focus is to gain an understanding of the process to help us to identify and assess risks of material misstatement and process risk points, when relevant.

Enhanced | Do we obtain an understanding of every type of transaction, events and conditions in a business process? [ISA | 1328.6460]

No, we only obtain an understanding of those transactions, events and conditions that have a 'reasonable possibility' of giving rise to a RMM within the process.

What questions do we ask during a walkthrough? [ISA | 1328.2000]

When we perform a walkthrough, we question the entity's personnel at the points at which important processing procedures occur about their understanding of what those procedures entails.

These probing questions, combined with the other walkthrough procedures, allow us to gain a sufficient understanding of the process and to use this information in determining our risk assessment procedures.

Additionally, probing questions that go beyond a narrow focus on the single transaction used as the basis for the walkthrough allow us to gain an understanding of the different types of significant transactions handled by the process.

Area of understanding	Example questions
Initiation	• Can you describe for me what happened previously in the process? • Can you describe for me what happens next in the process?
Authorization	• Can you describe for me how this transaction is authorized?
Processing	• Can you describe for me any data processing that occurs within the IT system? • Can you describe for me how data is transferred from one IT system to the other?
Recording and correcting as necessary	• Can you explain to me how you determine which general ledger account the transaction is recorded to? • Can you explain to me how incorrect entries in the general ledger get corrected?

	• Can you explain the accounting policies or principles applied to record the transaction?
Reported in the financial statements including related disclosures	• Can you describe to me the process to develop the disclosure? • Can you explain the source of information used to develop the disclosure?
Other transaction flows	• Is the transaction typical of all transactions that flow through the process, or do other transactions follow a different process? • Are there differences in the way you process the transactions depending on the details of the items?

Do we follow the transaction through IT systems in a walkthrough? [ISA | 1328.11309]

Yes. We follow the transaction selected *through* the relevant IT systems, not around them, so we can fully understand the flow of transactions. This includes understanding:

- how data enters into an IT system; and
- how it is stored, processed and accumulated for use in the operation of controls and for preparing financial statements.

We also understand how data associated with the transactions flows through information systems, including which applications, databases and other system components accept, maintain, manipulate and move the data.

Is there anything additional to consider when accounting estimates are involved? [ISA | 1328.11312]

Yes. We follow the procedures in activity 'Understand the process by which accounting estimates are developed.'

Enhanced | How often do we perform a walkthrough of each relevant process? [ISA | 1328.2100]

We perform a walkthrough of each relevant business process at least annually. We update our understanding of a business process more frequently (i.e., during the year) if changes in circumstances indicate.

Why do we perform the walkthrough each year? [ISA | 1328.11310]

Performing a walkthrough each year allows us to update our understanding of the business processes. Processes change over time due to a variety of factors, including personnel changes, changes in the way transactions are effected, changes in technology, etc.

These changes are inputs to our risk assessment, and provide information to help us identify and assess RMMs.

How much can we rely on our prior-year knowledge in performing a walkthrough? [ISA | 1328.11311]

While prior-year knowledge of an entity's processes and control activities may be informative, we do not rely on that knowledge because external or internal influences might have caused changes to the processes or presented new process risk points.

Fact pattern:

Because we audited the entity last year, we are confident we know which control activities to test. We ask management if anything has changed with respect to its ICFR. Management indicate that nothing has changed within the entity.

We obtain management's list of 'key' control activities, compare them to the control activities tested in the prior year and test the identified control activities in the same manner we tested them in prior audits.

Analysis:

In this instance, we did not obtain a sufficient understanding of the process in the current year and inappropriately relied on management's assertion. As a result, we fail to identify changes to the process and related process risk points that would lead us to test different control activities and/or alter our approach to testing certain control activities in the current year.

How do we document a walkthrough? [ISA | 1328.1600]

As with all audit procedures, walkthrough documentation allows an experienced auditor, with no prior experience with the entity, to reperform the walkthrough procedures. This involves the below.

The transaction(s), event or condition we followed / understood, location of the walkthrough, what we traced, and the participants	• Relevant identifiers of the documentation we traced (e.g. invoice number, invoice date, and invoice amounts); • How the transaction was initiated, authorized, processed and recorded in systems, until it is reflected in the entity's financial records; • How information about the event or condition is captured, processed, and included in the financial statements and related disclosures; • Flow of data through systems and spreadsheets, physical movements (if the walkthrough involved physical assets); and • Who we talked to along the way, including our probing questions and responses.

We may also include the documents or screenshots that we inspected or observed throughout the walkthrough. However, if we elect to record the walkthrough, the recording is not included within our audit documentation nor is it kept beyond the time period for which it is needed in accordance with the firm's retention and/or preservation guidelines, as applicable.

Examples

What is the difference between a process and a control activity? [ISA | 1328.2200]

Consider the descriptions below for the preparation and review of the tax packages. Are they describing the process or the control activity that's occurring?

Description	Process or control activity?
The Tax Director prepares a quarterly tax package to support the uncertain tax positions. The tax package includes a memo on new tax positions and tax positions that indicates a re-evaluation based on activity that occurred during the period -e.g. tax return filings, tax audits, settlements etc. The memo includes a summary and detailed roll-forwards of the uncertain tax positions, detailed calculations of the liability, interest and penalties, and other supporting documents such as legal/tax opinions, tax returns, and relevant court rulings, where appropriate.	This is a *process*, as it involves the preparation of the tax package, which is part of the steps the entity takes to record and disclose uncertain tax positions.
Every quarter, the Tax Vice President reviews the uncertain tax position liability for existence, completeness, accuracy and valuation. As part of this, he reviews the tax package prepared by the Tax Director and his team.	This is a *control activity*, as it involves the Tax Vice President reviewing information from the tax package that was created as part of the process.
As part of an entity's adoption of the new revenue recognition standard, an individual within the accounting department reviews a significant revenue contract, summarizes the terms of the contract and analyzes the related accounting implications in a contract summary form.	This is a *process*, as it involves how the entity initially analyzes the impact of adopting the new revenue recognition standard for a particular contract so that it can be accounted for and recorded appropriately. If the analysis was reviewed by an individual other than the initial preparer, the review performed is a *control activity*.

What are the consequences of doing a walkthrough of the control activities instead of the process? [ISA | 1328.2300]

The table below highlights what we might miss if we walkthrough controls instead of the process.

Scenario	What was missed?
The process owners provide a brief narrative describing how each control operates and provide example documentation.	In this scenario, we may miss the flow of the transaction from initiation through to the recording in the general ledger because it focuses only on certain controls and not on the entire process. If we fail to properly walkthrough the process, we risk not identifying all the relevant process risk points. Since the process risk points inform us as to the controls necessary, we may also fail to properly identify and/or evaluate the design and implementation of the process control activities that address the process risk points.
Management perform an annual update of their business process narratives, and then we select a completed transaction for a walkthrough of each process. In the walkthrough, we only focus on obtaining evidence that the selected transaction was subjected to the relevant controls management identified.	In this scenario, we focus on the controls again, and miss identifying the process risk points. This is not an appropriate approach for obtaining an understanding of a process and identifying relevant process risk points and the process control activities within the process.

1.1.2.2 Understand the period-end financial reporting process [ISA | 795]

What do we do?

Obtain an understanding of the period-end financial reporting process.

Why do we do this?

The period-end financial reporting process is a critical process that exists for all entities. In it, an entity compiles information from each related business processes, selects and applies accounting policies or principles, records recurring and non-recurring journal entries and other adjustments, and prepares the financial statements, including the related disclosures. The period-end financial reporting process is the last process to occur before the financial statements are issued, therefore it is important for the entity to have well designed and effective period-end financial controls, as errors or fraud in the period-end

financial reporting process can override effective control activities that occur throughout the entity's other processes.

Execute the Audit

What is the period-end financial reporting process? [ISA | 795.1300]

The period-end financial reporting process is the activities an entity or group performs to close the books and make post-closing adjustments when preparing the individual financial statements (e.g. balance sheet, statement of income) and related disclosures, collectively referred to as the financial statements. This process generally operates after or outside of the other processes and process control activities designed to record individual transactions.

What are the processes and procedures in the period-end financial reporting process? [ISA | 795.8654]

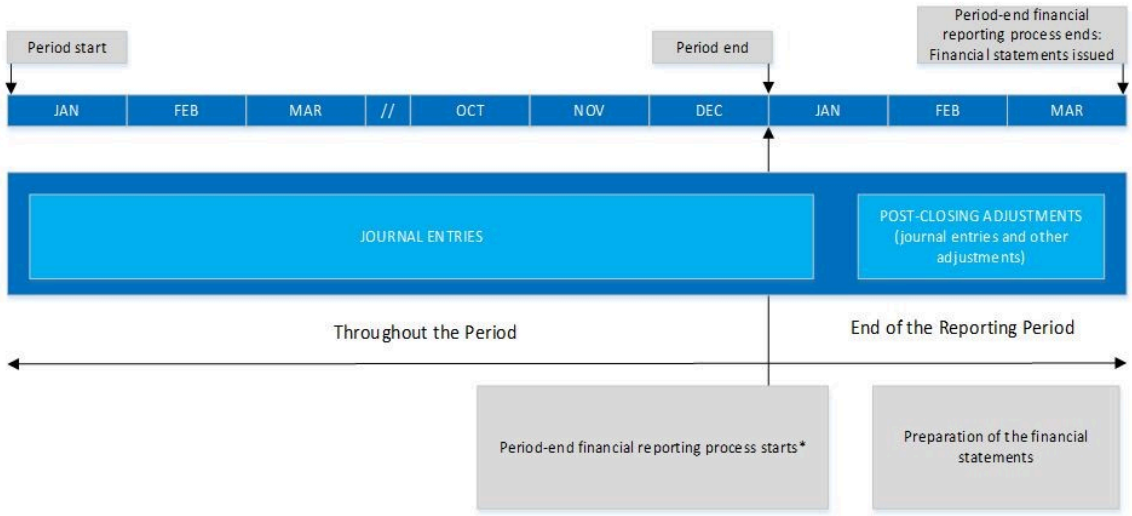
It includes process and procedures, hereafter referred to as financial reporting sub-processes, for:

Financial Reporting Sub-Process	Representative activities that are performed
Understand processes and procedures to enter transaction totals into the general ledger	Entering transaction totals into the general ledger and other systems (e.g. consolidation systems) Consolidating subsidiaries and other entities (e.g. variable interest entities) Translating local currency financial reporting packages into an entity's functional or reporting currency
Initiating, authorizing, recording, and processing journal entries and other adjustments	Initiating, authorizing, recording, and processing of recurring journal entries, including consolidating journal entries Initiating, authorizing, recording, and processing of nonrecurring journal entries and other adjustments
Preparation of annual and quarterly financial statements and related disclosures	Preparing current period financial statements (e.g. balance sheet, statements of income, comprehensive income, shareholders' equity, and cash flows) Preparing comparative period financial statements Identifying financial statement disclosure requirements, including earnings per share Identifying non-routine transactions requiring disclosure in the footnotes to the financial statements Preparing financial statement disclosures Assessing going concern assumptions

	Identifying and assessing the impact of subsequent events Identifying and assessing reportable segments

Where does the period-end financial reporting process start? [ISA | 795.13551]

The period-end financial reporting process starts when data is extracted from sub-ledgers used as part of business processes in order to enter the transactions into a general ledger that is used to record the accumulation of transactions from all business processes.



**The period-end financial reporting process begins before, at, or after the entity's period-end, depending on the entity's schedule.*

Where does the period-end financial reporting process end? [ISA | 795.1400]

The period-end financial reporting process ends when the entity issues or reports its final financial statements and disclosures.

When do we obtain an understanding of the period-end financial reporting process? [ISA | 795.13558]

We obtain an understanding of the entity's period-end financial reporting and related business processes as part of our risk assessment procedures.

In addition, we obtain an understanding of the entity's period-end financial reporting process prior to determining the nature, timing, and extent of our testing of journal entries and other adjustments as part of our response to management override of controls through the recording of journal entries and other adjustments.

What if new information comes to our attention when we perform other audit procedures? [ISA | 795.14041]

When new information comes to our attention when performing other audit procedures - e.g. as we complete the process of reconciling sub-ledgers to ledgers, accounting ledgers from one system

to another system, the accounting ledgers to the financial statements and how the disclosures are prepared, we update our understanding of the period-end financial reporting process and evaluate the effect of this new information on our risk assessment and the nature, timing, and extent of our testing of journal entries and other adjustments.

Enhanced | How do we obtain an understanding of the period-end financial reporting process? [ISA | 795.13552]

We obtain an understanding of each of the sub-processes of the period-end financial reporting process based on the applicable International-Enhanced methodology as follows:

Applicable International-Enhanced methodology	Sub-process of the period-end financial reporting process	Obtain an understanding of the sub-process by:
International-Enhanced PIE methodology	All sub-processes of the period-end financial reporting process listed in the question "What are the processes and procedures in the period-end financial reporting process?"	Performing a walkthrough
International-Enhanced Non-PIE methodology	Initiating, authorizing, recording, and processing journal entries and other adjustments sub-process (*) Sub-processes where we evaluate D&I of process control activities that address RMMs	Performing a walkthrough
	Sub-processes where we do not evaluate D&I of process control activities that address RMMs	Either performing (i) a walkthrough or (ii) through inquiry and observation or inspection. Walkthroughs are encouraged.
* We always perform a walkthrough for this sub-process since it involves journal entries and other adjustments, and we 'Evaluate the design and implementation of control activities over journal entries and other adjustments'.		

See question 'Which control activities do we obtain an understanding of and are relevant to the audit?' for guidance on when we evaluate D&I of process control activities that address RMMs.

Performing a walkthrough, if applicable, of the period-end financial reporting process and its sub-processes will not necessarily involve following a 'single transaction' through the process, because the period-end financial reporting process involves the entering of transactions into the entity's general ledger and consolidation systems and the reporting of the accumulation of transactions in the financial statements and related disclosures.

Therefore, our walkthrough follows the flow of data from the general ledger and consolidation systems to the consolidated financial statements and related disclosures for a particular financial reporting period.

As activities within the sub-processes of the period-end financial reporting process are related to or derived from transactions, events and conditions in business processes, we may have understood aspects of these activities in connection with our understanding of the business process.

> For example, in connection with understanding the process related to additions to Property, Plant and Equipment, we understood the selection and application of the accounting policy for capitalization as well as how additions are included in the financial statements and related disclosures.

For those period-end financial reporting sub-processes and representative activities not included in our understanding of the business process, we obtain an understanding of them in connection with the period-end financial reporting process.

To understand the complete flow of information, it may be effective to double-check our understanding by looking at the final financial statements and tracing the consolidated information back to respective information sources, and/or to where we ended our transactions in the various business processes.

Enhanced | How do we document our understanding of the period-end financial reporting process?

[ISA | 795.157351]

We document our understanding of each of the sub-processes of the period-end financial reporting process based on the applicable International-Enhanced methodology as follows:

Applicable International-Enhanced methodology	Sub-process of the period-end financial reporting process	Document our understanding of the process through a:
International-Enhanced PIE methodology	All sub-processes of the period-end financial reporting process listed in the question 'What are the processes and procedures in the period-end financial reporting process?'	Flowchart
International-Enhanced Non-PIE methodology	Initiating, authorizing, recording, and processing	Flowchart

	journal entries and other adjustments sub-process (*) Sub-processes where we evaluate D&I of process control activities that address RMMs	
	Sub-processes where we do not evaluate D&I of process control activities that address RMMs	Either (i) flowchart or (ii) narrative

***** We always document our understanding of this sub-process through a flowchart since it involves journal entries and other adjustments, and we 'Evaluate the design and implementation of control activities over journal entries and other adjustments'.

See question 'Which control activities do we obtain an understanding of and are relevant to the audit?' for guidance on when we evaluate D&I of process control activities that address RMMs.

If we use flowcharts to document our understanding of processes, we do so in accordance with the activity 'Prepare or use the entity's flowcharts to document our understanding of processes'

When we decide to use narratives, we document our understanding of processes in accordance with the question 'How do we prepare a narrative?'.

What elements are included in our understanding of the period-end financial reporting process? [ISA | 795.14049]

When we obtain an understanding of the period-end financial reporting process, we determine:

- the inputs, procedures performed, and outputs of the processes the entity uses to produce its financial statements and related disclosures;
- the resources, including: 1) the extent of IT involvement (i.e. IT environment), relevant in the period-end financial reporting process, and 2) who participates from management;
- the locations involved in the period-end financial reporting process;
- the types of adjusting and consolidating entries; and
- the nature and extent of the oversight of the process by management and those charged with governance.

Core and Less Complex | How do we obtain an understanding of the period-end financial reporting process? [ISA | 795.135525]

We obtain an understanding of each of the sub-processes of the period-end financial reporting process listed in the table in the question 'What are the processes and procedures in the period-end financial reporting process?' by performing either (i) a walkthrough or (ii) inquiry and observation or inspection. Walkthroughs may be the most effective way to obtain our understanding.

A walkthrough of the period-end financial reporting process and its sub-processes will not necessarily involve following a 'single transaction' through the process, because the period-end financial reporting

process involves the entering of transactions into the entity's general ledger and consolidation systems and the reporting of the accumulation of transactions in the financial statements and related disclosures.

Therefore, our walkthrough follows the flow of data from the general ledger and consolidation systems to the consolidated financial statements and related disclosures for a particular financial reporting period.

As activities within the sub-processes of the period-end financial reporting process are related to or derived from transactions, events and conditions in business processes, we may have understood aspects of these activities in connection with our understanding of the business process.

> For example, in connection with understanding the process related to additions to Property, Plant and Equipment, we understood the selection and application of the accounting policy for capitalization as well as how additions are included in the financial statements and related disclosures.

For those period-end financial reporting sub-processes and representative activities not included in our understanding of the business process, we obtain an understanding of them in connection with the period-end financial reporting process.

To understand the complete flow of information, it may be effective to double-check our understanding by looking at the final financial statements and tracing the consolidated information back to respective information sources, and/or to where we ended our transactions in the various business processes.

Core and Less Complex | What elements are included in our understanding of the period-end financial reporting process? [ISA | 795.157460]

When we obtain an understanding of the period-end financial reporting process, we determine:

- the inputs, procedures performed, and outputs of the processes the entity uses to produce its financial statements and related disclosures;
- the resources, including: 1) the extent of IT involvement (i.e. IT environment), relevant in the period-end financial reporting process, and 2) who participates from management;
- the locations involved in the period-end financial reporting process;
- the types of adjusting and consolidating entries; and
- the nature and extent of the oversight of the process by management and those charged with governance.

Core and Less Complex | How do we document our understanding of the period-end financial reporting process? [ISA | 795.13554]

Like with other processes, we document our understanding of the period-end financial reporting process through the preparation of a narrative or flowchart.

If we use flowcharts to document our understanding of processes, we do so in accordance with the activity 'Prepare or use the entity's flowcharts to document our understanding of processes'

When we decide to use narratives, we document our understanding of processes in accordance with the question 'How do we prepare a narrative?'.

How do we use the knowledge obtained regarding the period-end financial reporting process when we perform a financial statement audit? [ISA | 795.13555]

When we perform a financial statement audit (FSA), we use the knowledge obtained regarding the period-end financial reporting process to:

- identify and assess risks of material misstatement (RMM), including the risk of management override of controls; and
- determine the nature, timing, and extent of our testing of journal entries and other adjustments.

How do we use the knowledge obtained to identify and assess RMMs? [ISA | 795.13556]

The knowledge we obtain regarding the period-end financial reporting process may result in the identification of financial statement and assertion level RMMs, such as:

- omission, advancement, or delay of the recognition in the financial statements and related disclosures of events and transactions that have occurred during the period;
- omission, obscurement, or misstatement of disclosures required by the applicable financial reporting framework, or disclosures that are necessary to achieve fair presentation; or
- concealment of facts that could affect the amounts recorded in the financial statements.

How do we use the knowledge obtained to determine the nature, timing, and extent of testing of journal entries and other adjustments? [ISA | 795.13557]

When we determine the nature, timing, and extent of the procedures we plan to perform to test journal entries and other adjustments and the criteria we use to identify and select high risk journal entries and adjustments, we consider knowledge obtained about the financial reporting process, including sub-processes related to:

- the process and procedures to enter transaction totals into the general ledger; and
- the process and procedures related to journal entries and other adjustments.

1.1.2.2.1 Understand processes and procedures to enter transaction totals into the general ledger [ISA | 796]

What do we do?

Understand processes and procedures used to enter transaction totals into general ledger(s)

Why do we do this?

The process and procedures to enter transaction totals into the general ledger is a sub-process of the financial reporting process, which exists for all entities. Understanding the financial reporting process and its sub-processes helps us to:

- identify and assess risks of material misstatement (RMMs), including the risk of management override of controls and the risk that journal entries could be susceptible to unauthorized or inappropriate intervention or manipulation; and
- determine the nature, timing, and extent of our testing of journal entries and other adjustments.

Execute the Audit

How does an entity enter transaction totals into the general ledger? [ISA | 796.8599]

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 process and procedures used to enter transaction totals into the general ledger will depend on whether or not the entity uses separate transaction processing and general ledger IT systems.

For example, an entity may use an integrated enterprise resource planning (ERP) IT system that integrates all processes, including financial reporting and related business processes, into a single IT system. In these instances, there may not be separate processes and procedures to enter transaction totals into the general ledger and transactions processed using different modules within the ERP system are often transferred to and recorded in the general ledger using automated journal entries. Other entities may use multiple systems or sub ledgers that are not integrated and enter transaction totals from those systems and sub ledgers into the general ledger.

What are journal entries? [ISA | 796.1300]

Journal entries are any entries made directly within the general ledger system that are used to record transactions, allocations, adjustments and corrections. They include:

- standard journal entries used to record recurring transactions and adjustments; and
- non-standard journal entries used to record non-recurring, unusual transactions, or adjustments.

What are standard journal entries? [ISA | 796.13373]

Standard journal entries are journal entries used to record:

- recurring transactions - e.g., the day to day activities of the entity such as recurring sales, purchases, and cash disbursements; and
- recurring adjustments - e.g., adjustments related to accounting estimates that are made at each period-end such as changes in the estimate of uncollectible accounts receivable.

What are automated journal entries? [ISA | 796.13374]

Automated journal entries are standard journal entries that are automatically initiated, authorized, recorded and processed in the general ledger. The use of automated journal entries can reduce the risk of management override of controls because automated journal entries are less likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

What are non-standard journal entries? [ISA | 796.13375]

Non-standard journal entries are journal entries used to record:

- non-recurring or unusual transactions - e.g., business combinations or disposals; and
- non-recurring adjustments - e.g., adjustments related to accounting estimates that are typically not made at each period-end such as the impairment of an asset.

The process and procedures used to record non-standard journal entries are typically manual journal entries.

What are manual journal entries? [ISA | 796.13376]

Manual journal entries are journal entries that are initiated by an individual and manually entered into the general ledger system. The use of manual journal entries can increase the risk of management override of controls because manual journal entries are more likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

What are other adjustments? [ISA | 796.13378]

Other adjustments are adjustments made to the general ledger accounts outside of the general ledger system to determine the amounts presented on the face of the financial statements. Entities often use a spreadsheet to support other adjustments. Other times, entities may make other adjustments directly in the financial statements or disclosures themselves. Other adjustments are most often seen in period-end financial reporting through post-closing adjustments.

Similar to manual journal entries, the use of other adjustments can increase the risk of management override of controls because there is more opportunity for manual intervention in the process and procedures.

Enhanced | How do we understand the process and procedures used to enter transaction totals into the general ledger? [ISA | 796.157307]

We understand the process and procedures used to enter transaction totals into the general ledger based on whether the entity uses separate transaction processing IT systems or not as described in the following sub-questions.

Enhanced | What if an entity does not use separate transaction processing IT systems? [ISA | 796.157308]

When an entity does not use separate transaction processing IT systems, we obtain an understanding of how transaction totals are transferred to and recorded in the general ledger when we obtain an understanding of the related business process based on the applicable International-Enhanced methodology as follows:

Applicable International-Enhanced methodology	Business processes	Obtain an understanding of the process by:
International-Enhanced PIE methodology	All business processes and sub-processes	Performing a walkthrough
International-Enhanced Non-PIE methodology	Business processes, or sub-processes, where we evaluate D&I of process control activities that address RMMs	Performing a walkthrough
	Business processes, or sub-processes, where we do not evaluate D&I of process	Either performing (i) a walkthrough or (ii) through inquiry and observation or

	control activities that address RMMs	inspection. Walkthroughs are encouraged.

See question "Which control activities do we obtain an understanding of and are relevant to the audit?" for guidance on when we evaluate D&I of process control activities that address RMMs.

For example, consider an ERP system that includes customer relationship management (CRM), order management, and accounting modules as part of their sales process. When we obtain an understanding of the sales process, we obtain an understanding of the process from initiation - i.e., creating the customer in the CRM module and orders in the order management module - to the recording of the transaction totals in the general ledger in the accounting module. This includes understanding the flow of data and information through the ERP system data, including the different modules and general ledger.

Enhanced | What if an entity uses separate transaction processing IT systems? [ISA | 796.157309]

An entity that uses separate transaction processing IT systems - e.g., a billing system that is not integrated as part of the entity's ERP system - will often have separate processes and procedures to accumulate transactions into batches and enter those batch totals into the general ledger on a periodic basis - e.g., on a monthly basis.

In these instances, we obtain an understanding of how the accumulation of transactions for the period is transferred to and recorded in the general ledger based on the applicable International-Enhanced methodology as follows:

Applicable International-Enhanced methodology	Type of sub-process	Obtain an understanding of the sub-process by:
International-Enhanced PIE methodology	Sub-process to enter transaction totals into the general ledger	Performing a walkthrough
International-Enhanced Non-PIE methodology	Sub-process to enter transaction totals into the general ledger where we evaluate D&I of process control activities that address RMMs	Performing a walkthrough
	Sub-process to enter transaction totals into the general ledger where we do not evaluate D&I of process	Either performing (i) a walkthrough or (ii) through inquiry and observation or inspection. Walkthroughs are encouraged.

	control activities that address RMMs	

See question "Which control activities do we obtain an understanding of and are relevant to the audit?" for guidance on when we evaluate D&I of process control activities that address RMMs.

When we understand the process and procedures used to transfer and enter transaction totals into general ledger(s), we follow the flow of data and information from one IT system to another. This can include the flow of data and information from:

- other IT systems used as part of business processes, such as transaction processing systems, into general ledger IT systems; and
- different general ledger systems into consolidation IT systems.

Core and Less Complex | How do we understand the process and procedures used to enter transaction totals into the general ledger? [ISA | 796.6416]

We understand the process and procedures used to enter transaction totals into the general ledger by performing either (i) a walkthrough or (ii) inquiry and observation or inspection.

Core and Less Complex | What if an entity does not use separate transaction processing IT systems? [ISA | 796.13445]

When an entity does not use separate transaction processing IT systems, we obtain an understanding of how transactions are transferred to and recorded in the general ledger when we perform either (i) a walkthrough or (ii) inquiry and observation or inspection of the related business process.

For example, consider an entity that uses an ERP system that includes customer relationship management (CRM), order management, and accounting modules as part of their sales process. When we perform either (i) a walkthrough or (ii) inquiry and observation or inspection of the sales process, we obtain an understanding of the process from initiation - i.e., creating the customer in the CRM module and orders in the order management module - to the recording of the transaction totals in the general ledger in the accounting module. This includes understanding the flow of data and information through the ERP system data, including the different modules and general ledger.

Core and Less Complex | What if an entity uses separate transaction processing IT systems? [ISA | 796.13446]

An entity that uses separate transaction processing IT systems - e.g., a billing system that is not integrated as part of the entity's ERP system - will often have separate processes and procedures to accumulate transactions into batches and entered those batch totals into the general ledger on a periodic basis - e.g., on a monthly basis.

In these instances, we obtain an understanding of how the accumulation of transactions for the period is transferred to and recorded in the general ledger when we perform either (i) a walkthrough or (ii) inquiry and observation or inspection of the process and procedures to enter transaction totals into the general ledger.

When we understand the process and procedures used to transfer and enter transaction totals into general ledger(s), we follow the flow of data and information from one IT system to another. This can include then flow of data and information from

- other IT systems used as part of business processes, such as transaction processing systems, into general ledger IT systems; and
- different general ledger IT systems into consolidation IT systems.

Can an entity have multiple general ledgers? [ISA | 796.157311]

Yes. Depending on the complexity of the entity's legal and financial reporting structure, an entity may have multiple different systems where general ledgers exist. General ledgers might exist within:

- general ledger IT systems used by the entity (or components of the entity in a group audit); and
- consolidation IT systems used to consolidate components of a group.

> For example, consider an entity that uses three general ledger IT systems for different components of the group and a consolidation system to consolidate the financial information of each of the three different components. In this instance, the entity has four different general ledgers (three different general ledger IT systems for different components of the group and one consolidation system).

In these instances, we understand how transactions are transferred to and recorded in each of the general ledgers used by the entity when we obtain an understanding of financial reporting and related business processes.

What if the entity uses multiple consolidation IT systems? [ISA | 796.157312]

When an entity uses multiple consolidation IT systems, we understand the process and procedures to enter transactions into the general ledgers that exist within each of the different consolidation IT systems.

> **Example - entity uses multiple consolidation IT systems**
>
> For example, consider an entity that has operations in multiple different countries that cover different lines of business. As part of the financial reporting process, the entity first consolidates their different telecommunication service operations in the United Kingdom (UK) by entering transactions from multiple general ledger IT systems into a consolidation IT system for the UK. The entity then consolidates their operations across all different countries by entering the consolidated financial information for the UK into a different consolidation IT system. In this instance, we understand the process and procedures to enter transaction totals into both consolidation systems.

What do we focus on when we obtain our understanding of the process and procedures used to enter transaction totals into the general ledger? [ISA | 796.1600]

When we obtain our understanding of the process and procedures used to enter transaction totals into the general ledger, we focus on:

- how data and information is extracted from the source IT system;
- the resources, including: 1) the extent of IT involvement (i.e., IT environment), relevant to transferring transactions into the general ledger, and 2) who participates from management;
- how data and information is input into the general ledger or consolidation IT system
- the locations involved in the period-end financial reporting process
- the types of adjusting and consolidating entries; and

- the nature and extent of the oversight of the process by management, the board of directors, and the audit committee.

An entity may use either manual processes - e.g., manually transferring data and information from one IT system by entering transaction totals from the report into the general ledger of another IT system - or automated processes - e.g., transferring data and information between IT systems using an automated configuration or interface.

1.1.2.2.2 Understand processes and procedures for journal entries and other adjustments [ISA | 797]

What do we do?

Understand processes and procedures to initiate, authorize, record, and process recurring and non-recurring journal entries and other adjustments

Why do we do this?

The processes and procedures to initiate, authorize, record, and process recurring and non-recurring journal entries and other adjustments is a sub-process of the financial reporting process, which exists for all entities. Understanding the financial reporting process and its sub-processes helps us to:

- identify and assess risks of material misstatement (RMMs), including the risk of management override of controls and the risk that journal entries could be susceptible to unauthorized or inappropriate intervention or manipulation; and
- determine the nature, timing, and extent of our testing of journal entries and other adjustments.

Execute the Audit

What are journal entries? [ISA | 797.1300]

Journal entries are any entries made directly within the general ledger system that are used to record transactions, allocations, adjustments and corrections. They include:

- standard journal entries used to record recurring transactions and adjustments; and
- non-standard journal entries used to record non-recurring, unusual transactions, or adjustments.

What are standard journal entries? [ISA | 797.13373]

Standard journal entries are journal entries used to record:

- recurring transactions - e.g., the day to day activities of the entity such as recurring sales, purchases, and cash disbursements; and
- recurring adjustments - e.g., adjustments related to accounting estimates that are made at each period-end such as changes in the estimate of uncollectible accounts receivable.

What are automated journal entries? [ISA | 797.13374]

Automated journal entries are standard journal entries that are automatically initiated, authorized, recorded and processed in the general ledger. The use of automated journal entries can reduce

the risk of management override of controls because automated journal entries are less likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

What are non-standard journal entries? [ISA | 797.13375]

Non-standard journal entries are journal entries used to record:

- non-recurring or unusual transactions - e.g., business combinations or disposals; and
- non-recurring adjustments - e.g., adjustments related to accounting estimates that are typically not made at each period-end such as the impairment of an asset.

The process and procedures used to record non-standard journal entries are typically manual journal entries.

What are manual journal entries? [ISA | 797.13376]

Manual journal entries are journal entries that are initiated by an individual and manually entered into the general ledger system. The use of manual journal entries can increase the risk of management override of controls because manual journal entries are more likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

What are other adjustments? [ISA | 797.13378]

Other adjustments are adjustments made to the general ledger accounts outside of the general ledger system to determine the amounts presented on the face of the financial statements. Entities often use a spreadsheet to support other adjustments. Other times, entities may make other adjustments directly in the financial statements or disclosures themselves. Other adjustments are most often seen in period-end financial reporting through post-closing adjustments.

Similar to manual journal entries, the use of other adjustments can increase the risk of management override of controls because there is more opportunity for manual intervention in the process and procedures.

Enhanced | How do we understand the process and procedures related to journal entries and other adjustments? [ISA | 797.1301]

We obtain an understanding of the process and procedures used to initiate, authorize, record, and process journal entries and to record recurring and non-recurring adjustments to the financial statements by performing a walkthrough (refer to activity 'Perform a walkthrough to understand the business processes').

Core and Less Complex | How do we understand the process and procedures related to journal entries and other adjustments? [ISA | 797.1301]

We obtain an understanding of the process and procedures used to initiate, authorize, record, and process journal entries and to record recurring and non-recurring adjustments to the financial statements by either performing (i) a walkthrough or (ii) through inquiry and observation or inspection. Walkthroughs may be the most effective way to obtain our understanding.

We document our understanding through the preparation of a narrative or flowchart.

What specifically do we understand about the process and procedures for journal entries and other adjustments? [ISA | 797.13536]

When we understand the process and procedures related to journal entries and other adjustments, we specifically understand each of the following items related to the recording of journal entries:

- the process and procedures by which journal entries and other adjustments are initiated, authorized and recorded;
- the resources, including: 1) the extent of IT involvement (i.e., IT environment), relevant to initiate, authorize and record journal entries and other adjustments, and 2) who from management is involved;
- relevant aspects of the information system relating to information disclosed in the financial statements that is obtained from within or outside of the general and subsidiary ledgers;
- the types of journal entries that are recorded within the IT system - e.g., automated journal entries, manual journal entries, or both;
- the specific accounts that are used to record standard and non-standard transactions and adjustments - e.g., accounts that are utilized for recurring transactions and adjustments versus accounts that are used for non-recurring or unusual transactions and adjustments; and
- whether the records supporting the journal entries are in manual or electronic form.

What may we understand for each IT system where journal entries are recorded? [ISA | 797.13545]

For each IT system used as part of the entity's process and procedures related to journal entries and other adjustments, we may understand:

- how the IT system is used as part of the financial reporting and related business processes - e.g., the system is used by the entity to consolidate components of the group. See activity "Understand the entity's IT systems" for more information; and
- the types of journal entries that are recorded within the IT system - e.g. automated journal entries, manual journal entries, or both.

How do we consider management override of controls and the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation when we understand the process and procedures related to journal entries and other adjustments? [ISA | 797.1400]

When we understand the process and procedures used by the entity to initiate, authorize, record, and process journal entries and other adjustments, we specifically consider the risk of management override of controls by identifying each of the process risk points (PRPs) - i.e., the where and the how a material misstatement could occur - where management may be able to override previous process control activities in the financial reporting and business processes. We obtain an understanding of the journal entries process and how management override could be perpetrated in order to identify process risk points and design our audit response.

Additionally, we consider whether there are any additional PRPs related to the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation. See question "What journal entries may be susceptible to unauthorized or inappropriate intervention or manipulation?" for more information.

Do we identify PRPs related to journal entries and other adjustments in all audits? [ISA | 797.158987]

Yes. We identify PRPs and evaluate the design and implementation of relevant process control activities that address them for the risk of management override of controls and, if identified, the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation due to error. If we identify automated process control activities over journal entries, we also identify

and evaluate the design and implementation of GITCs that support the effective operation of those automated process control activities that address relevant Risks arising from IT.

1.1.2.3 Prepare or use the entity's flowcharts to document our understanding of processes, when applicable [ISA | 1333]

What do we do?

Prepare or use the entity's flowcharts to document our understanding of the business process, when applicable.

Why do we do this?

A flowchart is an effective way to understand and document a process which includes:

- how transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger and reported in the financial statements and related disclosures;
- how information about events and conditions, other than transactions, is captured, processed and included in the financial statements and related disclosures;
- the accounting records, specific accounts and disclosures in the financial statements and other supporting records relating to the flows of information in the information system; and
- the entity's resources, including the IT environment, relevant to the business process.

Flowcharts can be easier to understand and review than narratives and are highly effective in identifying gaps in our understanding of the process.

Execute the Audit

What is a flowchart? [ISA | 1333.1300]

Flowcharts show how information flows through an entity's process - including inputs, outputs and IT systems.

We use flowcharts to help us evidence our understanding of each business process that contains an RMM, as flowcharts can be easier to understand and review than a narrative.

Depending on the complexity of the process, we may supplement the flowchart with narrative explanations for specific areas in the flowchart to clarify and supplement the flowchart.

How can flowcharts help us in the audit? [ISA | 1333.11383]

In addition to evidencing our understanding of the flow of information through an entity's process, flowcharts also help us to:

- identify parts of the entity's processes that we do not adequately understand (i.e. gaps in our understanding of the flow of information).
- identify relevant layers of technology and understand the flow of information through the layers of technology.

- identify the points in the process where a material misstatement could arise (process risk points) and the relevant process control activities that address them.

Enhanced | Does completing a flowchart mean that we don't perform either (i) walkthroughs or (ii) inquiries and observations or inspections? [ISA | 1333.11384]

No. Flowcharts evidence our understanding of the process, but we still perform either (i) a walkthrough or (ii) inquiries and observations or inspections to obtain or confirm that understanding. We may use a flowchart as part of our understanding procedures because that's the most efficient and effective way to capture our understanding of the flow of information, process risk points and relevant process control activities.

See question "How do we obtain an understanding of business processes?" for guidance on when to perform (i) a walkthrough or (ii) inquiry and observation or inspection based on the applicable International-Enhanced methodology.

Core and Less Complex | Does completing a flowchart mean that we don't perform either (i) walkthroughs or (ii) inquiries and observations or inspections? [ISA | 1333.6371]

No. Flowcharts evidence our understanding of the process, but we still perform either (i) a walkthrough or (ii) inquiries and observations or inspections to obtain or confirm that understanding. We may use a flowchart as part of our understanding procedures because that's the most efficient and effective way to capture our understanding of the flow of information, process risk points and relevant process control activities.

Enhanced | When do we prepare a flowchart? [ISA | 1333.6374]

Flowcharts are prepared for processes that may have an RMM (i.e. where there is a reasonable possibility that an RMM exists) based on the applicable International-Enhanced methodology as follows:

Applicable International-Enhanced methodology	Processes
International-Enhanced PIE methodology	All processes and sub-processes
International-Enhanced Non-PIE methodology	Processes, or sub-processes, where we evaluate D&I of process control activities that address RMMs

Additionally, when we apply the International-Enhanced Non-PIE methodology in processes or sub-processes where we do not evaluate D&I of process control activities that address RMMs, we have the option to evidence our understanding of processes through the preparation of a flowchart or narrative. Flowcharts are encouraged.

See question 'Which control activities do we obtain an understanding of and are relevant to the audit?' for guidance on when we evaluate D&I of process control activities that address RMMs.

Core and Less Complex | When do we prepare a flowchart? [ISA | 1333.6373]

We have the option to evidence our understanding of business and financial reporting processes through the preparation of a narrative or flowchart.

Flowcharting can be an effective way to evidence our comprehensive understanding of a process and is particularly effective in helping us identify PRPs and process control activities within a process. Accordingly, we may find using flowcharts most beneficial for processes where we will rely on controls or where evaluation of D&I is required by the standards (i.e. when a walkthrough is performed).

Regardless of whether a narrative or flowchart is used, our process understanding documentation is comprehensive and demonstrates an adequate understanding of the process, including information in the question 'What specifically do we understand when obtaining our understanding of a process?'.

Can we use flowcharts prepared by the entity in our audit? [ISA | 1333.6376]

We may use flowcharts prepared by the entity as a helpful starting point, but we keep in mind they:

- may not include the level of detail for our objective; or
- may include too much detail (e.g. operational/non-financial-reporting information that detracts from the financial reporting flow).

In addition, a common pitfall of using the entity's flowcharts is that we obtain and review them and make selected inquiries of the entity's process owner, rather than actually performing a walkthrough or inquiry and observation or inspection. This may inadvertently shortcut our process understanding and risk identification, because we're basing our risk assessments on the entity's documentation, supplemented by inquiries influenced by that documentation.

When we use the entity's flowcharts, we still obtain an understanding of the business processes and flow of information for transactions, events and conditions by performing a walkthrough or inquiry and observation or inspection. Once we include an entity's flowchart in our file, that becomes our audit evidence. So if it does not appropriately reflect the process flow, we either create our own or request the entity to update the flowchart so that it is accurate.

What do we include on the flowchart? [ISA | 1333.11385]

Overall, a flowchart will:

- depict how transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger and reported in the financial statements and related disclosures;
- depict how information about events and conditions, other than transactions, is captured, processed and included in the financial statements and related disclosures;
- depict the accounting records, specific accounts and disclosures in the financial statements and other supporting records relating to the flows of information in the information system; and
- depict the entity's resources, including the IT environment, relevant to the business process

When we identify PRPs and process control activities, we include those in the flowchart. Refer to our *Flowcharting* guides available on Alex for specific guidance on how to use flowcharts, including following a standardized format.

US	INTL

How to Flowchart a Process Practice Aid https://alex.kpmg.com/AROWeb/bridge/12305/17808?d=US,INTL,AU,CH,UK	How to Flowchart a Process Practice Aid https://alex.kpmg.com/AROWeb/document/top/Intl_KCW_TOP_Illust_Bus_Proc_FlwChrts_INTL

Is an IT systems diagram (ISD) part of a flowchart? [ISA | 1333.11386]

An ISD is not part of a flowchart but rather a separate diagram that depicts the different IT systems, including the layers of technology within those systems, that an entity uses as part of its financial reporting and related business processes.

An ISD does not document our understanding of how information flows into, through and out of relevant IT systems as part of an entity's processes. Instead, this flow of information is captured in the flowchart.

How do we know we have created an effective flowchart? [ISA | 1333.11387]

When we review flowcharts or narratives, we think critically about whether we have adequately understood and documented information/responses to the following questions:

- Who is involved in the process (e.g. individuals, departments etc.)?
- Where does the process begin (i.e. the initiation of a transaction) and where does it end (i.e. with recording that transaction in the general ledger as well as how the transactions are reported in the financial statements and related disclosures)?
- What are the key activities in the process (both manual and automated)? How often are they performed and in what order do they occur?
- What IT systems are relevant to the process?
- Have we identified portions of the business process that we have not adequately understood - i.e. are there gaps in our understanding of the flow of transactions?
- Have we understood the flow of information for transactions, events and conditions through the IT systems, service organizations and locations or business units?
- What reports are generated as an output of the process and used in the performance of a control?

In those processes where we evaluate the design and implementation of process control activities, we also think about whether we have adequately understood and documented information/responses to the question:

- How and where in the process could a material misstatement arise (process risk points) and what process control activities have management implemented to address those process risk points?

Do we update our understanding of the business process and flowcharts throughout the audit? [ISA | 1333.11388]

Yes, when there are changes in our audit approach or we become aware of when there is a change in the business process, we update our flowcharts.

1.1.3 Evaluate the entity's information system [ISA | 7883]

What do we do?

Based on our understanding of the entity's information systems relevant to financial reporting, evaluate whether the entity's information system appropriately supports the preparation of the entity's financial statements in accordance with the applicable financial reporting framework considering the nature and complexity of the entity.

Why do we do this?

Information systems support informed decision making and the functioning of the internal control by processing relevant, timely, and quality information from internal and external sources. We evaluate the Information component of internal control over financial reporting (ICFR) as information is pervasive to the entity's overall ICFR and our evaluation impacts our identification and assessment of risks of material misstatement (RMMs), particularly financial statement level risks.

Execute the audit

How do we evaluate whether the entity's information system appropriately supports the preparation of the entity's financial statements? [ISA | 7883.8852]

We obtain an understanding of the entity's information system through performing various activities described in the question 'How do we obtain an understanding of the entity's information systems relevant to financial reporting?' This includes understanding the entity's business processes, including the financial reporting process, processes relevant to journal entries etc.

Based on the knowledge we gathered by performing these activities we evaluate whether the entity's information system appropriately supports the preparation of the entity's financial statements.

What if we conclude that the entity's information system does not appropriately support the preparation of the entity's financial statements? [ISA | 7883.8538]

When we conclude that the entity's information system does not appropriately support the preparation of the entity's financial statements, we consider the impact on the audit and whether to consult with DPP.

1.2 Understand and evaluate the entity's communications [ISA | 7848]

What do we do?

Obtain an understanding of how the entity communicates roles and responsibilities and significant matters relating to financial reporting and evaluate whether the entity's communication appropriately support the preparation of the entity's financial statements in accordance with the applicable financial reporting framework.

Why do we do this?

Communication is pervasive to the entity's overall ICFR, and communication of information internally and externally is necessary to support the functioning of ICFR. We obtain an understanding and evaluate how the entity communicates roles and responsibilities and significant matters relating to financial reporting,

which is part of the Information and Communication component of ICFR, to support our identification and assessment of risks of material misstatement (RMMs).

Execute the audit

Not Integrated Audit | How do we obtain an understanding of the entity's communications? [ISA | 7848.8533]

We obtain an understanding of the entity's communication relevant to the preparation of the financial statements by:

- understanding, through inquiry, the entity's communications related to the following elements/ principles:
  - how the entity communicates objectives and responsibilities for internal control internally (i.e. between people within the entity and between management and those charged with governance);
  - how the entity communicates matters affecting internal control externally (i.e. with external parties, such as those with regulatory authorities;and
- performing procedures to obtain an understanding of the CERAMIC components:
  - begin by performing inquiries
  - consider whether certain factors apply to determine whether to perform more than inquiry
  - If at least one of the factors apply, design additional procedures to obtain an understanding (i.e. observation and/or inspection)

Based on our understanding obtained, evaluating the entity's communications.

If we identify a control deficiency in a CERAMIC component(s), we evaluate the severity of the control deficiency and assess the impact on our evaluation.

What do we do if there are unaddressed elements after we obtain an understanding of CERAMIC? [ISA | 7848.8653]

When those charged with governance are not separate from management, it is appropriate for the following elements to be unaddressed:

- Element 2 - Those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Element 11 - The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

In all other circumstances, if there are unaddressed elements after we have obtained an understanding of the CERAMIC component, we identify a control deficiency in the related CERAMIC component.

How may the process for communications within a smaller, less complex entity be different? [ISA | 7848.8535]

In less complex entities, communication may be less structured (e.g., formal manuals may not be used) due to fewer levels of responsibility and management's greater visibility and availability.

Regardless of the size of the entity, open communication channels facilitate the reporting of exceptions and acting on them.

Examples

1.2.1 Understand how the entity communicates objectives and responsibilities for internal control internally [ISA | 1334]

What do we do?

Obtain an understanding of how the entity internally communicates information, including objectives and responsibilities for internal control over financial reporting (ICFR), necessary to support the functioning of ICFR.

Why do we do this?

Communication is pervasive to the entity's overall ICFR. We obtain an understanding of how the entity internally communicates information necessary to support the functioning of ICFR as the lack of communication of information internally may result in the risk that people within the entity do not understand their individual roles and responsibilities for ICFR and how their roles and responsibilities impact the achievement of the entity's objectives. In addition, the lack of communication between management and those charged may result in those charged with governance not receiving information needed to exercise its oversight responsibility for internal control.

Execute the Audit

What are Elements 10 and 11 of the Communication portion of the Information and Communication component? [ISA | 1334.11923]

Element 10:

T*he entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control* ***between people within the entity*** *, including how financial reporting roles and responsibilities are communicated.*

Element 11:

The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control ***between*** *management and those charged with governance.*

Element 10 is applicable to all entities; however, the applicability of Element 11 is based on the specific ownership and governance structure of the entity. The table below provides further information.

Communication	Applicability	Examples
Element 10: Within the entity	All entities.	N/A.
Element 11: Between management and those charged with governance	Entities where those charged with governance are separate from management.	This element is applicable regardless of whether the individual(s) charged with governance are independent or members of management. This element is not applicable when the role of governance is undertaken directly by the owner-manager (where there are no others charged with governance).

What are the points of focus related to Elements 10 and 11? [ISA | 1334.8539]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us understand of how the entity addresses the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus for Elements 10 and 11, along with questions that may help us obtain an understanding.

Points of focus	Questions
• Communicates internal control information • Communicates with those charged with governance • Provides separate communication lines • Selects relevant methods of communication	• Does the entity have a process is in place to communicate necessary information to enable all personnel to understand and carry out their responsibilities with respect to the entity's external financial reporting objectives and internal control? • Does communication exist between management and those charged with governance so that both have information needed to fulfil their roles with respect to the entity's external financial reporting objectives and internal control? • Are there separate communication channels, such as whistle-blower hotlines, in place to serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective? • Does the entity structure and tailor communication (inbound, outbound and cross-functionally) based on the need and the audience?

How may information related to financial reporting roles and responsibilities and significant matters related to financial reporting be communicated internally within an entity? [ISA | 1334.1500]

Area	Reason	Form
Individual roles and responsibility	Provides an appropriate understanding of how individuals' roles and responsibilities pertains to the system of internal control relevant to financial reporting, including how their activities relates to the work of others. It also allows for a means of reporting significant matters and/ or exceptions to an appropriate levels within the entity.	This communication may take such forms as: • policy manuals • accounting and financial reporting manuals • internal memoranda • accounting and finance meetings or conferences to discuss internal control matters and accounting policy changes • regular or ad hoc entity-wide emails, newsletters, conference calls, webcasts or meetings about updates on internal control matters • departmental meetings or conferences to discuss the business and its operations to exchange information about activities and decisions that may impact other departments • orally and/or through the actions of management - e.g., management site visits to plants, sales office, major customers, and other locations.
Significant matters related to financial reporting		

What information is communicated to those charged with governance and/or external parties? [ISA | 1334.11924]

It varies. Not all information communicated internally within the entity needs to be communicated by management to those charged with governance.

When understanding these elements of the Communication component of ICFR:

- we obtain an understanding of how management determines what information regarding financial reporting roles and responsibilities and what significant matters related to financial reporting are of importance and requires communication to those charged with governance.
- we consider whether this is appropriate based on the nature and complexity of the entity.

Examples

1.2.2 Understand how the entity communicates matters affecting internal control externally [ISA | 1335]

What do we do?

Obtain an understanding of how the entity communicates with external parties about matters affecting the functioning of internal control over financial reporting (ICFR).

Why do we do this?

We obtain an understanding of how the entity communicates with external parties about matters affecting the functioning of ICFR as the lack of communication with external parties may result in risks of material misstatement.

Execute the Audit

What is Element 12 of the Communication portion of the Information and Communication component? [ISA | 1335.8542]

Element 12:

The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control with external parties such as regulatory bodies.

The table below provides further information.

Communication	Applicability	Examples
With an external party(ies)	When required by local laws and regulations.	This communication is applicable when the entity is required to communicate (i) financial reporting roles and responsibilities, and/or (ii) significant matters related to financial reporting to an external party. • Local regulatory body or authority • Compliance with industry standards and rules - e.g., reporting of violations • Contractual agreements - e.g., debt provisions / covenants with financial institutions

What are the points of focus related to Element 13? [ISA | 1335.8543]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us understand how the entity addresses the objectives of the related element of a CERAMIC component.

The table below sets out the points of focus for Element 13, along with example questions that may help us obtain an understanding.

Points of focus	Questions
• Communicates to external parties • Selects relevant methods of communication	• Does the entity structure communication to external parties based on the need and the audience?

What information is communicated to external parties? [ISA | 1335.8544]

Only information that is to be communicated under local laws and regulations is communicated by the entity to external parties.

When understanding how the entity addresses this element of the Communication component of ICFR:

- we obtain an understanding of how management determines what information regarding financial reporting roles and responsibilities and what significant matters related to financial reporting are of importance and requires communication to external parties.
- we consider whether this is appropriate based on the circumstances of the entity, including its nature and complexity.

Examples

1.2.3 Not Integrated Audit | Perform procedures to obtain an understanding of the CERAMIC components [ISA | 7843]

What do we do?

Perform procedures to obtain an understanding of the CERAMIC components

Why do we do this?

We perform procedures to obtain an understanding of the CERAMIC components as part of our risk assessment to support our identification and assessment of risks of material misstatement (RMMs).

Execute the audit

What type of procedures do we perform to obtain an understanding of the CERAMIC components? [ISA | 7843.8495]

We begin by performing inquiries to obtain an understanding of the CERAMIC components. However, inquiry alone may not be sufficient to obtain the necessary understanding of the components when certain factors exist. We consider whether certain factors apply to determine whether to perform more than inquiry.

What factors do we consider when determining whether to perform more than inquiry in order to obtain an understanding of CERAMIC? [ISA | 7843.8496]

We consider the factors in the table below. When certain circumstances exist, there is a rebuttable presumption that we will perform more than inquiry in order to obtain an understanding over one or more of the CERAMIC components.

Factor	Impact on nature, timing, and extent of procedures
Size and complexity of the entity	The larger and more complex an entity, the more robust and comprehensive its set of controls, processes, structures, and communications necessary to address the elements/principles within each CERAMIC component. As such, for a large and/or complex entity, it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Conversely, less complex entities require simpler set of controls, processes, structures, and communications to achieve their objectives. For example, the entity may develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication rather than have a written code of code. Due the simplicity of their processes, inquiry alone may be sufficient to obtain an understanding of the entity's CERAMIC. The size of an entity (e.g. number of employees) may be an indicator of its complexity. However, some smaller entities may be complex, and some larger entities may be less complex. Refer to 'What characteristics of the entity do we think about to assess its complexity?' for additional information.
Our existing knowledge of the entity's system of internal control	When we have less knowledge of the entity's system of internal control (e.g. we are performing an initial audit), it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC.
Reliance on the entity's control activities	It is presumed that inquiry alone is not sufficient to obtain an understanding of CERAMIC when we plan to place reliance on the entity's control activities to reduce our control risk.

Nature and extent of changes in entity's systems and operations	Where there have been extensive changes in the entity's systems (e.g. new IT system implementation) and/or operations (e.g. product line or geographic expansion, significant changes in management or personnel) from the prior year, the entity's system of internal control may have significantly changed such that it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Inquiry alone may also not be sufficient when changes to the entity's CERAMIC have occurred to remediate prior year deficiencies.

What if we conclude that it is appropriate to rebut the presumption that 'inquiry alone is not sufficient'? [ISA | 7843.8497]

When we conclude that rebutting the presumption that 'inquiry alone is not sufficient' is appropriate in the circumstances of the engagement, and accordingly have only obtained an understanding of CERAMIC through inquiry, we document the reasons for that conclusion.

What characteristics influence the complexity of an entity? [ISA | 7843.8498]

The characteristics below influence the complexity of an entity. No one characteristic is more indicative than another of an entity's complexity. The presence of one characteristic that indicates 'more complexity' does not necessarily indicate a 'more complex' entity. We collectively think about all the characteristics when considering the factor 'size and complexity of the entity.'

Factor	Impact on nature, timing, and extent of procedures
Size and complexity of the entity	More robust and comprehensive sets of controls, processes, structures, and communications are necessary at larger and more complex entities to address the elements/principles within each CERAMIC component. As such, for a large and/or complex entity, it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Conversely, less complex entities require a simpler set of controls, processes, structures, and communications to achieve their objectives. For example, the entity may develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication rather than have a written code of code. Due the simplicity of their processes, inquiry alone may be sufficient to obtain an understanding of the entity's CERAMIC. The size of an entity (e.g. number of employees) may be an indicator of its complexity. However, some smaller entities may be complex, and some larger entities may be less complex.

	Refer to 'What characteristics influence the complexity of an entity ?' for additional information.
Our existing knowledge of the entity's system of internal control	When we have less knowledge of the entity's system of internal control (e.g. we are performing an initial audit), it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC.
Reliance on the entity's control activities	It is presumed that inquiry alone is not sufficient to obtain an understanding of CERAMIC when we plan to place reliance on the entity's control activities to reduce our control risk.
Nature and extent of changes in entity's systems and operations	Where there have been extensive changes in the entity's systems (e.g. new IT system implementation) and/or operations (e.g. product line or geographic expansion, significant changes in management or personnel) from the prior year, the entity's system of internal control may have significantly changed such that it is presumed that inquiry alone is not sufficient to obtain an understanding of the entity's CERAMIC. Inquiry alone may also not be sufficient when changes to the entity's CERAMIC have occurred to remediate prior year deficiencies.

Characteristics	Examples of less complexity	Examples of more complexity
Organizational structure and management personnel	An entity has few business segments or lines of business with a small management team and no internal audit.	An entity has several business segments or lines of business with multiple levels of management and a sophisticated internal audit department.
Ownership and governance structure	An owner-manager is responsible for the governance and direct oversight of the operations and accounting / financial reporting for the entity.	The entity is publicly traded, and those charged with governance operate independently of management.

Operating characteristics	The entity is a single legal entity with operations in only a few geographic locations.	The entity is a group that has many components that operate in several markets and geographic locations and are decentralized.
Nature of assets, liabilities and transactions	The entity processes routine transactions and the accounts do not require complex accounting or significant judgments.	The entity processes non-routine or unusual transactions, including in controversial or emerging areas, and the accounts require complex accounting or significant judgments.
Nature of the accounting processes and controls	The entity has simple record-keeping with few accounting processes with primarily manual control activities performed by a few people.	The entity has many IT systems (or many instances of a single system) and customizes the systems for the entity's specific needs.
IT systems	The entity has few IT systems and the entity uses pre-packaged purchased applications that are not able to be customized by the entity.	The entity has many IT systems (or many instances of a single system) and customizes the systems for the entity's specific needs.

1.2.4 Evaluate the entity's communication [ISA | 7847]

What do we do?

Based on our understanding of the entity's communication, evaluate whether the entity's communications appropriately supports the preparation of the entity's financial statements in accordance with the applicable financial reporting framework considering the nature and complexity of the entity.

Why do we do this?

Communication is pervasive to the entity's overall ICFR, and communication of information internally and externally is necessary to support the functioning of ICFR. We evaluate the Communication component of internal control over financial reporting (ICFR) as communication is pervasive to the entity's overall ICFR and our evaluation impacts our identification and assessment of risks of material misstatement (RMMs), particularly financial statement level risks.

Execute the audit

Not Integrated Audit | How do we evaluate whether the entity's circumstances considering the nature and complexity of the entity? [ISA | 7847.8546]

Based on our understanding of the entity's communication, we identify a CERAMIC control deficiency (refer to 'Evaluate the severity and assess the impact of CERAMIC control deficiencies' for additional information) if:

- there are unaddressed principles/elements or
- the entity's set of controls, processes and structures do not appropriately address the principle/element considering the nature and complexity of the entity

When there is at least one principle/element that is unaddressed or not appropriately addressed, we conclude that the entity's communication is not appropriate to the entity's circumstances considering the nature and complexity of the entity.

How may the process for communications within a smaller, less complex entity be different? [ISA | 7847.8535]

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

What if we conclude that the entity's communication does not appropriately support the preparation of the entity's financial statements? [ISA | 7847.8549]

When we conclude that the entity's communication does not appropriately support the preparation of the entity's financial statements considering the nature and complexity of the entity, we identify a financial statement level risk (see activity 'Evaluate RMs at the financial statement level' for additional information) and respond to the risk in line with activity 'Design and implement overall responses'.

Control Activities

International Standards on Auditing: ISA 315.26

Control activities

26. The auditor shall obtain an understanding of the control activities component, through performing risk assessment procedures, by: (Ref: Para. A147-A157)	
(a) Identifying controls that address risks of material misstatement at the assertion level in the control activities component as follows: (i) Controls that address a risk that is determined to be a significant risk; (Ref: Para. A158.A159)	and (d) For each control identified in (a) or (c)(ii): (Ref: Para. A175.A181) (i) Evaluating whether the control is designed effectively to address the risk of material misstatement at the assertion

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

(iii) Controls for which the auditor plans to test operating effectiveness in determining the nature, timing and extent of substantive testing, which shall include controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence; and (Ref: Para. A162.A164)

(iv) Other controls that the auditor considers are appropriate to enable the auditor to meet the objectives of paragraph 13 with respect to risks at the assertion level, based on the auditor's professional judgment; (Ref: Para. A165)

(b) Based on controls identified in (a), identifying the IT applications and the other aspects of the entity's IT environment that are subject to risks arising from the use of IT; (Ref: Para. A166.A172)

(c) For such IT applications and other aspects of the IT environment identified in (b), identifying: (Ref: Para. A173.A174)

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

(ii) The entity's general IT controls that address such risks;

level, or effectively designed to support the operation of other controls; and

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

ISA Application and Other Explanatory Material: ISA 315.A123-A130 | ISA 315.A147-A181

Information System and Communication, and Control Activities (Ref: Para. 25.26)

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

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

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

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

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

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

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

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

A129. The auditor's assessment of inherent risk may also influence the identification of controls in the control activities component. For example, the auditor's identification of controls relating to significant

risks may only be identifiable when the auditor has assessed inherent risk at the assertion level in accordance with paragraph 31. Furthermore, controls addressing risks for which the auditor has determined that substantive procedures alone do not provide sufficient appropriate audit evidence (in accordance with paragraph 33) may also only be identifiable once the auditor's inherent risk assessments have been undertaken.

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

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

Control Activities (Ref: Para. 26)

Controls in the control activities component

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

A147. The control activities component includes controls that are designed to ensure the proper application of policies (which are also controls) in all the other components of the entity's system of internal control, and includes both direct and indirect controls.

Example:

The controls that an entity has established to ensure that its personnel are properly counting and recording the annual physical inventory relate directly to the risks of material misstatement relevant to the existence and completeness assertions for the inventory account balance.

A148. The auditor's identification and evaluation of controls in the control activities component is focused on information processing controls, which are controls applied during the processing of information in the entity's information system that directly address risks to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information). However, the auditor is not required to identify and evaluate all information processing controls related to the entity's policies that define the flows of transactions and other aspects of the entity's information processing activities for the significant classes of transactions, account balances and disclosures.

A149. There may also be direct controls that exist in the control environment, the entity's risk assessment process or the entity's process to monitor the system of internal control, which may be identified in accordance with paragraph 26. However, the more indirect the relationship between controls that support other controls and the control that is being considered, the less effective that control may be in preventing, or detecting and correcting, related misstatements.

Example:

A sales manager's review of a summary of sales activity for specific stores by region ordinarily is only indirectly related to the risks of material misstatement relevant to the completeness assertion

for sales revenue. Accordingly, it may be less effective in addressing those risks than controls more directly related thereto, such as matching shipping documents with billing documents.

A150. Paragraph 26 also requires the auditor to identify and evaluate general IT controls for IT applications and other aspects of the IT environment that the auditor has determined to be subject to risks arising from the use of IT, because general IT controls support the continued effective functioning of information processing controls. A general IT control alone is typically not sufficient to address a risk of material misstatement at the assertion level.

A151. The controls that the auditor is required to identify and evaluate the design, and determine the implementation of, in accordance with paragraph 26 are those:

- Controls which the auditor plans to test the operating effectiveness of in determining the nature, timing and extent of substantive procedures. The evaluation of such controls provides the basis for the auditor's design of test of control procedures in accordance with ISA 330. These controls also include controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.
- Controls include controls that address significant risks and controls over journal entries. The auditor's identification and evaluation of such controls may also influence the auditor's understanding of the risks of material misstatement, including the identification of additional risks of material misstatement (see paragraph A95). This understanding also provides the basis for the auditor's design of the nature, timing and extent of substantive audit procedures that are responsive to the related assessed risks of material misstatement.
- Other controls that the auditor considers are appropriate to enable the auditor to meet the objectives of paragraph 13 with respect to risks at the assertion level, based on the auditor's professional judgment.

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

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

A153. Examples of controls in the control activities component include authorizations and approvals, reconciliations, verifications (such as edit and validation checks or automated calculations), segregation of duties, and physical or logical controls, including those addressing safeguarding of assets.

A154. Controls in the control activities component may also include controls established by management that address risks of material misstatement related to disclosures not being prepared in accordance with the applicable financial reporting framework. Such controls may relate to information included in the financial statements that is obtained from outside of the general and subsidiary ledgers.

A155. Regardless of whether controls are within the IT environment or manual systems, controls may have various objectives and may be applied at various organizational and functional levels.

Scalability (Ref: Para. 26)

A156. Controls in the control activities component for less complex entities are likely to be similar to those in larger entities, but the formality with which they operate may vary. Further, in less complex entities, more controls may be directly applied by management.

Example:

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

A157. It may be less practicable to establish segregation of duties in less complex entities that have fewer employees. However, in an owner-managed entity, the owner-manager may be able to exercise more effective oversight through direct involvement than in a larger entity, which may compensate for the generally more limited opportunities for segregation of duties. Although, as also explained in ISA 240, domination of management by a single individual can be a potential control deficiency since there is an opportunity for management override of controls.[39]

39 ISA 240, paragraph A28

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

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

A158. Regardless of whether the auditor plans to test the operating effectiveness of controls that address significant risks, the understanding obtained about management's approach to addressing those risks may provide a basis for the design and performance of substantive procedures responsive to significant risks as required by ISA 330.[40] Although risks relating to significant non-routine or judgmental matters are often less likely to be subject to routine controls, management may have other responses intended to deal with such risks. Accordingly, the auditor's understanding of whether the entity has designed and implemented controls for significant risks arising from non-routine or judgmental matters may include whether and how management responds to the risks. Such responses may include:

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

Example:

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

40 ISA 330, paragraph 21

A159. ISA 240[41] requires the auditor to understand controls related to assessed risks of material misstatement due to fraud (which are treated as significant risks), and further explains that it is important

for the auditor to obtain an understanding of the controls that management has designed, implemented and maintained to prevent and detect fraud.

---

41 ISA 240, paragraphs 28 and A33

Controls over journal entries (Ref: Para. 26(a)(ii))

A160. Controls that address risks of material misstatement at the assertion level that are expected to be identified for all audits are controls over journal entries, because the manner in which an entity incorporates information from transaction processing into the general ledger ordinarily involves the use of journal entries, whether standard or non-standard, or automated or manual. The extent to which other controls are identified may vary based on the nature of the entity and the auditor's planned approach to further audit procedures.

Example:

In an audit of a less complex entity, the entity's information system may not be complex and the auditor may not plan to rely on the operating effectiveness of controls. Further, the auditor may not have identified any significant risks or any other risks of material misstatement for which it is necessary for the auditor to evaluate the design of controls and determine that they have been implemented. In such an audit, the auditor may determine that there are no identified controls other than the entity's controls over journal entries.

Automated tools and techniques

A161. In manual general ledger systems, non-standard journal entries may be identified through inspection of ledgers, journals, and supporting documentation. When automated procedures are used to maintain the general ledger and prepare financial statements, such entries may exist only in electronic form and may therefore be more easily identified through the use of automated techniques.

Example:

In the audit of a less complex entity, the auditor may be able to extract a total listing of all journal entries into a simple spreadsheet. It may then be possible for the auditor to sort the journal entries by applying a variety of filters such as currency amount, name of the preparer or reviewer, journal entries that gross up the balance sheet and income statement only, or to view the listing by the date the journal entry was posted to the general ledger, to assist the auditor in designing responses to the risks identified relating to journal entries.

Controls for which the auditor plans to test the operating effectiveness (Ref: Para. 26(a)(iii))

A162. The auditor determines whether there are any risks of material misstatement at the assertion level for which it is not possible to obtain sufficient appropriate audit evidence through substantive procedures alone. The auditor is required, in accordance with ISA 330,[42] to design and perform tests of controls that address such risks of material misstatement when substantive procedures alone do not provide sufficient

appropriate audit evidence at the assertion level. As a result, when such controls exist that address these risks, they are required to be identified and evaluated.

---

42 ISA 330, paragraph 8(b)

A163. In other cases, when the auditor plans to take into account the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures in accordance with ISA 330, such controls are also required to be identified because ISA 33043 requires the auditor to design and perform tests of those controls.

Examples:

The auditor may plan to test the operating effectiveness of controls:

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

---

43 ISA 330, paragraph 8(a)

A164. The auditor's plans to test the operating effectiveness of controls may also be influenced by the identified risks of material misstatement at the financial statement level. For example, if deficiencies are identified related to the control environment, this may affect the auditor's overall expectations about the operating effectiveness of direct controls.

Other controls that the auditor considers appropriate (Ref: Para. 26(a)(iv))

A165. Other controls that the auditor may consider are appropriate to identify, and evaluate the design and determine the implementation, may include:

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

---

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

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

Appendix 5 includes example characteristics of IT applications and other aspects of the IT environment, and guidance related to those characteristics, that may be relevant in identifying IT applications and other aspects of the IT environment subject to risks arising from the use of IT.

Identifying IT applications and other aspects of the IT environment (Ref: Para. 26(b))

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

A166. Understanding the risks arising from the use of IT and the general IT controls implemented by the entity to address those risks may affect:

- The auditor's decision about whether to test the operating effectiveness of controls to address risks of material misstatement at the assertion level;

Example:

When general IT controls are not designed effectively or appropriately implemented to address risks arising from the use of IT (e.g., controls do not appropriately prevent or detect unauthorized program changes or unauthorized access to IT applications), this may affect the auditor's decision to rely on automated controls within the affected IT applications.

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

Example:

The ongoing operating effectiveness of an information processing control may depend on certain general IT controls that prevent or detect unauthorized program changes to the IT information processing control (i.e., program change controls over the related IT application). In such circumstances, the expected operating effectiveness (or lack thereof) of the general IT control may affect the auditor's assessment of control risk (e.g., control risk may be higher when such general IT controls are expected to be ineffective or if the auditor does not plan to test the general IT controls).

- The auditor's strategy for testing information produced by the entity that is produced by or involves information from the entity's IT applications;

Example:

When information produced by the entity to be used as audit evidence is produced by IT applications, the auditor may determine to test controls over system-generated reports, including identification and testing of the general IT controls that address risks of inappropriate or unauthorized program changes or direct data changes to the reports.

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

Example:

When there are significant or extensive programming changes to an IT application to address new or revised reporting requirements of the applicable financial reporting framework, this may be an indicator of the complexity of the new requirements and their effect on the entity's financial statements. When such extensive programming or data changes occur, the IT application is also likely to be subject to risks arising from the use of IT.

- The design of further audit procedures.

Example:

If information processing controls depend on general IT controls, the auditor may determine to test the operating effectiveness of the general IT controls, which will then require the design of tests of controls for such general IT controls. If, in the same circumstances, the auditor determines not to test the operating effectiveness of the general IT controls, or the general IT controls are expected to be ineffective, the related risks arising from the use of IT may need to be addressed through the design of substantive procedures. However, the risks arising from the use of IT may not be able to be addressed when such risks relate to risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. In such circumstances, the auditor may need to consider the implications for the audit opinion.

Identifying IT applications that are subject to risks arising from the use of IT

A167. For the IT applications relevant to the information system, understanding the nature and complexity of the specific IT processes and general IT controls that the entity has in place may assist the auditor in determining which IT applications the entity is relying upon to accurately process and maintain the integrity of information in the entity's information system. Such IT applications may be subject to risks arising from the use of IT.

A168. Identifying the IT applications that are subject to risks arising from the use of IT involves taking into account controls identified by the auditor because such controls may involve the use of IT or rely on IT. The auditor may focus on whether an IT application includes automated controls that management is relying on and that the auditor has identified, including controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. The auditor may also consider how information is stored and processed in the information system relating to significant classes of transactions, account balances and disclosures and whether management is relying on general IT controls to maintain the integrity of that information.

A169. The controls identified by the auditor may depend on system-generated reports, in which case the IT applications that produce those reports may be subject to risks arising from the use of IT. In other cases, the auditor may not plan to rely on controls over the system-generated reports and plan to directly test the inputs and outputs of such reports, in which case the auditor may not identify the related IT applications as being subject to risks arising from IT.

Scalability

A170. The extent of the auditor's understanding of the IT processes, including the extent to which the entity has general IT controls in place, will vary with the nature and the circumstances of the entity and its IT environment, as well as based on the nature and extent of controls identified by the auditor. The

number of IT applications that are subject to risks arising from the use of IT also will vary based on these factors.

Examples:

- An entity that uses commercial software and does not have access to the source code to make any program changes is unlikely to have a process for program changes, but may have a process or procedures to configure the software (e.g., the chart of accounts, reporting parameters or thresholds). In addition, the entity may have a process or procedures to manage access to the application (e.g., a designated individual with administrative access to the commercial software). In such circumstances, the entity is unlikely to have or need formalized general IT controls.
- In contrast, a larger entity may rely on IT to a great extent and the IT environment may involve multiple IT applications and the IT processes to manage the IT environment may be complex (e.g., a dedicated IT department exists that develops and implements program changes and manages access rights), including that the entity has implemented formalized general IT controls over its IT processes.
- When management is not relying on automated controls or general IT controls to process transactions or maintain the data, and the auditor has not identified any automated controls or other information processing controls (or any that depend on general IT controls), the auditor may plan to directly test any information produced by the entity involving IT and may not identify any IT applications that are subject to risks arising from the use of IT.
- When management relies on an IT application to process or maintain data and the volume of data is significant, and management relies upon the IT application to perform automated controls that the auditor has also identified, the IT application is likely to be subject to risks arising from the use of IT.

A171. When an entity has greater complexity in its IT environment, identifying the IT applications and other aspects of the IT environment, determining the related risks arising from the use of IT, and identifying general IT controls is likely to require the involvement of team members with specialized skills in IT. Such involvement is likely to be essential, and may need to be extensive, for complex IT environments.

Identifying other aspects of the IT environment that are subject to risks arising from the use of IT

A172. The other aspects of the IT environment that may be subject to risks arising from the use of IT include the network, operating system and databases, and, in certain circumstances, interfaces between IT applications. Other aspects of the IT environment are generally not identified when the auditor does not identify IT applications that are subject to risks arising from the use of IT. When the auditor has identified IT applications that are subject to risks arising from IT, other aspects of the IT environment (e.g., database, operating system, network) are likely to be identified because such aspects support and interact with the identified IT applications.

Identifying risks arising from the use of IT and general IT controls (Ref: Para. 26(c))

Appendix 6 sets out considerations for understanding general IT controls.

A173. In identifying the risks arising from the use of IT, the auditor may consider the nature of the identified IT application or other aspect of the IT environment and the reasons for it being subject to risks arising from the use of IT. For some identified IT applications or other aspects of the IT environment, the auditor may identify applicable risks arising from the use of IT that relate primarily to unauthorized access or unauthorized program changes, as well as that address risks related to inappropriate data changes (e.g., the risk of inappropriate changes to the data through direct database access or the ability to directly manipulate information).

A174. The extent and nature of the applicable risks arising from the use of IT vary depending on the nature and characteristics of the identified IT applications and other aspects of the IT environment. Applicable IT risks may result when the entity uses external or internal service providers for identified aspects of its IT environment (e.g., outsourcing the hosting of its IT environment to a third party or using a shared service center for central management of IT processes in a group). Applicable risks arising from the use of IT may also be identified related to cybersecurity. It is more likely that there will be more risks arising from the use of IT when the volume or complexity of automated application controls is higher and management is placing greater reliance on those controls for effective processing of transactions or the effective maintenance of the integrity of underlying information.

Evaluating the design, and determining implementation, of identified controls in the control activities component (Ref: Para 26(d))

A175. Evaluating the design of an identified control involves the auditor's consideration of whether the control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting, material misstatements (i.e., the control objective).

A176. The auditor determines the implementation of an identified control by establishing that the control exists and that the entity is using it. There is little point in the auditor assessing the implementation of a control that is not designed effectively. Therefore, the auditor evaluates the design of a control first. An improperly designed control may represent a control deficiency.

A177. Risk assessment procedures to obtain audit evidence about the design and implementation of identified controls in the control activities component may include:

- Inquiring of entity personnel.
- Observing the application of specific controls.
- Inspecting documents and reports.

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

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

A179. The auditor may conclude that a control, which is effectively designed and implemented, may be appropriate to test in order to take its operating effectiveness into account in designing substantive procedures. However, when a control is not designed or implemented effectively, there is no benefit in testing it. When the auditor plans to test a control, the information obtained about the extent to which the control addresses the risk(s) of material misstatement is an input to the auditor's control risk assessment at the assertion level.

A180. Evaluating the design and determining the implementation of identified controls in the control activities component is not sufficient to test their operating effectiveness. However, for automated controls, the auditor may plan to test the operating effectiveness of automated controls by identifying and testing general IT controls that provide for the consistent operation of an automated control instead of performing tests of operating effectiveness on the automated controls directly. Obtaining audit evidence about the implementation of a manual control at a point in time does not provide audit evidence about the operating effectiveness of the control at other times during the period under audit. Tests of the operating effectiveness of controls, including tests of indirect controls, are further described in ISA 330.[45]

---

45 ISA 330, paragraphs 8-11

A181. When the auditor does not plan to test the operating effectiveness of identified controls, the auditor's understanding may still assist in the design of the nature, timing and extent of substantive audit procedures that are responsive to the related risks of material misstatement.

Example:

The results of these risk assessment procedures may provide a basis for the auditor's consideration of possible deviations in a population when designing audit samples.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Understand control activities [ISA | 1340]

What do we do?

Obtain an understanding of control activities that is sufficient to assess the factors that affect the risks of material misstatement and to design further audit procedures.

Why do we do this?

We understand control activities, including evaluating their design and implementation, when we plan to test their operating effectiveness or when we are otherwise evaluating them as a part of risk assessment (e.g. controls over significant risks, journal entries, etc.). We refer to the control activities that we understand as relevant control activities.

Execute the Audit

What are control activities? [ISA | 1340.12185]

Control activities	Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity and at various stages within business processes, and over the technology environment. Specific to financial reporting, control activities are the policies and procedures established to mitigate (either directly or indirectly) risks of material misstatement in the business processes and financial reporting processes.

Control activities include both process control activities and general IT controls (GITCs). The table below illustrates the distinction between these two types of control activities.

	Control activities	
Types of control activities	Process control activities	General IT controls
Address	PRPs	RAFITs
Nature	Manual or Automated	

These terms are used in KAEG to distinguish how the methodology applies to each type of control activity. However, KAEG may also use the term 'control activities' or 'control' when the type of control activity being address is established in the content or is not relevant.

> For example, '*The precision of a process control activity is essentially the size of a potential misstatement the control would prevent, or detect and correct, when it operates effectively. So, a control's precision is the maximum size of a misstatement that could be accepted based on the control's design and operation.*'

We only evaluate precision for process control activities, which is made clear in the beginning of the first sentence. The broader term 'control' is used later for convenience as it is shorter and does not detract from the established application of the content.

What are process control activities? [ISA | 1340.8434]

Process control activities relate to the processing of information, in IT systems or other manual processes, that directly address PRPs.

KAEG may refer to process control activities as 'control activities' when it is apparent from the context of content that the control activity occurs in a business process and addresses a PRP.

What are general IT controls? [ISA | 1340.1300]

General IT controls (GITCs) are control activities over the entity's IT processes that support the continued effective operation of the IT environment, including:

- the continued effective operation of automated controls, and
- the integrity of data and information within the entity's IT system.

The IT processes are the entity's processes to manage access to programs and data, manage program changes, manage program acquisition and development, and manage computer operations (see activity 'Understand the entity's IT processes' for more information).

The IT environment encompasses the IT systems the entity uses as part of its financial reporting and business processes, including its layers of technology (application, database, operating system and network), the IT processes and the IT organization (see activity 'Understand how the entity uses IT as part of financial reporting' for more information).

GITCs are not expected to directly prevent, or detect and correct, material misstatements on a timely basis, but ineffective GITCs may lead to automated controls that don't operate consistently and effectively, and therefore might not prevent, or detect and correct, a material misstatement on a timely basis.

What is the difference between a control activity and a process? [ISA | 1340.12186]

We might think about the process as the actual steps necessary to record an amount into the financial records, whereas control activities are the specific actions taken along the way to mitigate risks that are introduced during the process. Said differently - processes are 'how' an entity records transactions and control activities are the different checks performed throughout the process to prevent or detect misstatements that could occur.

Why do we differentiate process activities from control activities? [ISA | 1340.11409]

Understanding the difference between activities that introduce risks - i.e. process activities - and activities that mitigate risks - i.e. control activities - is a key first step to understanding the process and flow of transactions.

Blurring the lines or misunderstanding the distinction between the process activities and the control activities hinders us from properly understanding the process and flow of transactions. This makes it difficult to appropriately perform our risk assessment procedures.

What is an example of the differences and relationship between process activities and control activities? [ISA | 1340.11410]

Consider the following example — the credit limit illustrates the differences and relationship between process activities and control activities.

Process activities	Customers place their purchase orders electronically. These orders are captured in the entity's enterprise resource planning (ERP) system and processed for fulfilment.
Identified risk	Customers could exceed their established credit limit.

Control activities to address the identified risk	The entity's ERP system compares the open receivables from the customer plus the submitted purchase order amount to the established customer credit limit. If the total amount of open receivables and purchase orders exceeds the credit limit, the purchase order is not processed further. Each purchase order not processed is followed-up manually.

Which control activities do we understand and are relevant to the audit? [ISA | 1340.1600]

We obtain an understanding of control activities that are 'relevant to the audit'. 'Control activities relevant to the audit' or 'relevant control activities' have a specific meaning in our methodology. This terminology identifies control activities that we understand and, thus, perform procedures to evaluate their design and implementation. The following are control activities relevant to the audit:

- process control activities that address RMMs:
  - where we plan to take a controls reliance approach;
  - that are significant risks;
  - that are associated with SUTs (refer to activity 'Identify SUTs') or related parties (refer to activity 'Obtain an understanding of related party processes and controls');
  - that are associated with journal entries and other adjustments (refer to activity 'Evaluate the design and implementation of control activities over journal entries and other adjustments'); or
  - where we cannot obtain sufficient evidence through substantive testing alone; or
- process control activities:
  - that we are testing over the accuracy and completeness of internal information and the RDE(s) to evaluate the reliability of such information (see activity 'Test management's controls over the accuracy and completeness of internal information'); or
  - that, in our professional judgment, we consider it appropriate to understand in order to enable us to effectively identify and assess the risk of material misstatement and design further audit procedures; and
- general IT controls that address 'relevant RAFITs' associated with 'relevant automated controls' or data integrity risks (refer to question 'Under what circumstances do we obtain an understanding of general IT controls').

What are examples of control activities that we may decide to understand for risk assessment purposes even though we will not test their operating effectiveness? [ISA | 1340.8436]

We may consider it appropriate to understand certain control activities, including evaluating their design and implementation even though we do not plan to test their operating effectiveness for the purpose of providing an appropriate basis for the identification, assessment of and response to risks of material misstatement. Examples of such controls may include:

- controls that address risks assessed as Elevated that are higher on the spectrum of inherent risk but have not been determined to be a significant risk;
- controls related to reconciling detailed records to the general ledger;
- controls related to accounting estimates; or
- complementary user entity controls, if the entity uses a service organization

How do we identify and understand relevant process control activities? [ISA | 1340.11412]

There are four steps in identifying and obtaining an understanding of relevant process control activities.

(1) Understand business processes and the financial reporting process.
(2) Identify process risk points.
(3) Determine which controls are relevant to the audit.
(4) Evaluate the design and implementation of relevant process control activities.

We achieve these four steps through properly planning and executing either (i) a walkthrough or (ii) inquiries and observations or inspections of relevant control documentation to sufficiently evaluate the design and implementation of identified controls.

Remember: we perform the first step (understanding the business process, including our understanding of IT) regardless of whether we obtain an understanding, including evaluate design and implementation, of the process control activity.

Refer to activity 'Understand how the entity has responded to RAFITs' for the steps to identify and obtain an understanding of general IT controls.

How do we efficiently obtain an understanding of relevant process control activities? [ISA | 1340.11416]

It is efficient to both:

- identify the PRPs and relevant controls; and
- evaluate the design and implementation of those controls

at the same time as obtaining an understanding of the process.

However, in doing this, we also keep in mind two things:

(1) If we're not careful, we may focus our walkthrough or inquiries and observations or inspections only on identifying PRPs and relevant process control activities, and fail to obtain an adequate understanding of the business process.
(2) Once we've determined the RMMs, we revisit the PRPs and process control activities we've identified to determine that those RMMs have associated relevant control activities, if applicable.

What is a process risk point? [ISA | 1340.11420]

A process risk point (PRP) is a point in the entity's process that a misstatement could, individually or in aggregate, yield a material misstatement to the financial statements. We describe the PRP as the 'where' and the 'how' in the entity's process that misstatement could be introduced.

PRPs are likely to be different from one entity to the next because each entity's processes are different. To be able to determine PRPs, we understand the entity's process.

How and where might PRPs arise in a business process? [ISA | 1340.11421]

PRPs arise throughout a business process or IT system, and include where and how an error could be introduced to data and information used as part of the process, including risks relating to:

- data input;
- data integrity; and
- data extraction and manipulation.

PRPs may also relate to the accuracy of calculations or other data manipulation performed by the IT system.

Every business process is likely to contain multiple PRPs. And every RMM identified also has at least one PRP.

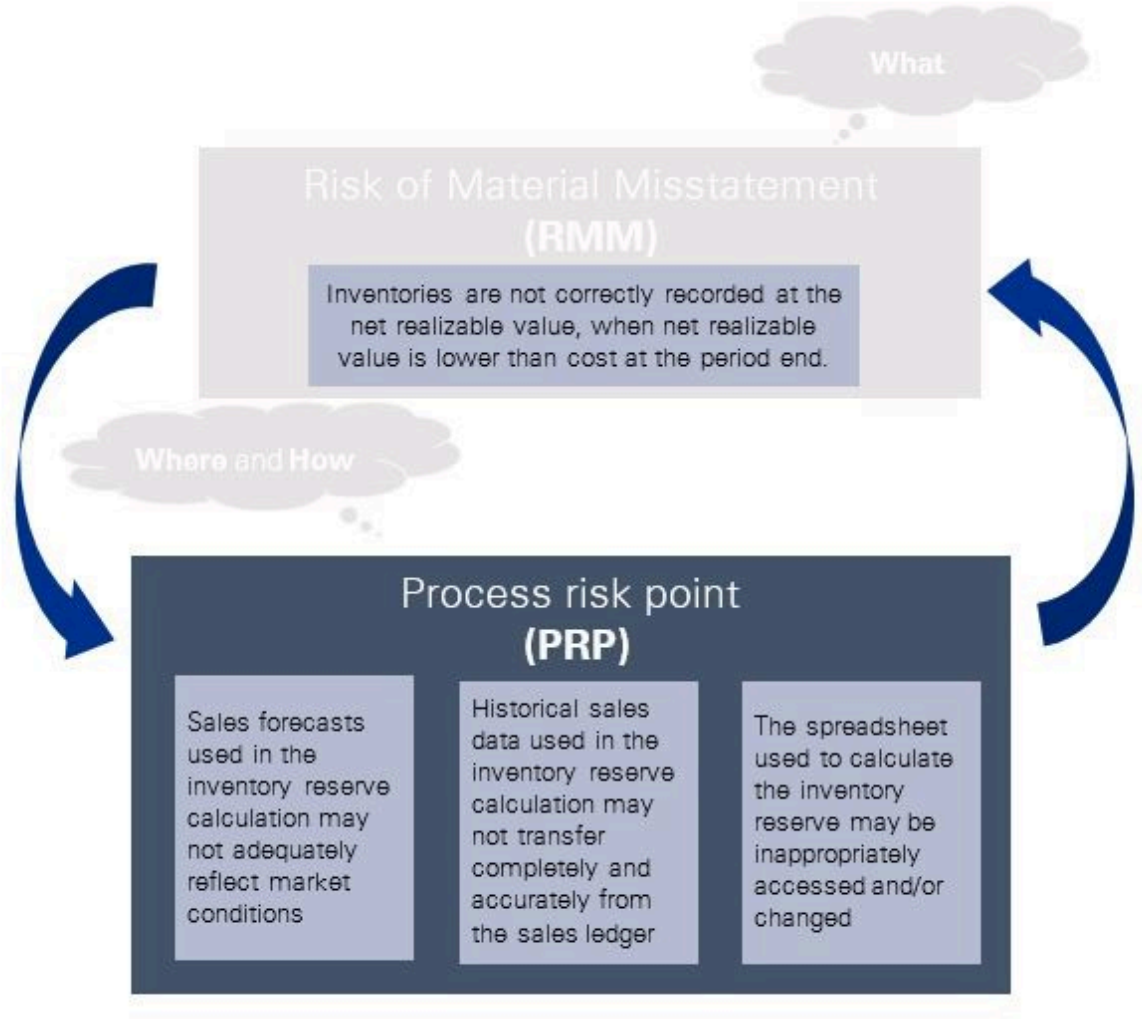
PRPs also include risks of unauthorized acquisition, use or disposition of assets that could result in a material misstatement of the financial statements.

What is the difference between a risk of misstatement and a process risk point? [ISA | 1340.11422]

Risks of misstatement (RMs) generally stem from the accounting framework, so we expect them to be the same for similar transactions across entities. Process risk points (PRPs) are the specific points where a material misstatement could be introduced by the process.

What is the relationship between an RMM and a PRP? [ISA | 1340.11423]

The RMM is really the 'what' could be misstated, whereas the PRP are the 'where' and the 'how' in the process an RMM can arise. Therefore each RMM has at least one PRP.



Will every relevant PRP be associated with an RMM? [ISA | 1340.11424]

Yes. Every relevant PRP will be associated with at least one RMM. If we have a PRP without an RMM, we revisit the identification of RMMs.

Can an RMM and a PRP ever be the same thing? [ISA | 1340.11425]

Possibly. This may happen when there is a review control designed to determine whether the accounting criteria is met.

For example, suppose the RMM is that a contract is inappropriately determined to be within or outside the scope of the revenue recognition standard (from the Library "Contracts, or parts of contracts, are not appropriately identified as within or outside the scope of Topic 606/IFRS 15").

The entity's process may be that someone analyzes each contract to determine whether it is within the scope of the revenue recognition standard. There is a PRP that the analysis is incorrect and the person reaches the wrong conclusion. This PRP mirrors the RMM.

However, other PRPs are likely in that process that may also be linked to this RMM. For example, there could be a PRP that all contracts are not sent to Finance for analysis. This type of PRP still

relates to the RMM that a contract is inappropriately determined to be within or outside the scope of the revenue recognition standard, but it is not the same as the RMM.

Other PRPs that are tied to an RMM but are not the same as the RMM might include risks related to the completeness and accuracy of data as it:

- moves through a system;
- is generated into a report;
- is stored in a database; or
- is recorded in the ledger via an automated or manual journal entry.

Why do we distinguish between RMMs and PRPs? [ISA | 1340.11426]

PRPs are related to the RMMs because an entity's process is designed to account for transactions - i.e. apply appropriate accounting standards given the transaction. However, although they are related, our audit response is different depending on whether we are addressing an RMM or a PRP.

Our substantive procedures are designed to address RMMs, while our control testwork procedures are designed to test the entity's controls that address PRPs.

For example, the RMM might be that a contract does not belong within the scope of the revenue recognition standard.

PRPs, on the other hand, are specific to the entity's process and may include the following:

- not all contracts are sent to the Finance department to be analyzed; or
- the contract is analyzed, but an incorrect conclusion is reached.

Clearly, the RMM and the PRPs are related, but the RMM calls for a different response than the PRPs.

Our substantive procedures to address the RMM could be to sample contracts and analyze them to determine whether they are within the scope of the revenue recognition standard. The attributes of our substantive tests do not include whether all contracts were sent to Finance, or whether they were analyzed by Finance; those are procedures to address the PRPs.

Our control testwork procedures are designed to test the entity's controls that address the PRPs, and therefore focus on whether all contracts were analyzed by Finance and whether the analysis reached an appropriate conclusion.

How are control activities affected by the other components of ICFR? [ISA | 1340.1801]

Control activities complement the other components of internal control. For example:

- proper design and implementation of control activities are supported by an effective risk assessment;
- determining that the controls operate as intended is supported by monitoring;
- providing control operators with the information to operate controls properly is supported by appropriate levels of information and communication; and
- a robust control environment lays the foundation for an effective system of internal controls.

Because the five ICFR components are distinct but interrelated, deficiencies in one component may affect controls in another, and so may ultimately cause us to change our audit response for other tests of controls or substantive procedures.

How are monitoring activities different from process control activities? [ISA | 1340.1800]

The key difference between process control activities and monitoring activities relates to their objective and their relationship to the risk of material misstatement of an entity's financial statements.

With process control activities, that relationship is direct: each process control activity's objective is to mitigate a specific risk within a business process that could lead to a material misstatement of the entity's financial statements. We call that risk a process risk point (PRP).

Accordingly, process control activities are designed and operated with a level of precision that allows both management and external auditors to be confident that they would prevent or detect, in a timely manner, a material misstatement to the entity's financial statements.

On the other hand, monitoring activities have only an indirect relationship to the risk of misstatement (RM) of an entity's financial statements. They do not themselves mitigate risks to specific financial statement assertions. Instead, they monitor the continuing appropriateness of the design and operating effectiveness of control activities and controls within other components of ICFR (Control Environment, Risk Assessment, Control Activities, and Information and Communication).

The objective of monitoring activities is to:

- timely identify deficiencies in controls;
- analyze their root causes; and
- design and implement effective remediation plans.

For example, the intent of a monthly completeness control activity would be to detect and correct errors; whereas a monitoring activity would ask why there were errors in the first place and assign management the responsibility of fixing the process to prevent future errors.

Monitoring activities *could* identify a misstatement in the entity's financial statements. But they're more likely to identify instances where control activities did not operate effectively, and where further investigation as to the propriety of financial reporting may be necessary.

When it comes to mitigating the RMMs of an entity's financial statements, the difference in the level of assurance provided by process control activities ('would' level) and monitoring activities ('could' level) has implications for how we rely on their assessment of the entity's ICFR.

Process Control activities	Monitoring activities
• Respond to specific risks (PRPs) at the process level	• Monitor the effective operation of control activities and other components of ICFR • Monitor operations to identify unusual trends or anomalies that may warrant investigation
• Designed with sufficient precision to prevent, or detect and correct errors	• Could identify errors themselves, but that is not the objective of their design

in financial statement assertions at the 'would' level of assurance	• Designed to identify the cause of errors • Monitor the remediation of deficiencies

1.1 Identify process risk points [ISA | 1341]

What do we do?

Identify process risk points that could cause the financial statements to be materially misstated.

Why do we do this?

We identify the points in the entity's process where a misstatement could be introduced so that we can then:

- determine which controls are relevant to address those process risk points (PRPs);
- further assess the factors that affect the risks of material misstatement (RMMs); and
- design further audit procedures.

Execute the Audit

Where are we in identifying and understanding relevant process control activities'? [ISA | 1341.1300]

We are in step 2 of identifying and obtaining an understanding of relevant process control activities.

(1) Understand business processes and the financial reporting process
(2) **Identify process risk points**
(3) Determine which control activities are relevant to the audit
(4) Evaluate the design and implementation of relevant process control activities

Under what circumstances do we identify process risk points? [ISA | 1341.1400]

We identify PRPs, and the relevant process control activities that mitigate them, in the following cases:

- an integrated audit;
- when we evaluate the design and implementation (regardless of whether we go on to test the operating effectiveness of process control activities) in a non-integrated audit

How do we identify PRPs? [ISA | 1341.2000]

We identify PRPs as part of our understanding of a process and link them to relevant RMMs.

We identify PRPs in either:

- our flowcharts (supplemented by a description outside the flowchart when necessary); or
- a process narrative.

When we identify PRPs, they are in sufficient detail to allow a reviewer to understand the specific condition that allows for a material misstatement to be introduced in the process. The specificity and clarity with which we define an identified PRP is key to our ability to identify relevant process control activities that respond appropriately to that specific PRP.

PRPs are likely to be more detailed than the associated RMMs as a PRP is intended to describe the 'where' and the 'how' a misstatement could occur in the process.

Poorly worded PRPs	Better
Accounts payable and accrual balances (A/P and Accruals) are incomplete	Invoices are received in the mail after period-end that relate to the current period but are not accrued for in the correct period. [CEA of A/P and Accruals.] Significant agreements contain embedded derivatives, leases, contingencies, guarantees, and/or consolidation issues that are not identified and accounted for appropriately. [CEA of A/P and Accruals; C of Derivative Assets/Liabilities; C of Capital Leases; C of Derivatives, Lease, Guarantee and Consolidation Disclosure Matters.]
Expenditures are overstated	Duplicate vendor invoices are paid. [E of Expenses.]
Accounts payable is not accurately presented in the financial statements.	Receivables and accounts payable are inappropriately presented net (i.e., offset). [P of Receivables and A/P.] Debit balance inappropriately exist within the accounts payable balance that is ultimately recorded on the financial statements (i.e., debit balances exist in the accounts payable sub-ledger). [P of A/P.]
Selling, general and administrative expenses are incomplete.	Vendor invoices are not submitted on a timely basis to the accounts payable department by various corporate head office departments, and thus are not recorded in the correct period. [CEA of SG&A Expenses and A/P.]

When documenting PRPs, we do not anchor to PRPs identified in prior year audits. Management's processes frequently change due to changes in the business, changes in IT systems, changes in personnel, etc.

How could a poorly worded PRP lead to ineffective identification or evaluation of process control activities? [ISA | 1341.11435]

When we identify very general PRPs, identifying a specific process control activity (or process control activities) that mitigate the risk may be difficult. Without sufficiently detailed PRPs, we may fail to:

- identify the right process control activities; and/or

- properly evaluate whether the process control activities addresses all the relevant PRPs.

For example, a poorly worded PRP might be:

"The statement of cash flows is incorrect."

To address the PRP as documented we may choose to rely on and evaluate the design and implementation and test the operating effectiveness of a process control activity defined as:

"Management's review of the statement of cash flows."

However, a properly designed review of the statement of cash flows does more than just review its 'proof' and tie numbers to the balance sheet, such as reviewing:

- key information about non-cash transactions;
- proper classification of certain cash inflows or outflows;
- foreign currency impacts; and/or
- items that are reported on a gross basis.

Where might PRPs occur in a process? [ISA | 1341.11436]

There are many points in a process where PRPs may occur. When identifying PRPs, we pay particular attention to circumstances where PRPs are more likely, such as:

- how data:
  - enters an IT system;
  - is stored within the IT system;
  - may be accessed or transferred to another system;
- points in the process at which data is summarized, accumulated, subjected to calculations or otherwise manipulated;
- manual processes that affect the data (e.g. manual journal entries);
- management review processes over the data ;
- judgments made by management in determining:
  - whether or not to adjust data; and
  - the amount of any adjustments;
- how data is affected when it is summarized for inclusion in the financial statements (e.g. top-side entries during the period-end financial reporting process).

Examples

What is the difference between an RMM and a PRP? [ISA | 1341.2300]

Scenario 1

Fact pattern:

Two entities operate in the same industry, are the same size and complexity, have very similar contracts and transactions with their customers, and apply the same accounting policies or principles.

Analysis:

The same RMs applies to these entities, because they are based on:

- balances, classes of transactions and disclosures; and
- inherent risk without regard to controls.

Since the entities transactions are similar in size and nature, the engagement team identifies and assesses the same RMMs.

Scenario 2

Fact pattern:

The same two entities from Scenario 1 use IT in different ways.

Entity One is heavily IT-reliant, with connected information systems, electronic source data and automated controls.

Entity Two uses IT scarcely. Most business processes are maintained in separate systems and the organization is reliant on spreadsheets and manual controls.

Analysis:

The entities still have the same RMMs because the balances, classes of transactions and disclosures are the same and RMMs are driven by accounting policies or principles, not the entity's specific processes.

However, they have different PRPs because the business processes differs.

The PRPs for Entity One relate to:

- automated processes;
- data transfers; and
- risks around identification and review of exceptions.

The PRPs for Entity Two relate to:

- the relevance and reliability of data in manual spreadsheets; and
- the many points within the process where manual errors could occur.

How do RMMs relate to PRPs and process control activities? [ISA | 1341.11438]

RMMs describe **what** the misstatement to the financial statements can be and PRPs describe **where** and **how** in the process the misstatement can occur. The below shows an example of how each relate to each other.

Example risk of misstatement (What)	Example Process risk points (Where and How)	Example process control activities
For performance obligations satisfied at a point in time, revenue is not recognized when control is transferred to the customer, resulting in revenue not being recognized in the correct period	PRP1: The record of goods shipped (i.e. the shipping documents) does not match the goods shipped (either for quantity or product).	Control 1 (PRP1): Warehouse personnel authorize the shipping documents by counting the goods staged for shipment to verify quantities match the shipping paperwork to ensure completeness and

		accuracy of the materials and quantities shipped.
	PRP2: The system is not configured appropriately to recognize revenue upon shipment delivered to the customer.	Control 2 (PRP2): The system is configured such that a shipping document is not generated without a processed sales order and the sales order cannot be invoiced until a delivery record is confirmed and entered into the system by the staff.

1.2 Determine which control activities are relevant to the audit [ISA | 1342]

What do we do?

Determine which controls are relevant to the audit.

Why do we do this?

When we determine which control activities are relevant to the audit, we identify the control activities that we will understand and perform procedures to evaluate their design and implementation.

Execute the Audit

Where are we in identifying and understanding relevant process control activities? [ISA | 1342.1300]

We are in step 3 of identifying and obtaining an understanding of relevant process control activities.

(1) Understand business processes and the financial reporting process
(2) Identify process risk points
(3) **Determine which controls activities are relevant to the audit**
(4) Evaluate the design and implementation of relevant process control activities

Which control activities do we understand and are relevant to the audit? [ISA | 1342.1600]

We obtain an understanding of control activities that are 'relevant to the audit'. 'Control activities relevant to the audit' or 'relevant control activities' have a specific meaning in our methodology. This terminology identifies control activities that we understand and, thus, perform procedures to evaluate their design and implementation. The following are control activities relevant to the audit:

- process control activities that address RMMs:
  - where we plan to take a controls reliance approach;
  - that are significant risks;

  - that are associated with SUTs (refer to activity 'Identify SUTs') or related parties (refer to activity 'Obtain an understanding of related party processes and controls');
  - that are associated with journal entries and other adjustments (refer to activity 'Evaluate the design and implementation of control activities over journal entries and other adjustments'); or
  - where we cannot obtain sufficient evidence through substantive testing alone; or
- process control activities:
  - that we are testing over the accuracy and completeness of internal information and the RDE(s) to evaluate the reliability of such information (see activity 'Test management's controls over the accuracy and completeness of internal information'); or
  - that, in our professional judgment, we consider it appropriate to understand in order to enable us to effectively identify and assess the risk of material misstatement and design further audit procedures; and
- general IT controls that address 'relevant RAFITs' associated with 'relevant automated controls' or data integrity risks (refer to question 'Under what circumstances do we obtain an understanding of general IT controls').

What are examples of control activities that we may decide to understand for risk assessment purposes even though we will not test their operating effectiveness? [ISA | 1342.8436]

We may consider it appropriate to understand certain control activities, including evaluating their design and implementation even though we do not plan to test their operating effectiveness for the purpose of providing an appropriate basis for the identification, assessment of and response to risks of material misstatement. Examples of such controls may include:

- controls that address risks assessed as Elevated that are higher on the spectrum of inherent risk but have not been determined to be a significant risk;
- controls related to reconciling detailed records to the general ledger;
- controls related to accounting estimates; or
- complementary user entity controls, if the entity uses a service organization

How do we determine which control activities to understand and evaluate when there are two or more control activities that address the same objective? [ISA | 1342.8442]

If there are multiple control activities that address the same objective - e.g. redundant or duplicative controls that address either the same PRP or RAFIT, then we identify the control activity that management relies on and evaluate the design and implementation of that control activity.

What if we have not identified all significant risks at this point in the risk assessment process? [ISA | 1342.1500]

At this point in the risk assessment process (and because an audit is iterative), we may not have assessed significant risks. However, we may have performed several risk assessment procedures - such as considering information from prior audits, analytical procedures, and inquiries - so we have a preliminary idea of the processes likely to contain an RMM.

The risk assessment process is iterative; if we later identify a significant risk, we:

- evaluate the design and implementation of those control activities; and
- consider that evidence in the identification of this and other risks.

How do we identify relevant process control activities to test? [ISA | 1342.1601]

To determine which process control activities are relevant to the audit, we identify the process control activities that address relevant PRPs that are linked to the RMMs. We may do this while we obtain our understanding of the business process.

The process control activities we identify are the entity's manual or automated policies or procedures to prevent, or detect and correct, errors or fraud that could directly result in material misstatements of the financial statements. Process control activities operate at a 'would' level of assurance.

What is a 'would' level of assurance? [ISA | 1342.11267]

We have coined the phrase 'would-level control' to differentiate those controls that provide reasonable assurance that the control would prevent, or detect and correct, a material misstatement on a timely basis.

'Would' in this context means 'probable'. For a control to function properly as a process control activity, it operates in a manner that allows management and us to confidently say it would - i.e. probably will - prevent or detect a material misstatement.

How do we identify relevant general IT controls to test? [ISA | 1342.8443]

To determine which general IT controls are relevant to the audit, we understand how the entity has responded to RAFITs (refer to activity 'Understand how the entity has responded to RAFITs'.

Are control activities that mitigate fraud risks always relevant to the audit? [ISA | 1342.1700]

Yes. As fraud risks are significant risks, the control activities an entity designs and implements to mitigate fraud risks are relevant control activities.

Can one process control activity address multiple PRPs or multiple RMMs? [ISA | 1342.11265]

Yes, when the control is designed to adequately address each PRP for the related RMMs. However, we carefully evaluate how the control responds to each PRP and clearly capture how the control is designed to address each PRP in our evaluation of design and test of operating effectiveness of the control.

For example, companies may have a comprehensive control over the review of a financial statement tie-out binder or a comprehensive review and reconciliation control over the presentation of the cash flow statement, which are designed to cover multiple PRPs and RMMs. To the extent that the control

is appropriately designed to address each of the associated PRPs, it may be appropriate to link the comprehensive control to multiple PRPs.

Do we identify PRPs and controls related to a service organization? [ISA | 1342.11266]

If the service organization's controls are relevant to the audit, we identify PRPs within the entity's business process that relate to activities at the service organization and the related service organization controls. We also identify PRPs around the relevant handoffs of data between the service organization and the entity as well as any complementary user entity controls (CUEC). Refer to 'Understand the service organization's activities and internal controls' for further information.

1.3 Evaluate the design and implementation of relevant process control activities [ISA | 1343]

What do we do?

Evaluate the design and implementation of relevant process control activities

Why do we do this?

As part of obtaining an understanding of internal control over financial reporting (ICFR), we:

- evaluate the design of process control activities that are relevant to the audit; and
- determine whether they have been implemented.

We use the understanding obtained to identify and assess RMMs and consider our planned response to identified risks.

Execute the Audit

Where are we in identifying and understanding relevant process control activities? [ISA | 1343.1300]

We are in step 4 of identifying and obtaining an understanding of relevant process control activities.

(1) Obtain an understanding of the process that is sufficient to assess the factors that affect the risks of material misstatement and to design further audit procedures.
(2) Identify process risk points
(3) Determine which controls are relevant to the audit.
(4) **Evaluate the design and implementation of relevant process control activities.**

Which control activities do we understand and are relevant to the audit? [ISA | 1343.1600]

We obtain an understanding of control activities that are 'relevant to the audit'. 'Control activities relevant to the audit' or 'relevant control activities' have a specific meaning in our methodology. This terminology identifies control activities that we understand and, thus, perform procedures to evaluate their design and implementation. The following are control activities relevant to the audit:

- process control activities that address RMMs:
  - where we plan to take a controls reliance approach;
  - that are significant risks;