THE RISK IDENTIFICATION AND ASSESSMENT PROCESS: TIPS ON IMPLEMENTING ISA 315 (REVISED 2019)

Looking for tips on how to implement selected new and other requirements in International Standard on Auditing (ISA) 315 (Revised 2019)? Interested in why some of the requirements in ISA 315 (Revised 2019) exist and how they drive an effective audit? Read this guidance to find out!

DISCLAIMER

This Tool is designed to assist practitioners in the implementation of ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement*, but is not intended to be a substitute for reading the standard itself. It does not address all requirements in ISA 315 (Revised 2019) and focuses on only selected new requirements and certain other requirements.

Furthermore, a practitioner should utilize this Tool in light of his/her professional judgment and the facts and circumstances involved in each particular audit. It should also be noted that the examples provided are not exhaustive and do not represent every aspect of risk identification and assessment but are rather provided to help guide the auditor through some specific scenarios rather than through every situation that may be encountered on an audit.

IFAC disclaims any responsibility or liability that may occur, directly or indirectly, as a consequence of the use and application of this Tool.

Standard Discussed

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

Effective Date

The changes to ISA 315 (Revised 2019) are effective for audits of financial statements for periods beginning on or after December 15, 2021. [1]

1 ISA 315 (Revised 2019) also applies to audits within the scope of ISA 805, *Special Considerations — Audits of Single Financial Statements and Specific Elements, Accounts or Items of Financial Statement.* ISA 315 (Revised 2019) is adapted as necessary in the circumstances when applied to audits of other historical financial information.

Focus of This Tool

This non-authoritative *Implementation Tool for Auditors (Tool)* emphasizes the scalability of the standard with a focus on less complex entities (LCEs).[2]

Form and Content of This Tool

The following is a summary of the contents of this *Tool*:

- Figure 1 — an overview of the risk identification and assessment process in ISA 315 (Revised 2019).
  - Each **Figure 1** label appears in a callout indicated by N1. To get to a section discussing a particular subject, click on the appropriate label. To get back to Figure 1, click directly from each section. The positioning of the callout in Figure 1 indicates the part of the risk identification and assessment process to which the matter discussed primarily relates.
- A brief discussion of selected core concepts underlying the risk identification and assessment process and how you apply it such as:
  - Dynamic and iterative risk assessment process
  - Professional judgment and professional skepticism
  - Scalability
- Explanations of certain:
  - New requirements (questions N1 to N6)
    - The explanations of new requirements (questions N1 to N6) may include how they relate to other requirements and application material that are not new.
  - Other requirements (questions O1 to O5)

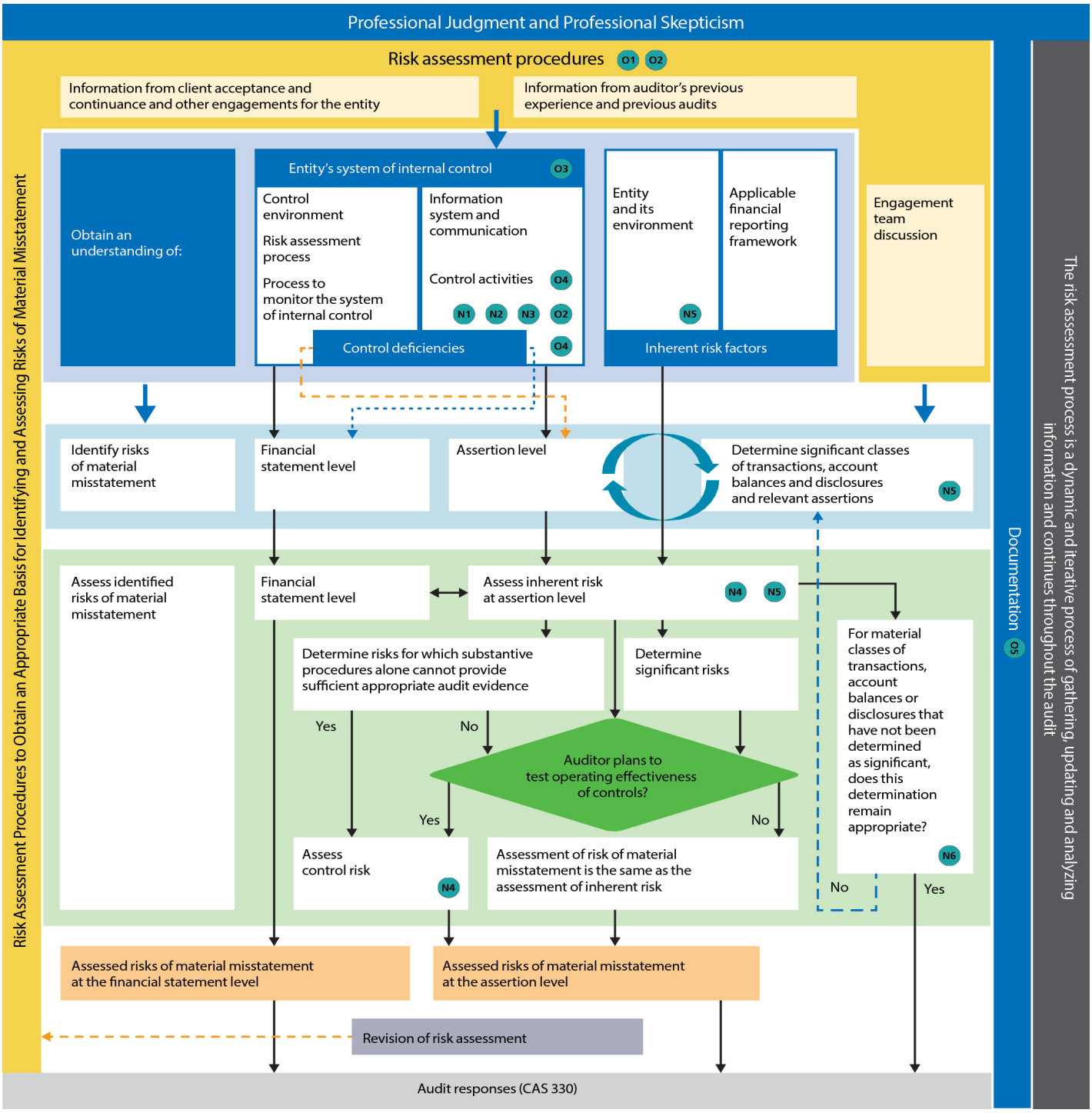
Acknowledgement

The *Tool* is based on the Chartered Professional Accountants of Canada (CPA Canada) Implementation Tool for Auditors and is used with permission of CPA Canada.

2 The ISAs do not define a less complex entity (LCE). ISA 315 (Revised 2019) is intended for audits of all entities, regardless of size or complexity, and the application material therefore incorporates specific considerations for 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. The IAASB currently has a **proposal** for a new standard for audits of LCEs that provides some additional context on what might constitute an LCE.

Overview of the Risk Identification and Assessment Process in ISA 315 (Revised 2019)

Figure 1[3,4]: OVERVIEW OF THE RISK IDENTIFICATION AND ASSESSMENT PROCESS IN ISA 315 (Revised 2019)



3 This figure is an extract from Introduction to ISA 315 (Revised 2019): *Identifying and Assessing the Risks of Material Misstatement* of the International Auditing and Assurance Standards Board, published by the International Federation of Accountants in December 2019.

4 ISA 315 (Revised 2019) is intended for audits of all entities regardless of size or complexity. The application material and this guidance incorporate considerations specific to less complex entities.

Selected Core Concepts Underlying the Risk Identification and Assessment Process

Objective

ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement*, has been significantly revised. The changes and new requirements are intended to clarify and assist you in identifying and assessing the risks of material misstatement in a more consistent and robust manner. Once risks of material misstatement are identified and assessed, ISA 330, *The Auditor's Responses to Assessed Risks*, requires you to design and perform further audit procedures to appropriately respond to those risks of material misstatement and conclude whether you obtained sufficient appropriate audit evidence. The quality of your risk identification and assessment (herein referred to as "risk assessment") process therefore has a pervasive effect on all aspects of the audit. Obtaining an understanding of the entity and its environment, the applicable financial reporting framework (AFRF) and the entity's system of internal control provides you with a frame of reference within which you identify and assess risks of material misstatement. While this ISA has been significantly revised, the audit risk model and your objective to identify and assess the risks of material misstatement at the financial statement and assertion levels, whether due to fraud or error, remain unchanged.[5]

Dynamic and Iterative Risk Assessment Process

The right-hand column in **Figure 1** states that the risk assessment process is dynamic and iterative. Your preliminary risk assessments, and planned responses to those assessments, may need to change when new information is obtained as your audit progresses. You need to be alert to this possibility throughout the audit. This may include changes to both your overall responses and further audit procedures. This key point is highlighted by the inclusion of the "revision of risk assessment" box near the bottom of the figure.

Professional Judgment and Professional Skepticism

ISA 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing* requires you to exercise professional judgment and maintain professional skepticism[6] throughout the planning and performance of the audit, including when performing risk assessment procedures.[7] For example, one judgment you need to make is whether an identified risk is a significant risk (see question **N5**).

Changes have been made within the standard to encourage a more skeptical mindset of the auditor when undertaking risk assessment procedures. It is important to emphasize that when designing and performing risk assessment procedures, you do so in a way that is not biased toward obtaining audit evidence that may be corroborative or toward excluding audit evidence that may be contradictory. This may assist you in exercising professional skepticism in identifying and assessing the risks of material misstatement. Professional skepticism is an attitude applied when making professional judgments, which then provides the basis for one's actions.

5 The IAASB **Fact Sheet** Introduction to ISA 315 (Revised 2019) *Identifying and Assessing Risks of Material Misstatement* contains an overview of the significant changes.

6 ISA 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*, defines "professional judgment" and "professional skepticism." See ISA 200.13 (k) and (l).

7 ISA 315.12(j) defines "risk assessment procedures" as 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.

In simple terms, when exercising professional skepticism, you are not simply aiming to evidence a figure presented in the financial statements. You may exercise professional skepticism by:

- 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 your identification and assessment of the risks of material misstatement in light of the entity's nature and circumstances.

Scalability

ISA 315 (Revised 2019) applies to the audit of the financial statements of all entities, regardless of their nature, size or complexity. ISA 315 (Revised 2019) includes some new application material paragraphs (including examples) setting out matters for you to consider when auditing the financial statements of a less complex entity (LCE). These paragraphs are identified by "Scalability" headings.

Overall, the scalability paragraphs provide you with context for how to apply the requirements of ISA 315 (Revised 2019) to all types of entities – from those entities that are less complex to those that are complex – and support the exercise of professional judgment in determining the audit procedures you perform. Also, these paragraphs provide useful reminders that LCEs may have systems and processes that lack formality and that various aspects of the LCE's system of internal control are affected by the direct involvement of the owner-manager of a business or the executive director of a not-for-profit organization (for simplicity, referred to as the "owner-manager" in the examples included within this *Tool*), and may still be appropriate to the nature and circumstances of the entity.

Note: This Tool discusses various matters related to scalability. The explanations and examples included below are provided in the context of auditing the financial statements of an LCE.

Explanation of New Requirements

N1 - Why does ISA 315 (Revised 2019) now specify the controls you are required to identify in order to understand the control activities component?
(ISA 315.26)

Previously, you were required to identify "controls relevant to the audit." The specific controls required to be identified were included in various standards, resulting in different interpretations and inconsistent practice. Therefore, in revising ISA 315 (Revised 2019) the IAASB collected and grouped together all the relevant controls required to be understood for the purpose of identifying and assessing risks of material misstatement that will provide clarity on which controls are subject to the requirements of the control activities component.

Return to **Figure 1**.

In order to understand the control activities component, you are required to identify controls that address risks of material misstatement at the assertion level.

Where they exist, they include:

1. Controls that address a risk you determine to be a significant risk
2. Controls over journal entries, including non-standard journal entities used to record non-recurring unusual transactions or adjustments
3. Controls for which you plan to test operating effectiveness in determining the nature, timing and extent of substantive testing (these controls include controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.)
4. Other controls that, based on your professional judgment, you consider are appropriate for you to meet the objectives of obtaining audit evidence that provides an appropriate basis for:
    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

- General IT controls that address risks arising from the entity's use of IT

Other International Standards on Auditing[8] also ask you to identify the following specific controls within the components of internal control when applicable:

- Controls that relate to information processed by a service organization
- Controls established in relation to related party relationships to identify, account for, and disclose in accordance with the AFRF, authorize and approve significant transactions and agreements with related parties, and authorize and approve significant transactions and arrangements outside the normal course of business

You should refer to the applicable subparagraphs in ISA 315.26 and paragraphs A147-A157 for more details regarding controls 1. through 5. above. In addition, the IAASB has developed an **ISA 315 (Revised 2019) First-Time Implementation Guide**, and paragraphs 57-64 are particularly helpful explaining the identified controls in the control activities component.

8 ISA 402, *Audit Considerations Relating to an Entity Using a Service Organization* (paragraph 10) and ISA 550, Related Parties (paragraph 14).

For those controls you identify in the control activities component, you are required to:

- Evaluate whether the control is designed effectively to address the risk of material misstatement at the assertion level, or effectively designed to support the operation of other controls, and
- Determine whether the control has been implemented by performing procedures in addition to inquiry of the entity's personnel.

If you conclude that these controls are not appropriately designed to prevent, or detect and correct, a material misstatement, or have not been implemented, you are required to determine whether, individually or in combination, such deficiencies constitute a significant deficiency under ISA 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*,[9] and may need to consider the effect of the control deficiency on the design of further audit procedures in accordance with ISA 330.[10]

See question **O3** for a discussion of why you are required to obtain an understanding of the control activities component of the entity's system of internal control.

See question **O2** for more information on obtaining audit evidence about the design and implementation of controls in the control activities components.

The following are examples of how paragraph 26 in ISA 315 (Revised 2019) may be applied.

1. Controls that address a risk you determine to be a significant risk

All assessed risks of material misstatement due to fraud are treated as significant risks - there is a rebuttable presumption that there are risks of fraud in revenue recognition.[11] In addition, there could also be significant risks that are not related to risks of fraud in revenue recognition.

Example 1

A significant risk of material misstatement in revenue may arise, for example, when an LCE provides services under contracts where the terms of such agreements introduce complexities, including the need for estimates regarding when to recognize revenue and the amounts to be recognized. The risk would be that revenue is not being captured in the proper period and the amounts recognized are not in accordance with the AFRF. In this case, processes related to testing controls design and implementation may relate to (1) the way such contracts are identified, (2) the determination by knowledgeable personnel of how the contracts should be accounted for in accordance with the AFRF and (3) performance obligations and management's estimates, to help ensure that the appropriate amounts have been recorded.

Example 2

The LCE may have designed its accounting system to record revenues from the sale of its goods on a free-onboard (FOB) shipping point basis. That is, under the terms of the sales contracts, transfer of risks from the LCE to its customer takes place when the goods leave the LCE's premises. However, the LCE may also have FOB destination sales contracts. That is, the transfer of risks and rewards required to recognize revenues takes place only when the customer receives the goods. Therefore, at period end, revenues could be overstated for goods shipped on an FOB destination basis that have not yet been received by

9 ISA 315.A183.

10 ISA 315, A182.

11 ISA 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements* (paragraphs 27-28).

customers. The LCE has designed a control to identify all FOB destination sales whereby the goods have not yet arrived at the destination by yearend. Based on the average lag time to arrive at the destination (about two weeks), the A/R clerk obtains the last two weeks of FOB destination sales and reconciles them to the carrier information confirming arrival date at the destination. Any goods not received by year-end require a journal entry to reverse the sale.

Having identified an opportunity to commit fraud by shifting revenues to the current period without having met the revenue recognition criteria, the auditor should consider the fraud risk factors related to incentive or pressure to commit fraud and the magnitude of FOB destination sales and therefore that a fraud risk in revenue recognition could exist because of the possibility of a material misstatement. The identified control "A/R clerk reconciliation of FOB destination sales to carrier information" would therefore be identified as the appropriate control to address the significant risk.

2. **Controls over journal entries (including non-standard journal entities used to record non-recurring unusual transactions or adjustments)**

Because of 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, automated or manual, controls over journal entries are identified for all audits. In addition, there could be a risk that "improper" journal entries can be used to override valid recording or to manipulate the financial statements.

Specific examples include:

a. Having appropriate segregation of duties between the preparer and the approver of manual journal entries

b. Having appropriate interface controls between sub-ledgers and the general ledger for automated journal entries

See question **N2** for information on what controls over journal entries are within the scope of paragraph 26.

See question **N3** for a discussion and example on which general IT controls are required to be identified in relation to controls over journal entries.

3. **Controls for which you plan to test operating effectiveness in determining the nature, timing and extent of substantive testing**

You may encounter circumstances when you conclude that testing the operating effectiveness of one or more controls is likely to be an effective and efficient audit approach in determining the nature, timing and extent of your substantive procedures. This may be the case, for example, when the revenue transaction stream of the LCE comprises a large volume of small homogeneous amounts.

For example, when auditing the financial statements of a convenience store, you may evaluate that this LCE has effectively designed and implemented controls over its automated point-of-sale receipts process and its process to reconcile sales receipts to recorded bank deposits. As a result, you may conclude that it would be appropriate to test the operating effectiveness of those controls in order to help design your substantive procedures, including determining the extent of that testing.

4. **Other controls that, based on your professional judgment, you consider are appropriate for you to meet the objectives (see point 4 above for objectives)**

Controls that you may consider are appropriate to meet the objectives of obtaining audit evidence that provides an appropriate basis for the identification and assessment of risks and the design of further audit procedures. This may include controls that address identified risks of material misstatement you have assessed as being higher on the spectrum of inherent risk but have not been determined to be significant risks. Such controls may, for example, be intended to address inherent risks in the dark pink boxes in **Figure 3** (i.e., those relating to the combination of moderate likelihood / high magnitude or high likelihood / moderate magnitude).

For example, the nature of the LCE's business and aspects of its information system may result in numerous items being placed in suspense accounts. Because of the nature of suspense account, you have initially determined suspense accounts to be assessed as being higher on the spectrum of inherent risk (but not a significant risk) – i.e., there is a higher risk of material misstatement in the suspense account but its not a significant risk for the LCE. Based on your professional judgment, you may determine that policies and procedures (i.e., the controls) related to the timely follow-up and clearing of suspense items are important to preventing or detecting and correcting any material misstatements that may arise. You identify controls over the reconciliation, clearing, and review of suspense accounts, and the types of activities that can be performed related to those accounts. These controls are in the control activities component. If you conclude that these controls are not appropriately designed to prevent, or detect and correct, a material misstatement, or have not been implemented, you are required to determine whether, individually or in combination, the deficiencies constitute a significant deficiency under ISA 265[12]. If you have identified one or more controls deficiencies, you may consider the effect of those deficiencies on the design of further audit procedures in accordance with ISA 330[13], such as performing more extensive or different procedures regarding the disposition of suspense items, and perhaps assigning more experienced personnel to perform these procedures. As a result of this, you may also identify new risks of material misstatements or assess inherent risk higher on the inherent risk spectrum. For example, you may have initially determined that suspense accounts are not a significant risk; however, after obtaining the above information, you may conclude that the likelihood of a risk of a material misstatement is actually higher if there are no controls over the suspense accounts.

5. **General IT Controls (GITCs)**

You identify these GITCs by[14]:

a. Identifying the related IT applications and other aspects of the entity's IT environment (i.e., IT infrastructure and IT processes) that are subject to risks arising from using that IT, **based on the controls identified in points 1. to 4. of the first paragraph of this section**

b. Identifying the risks arising from the entity's use of IT for those applications and other aspects of its IT environment identified in the bullet above

c. Identifying the GITCs that address those risks[15]

12 ISA 315.A183.

13 ISA 315.A182.

14 ISA 315.26 (b)-(c).

15 ISA 315.12 contains definitions of GITCs, IT environment and risks arising from the use of IT.

The above steps need not be complex but are dependent on the controls identified in points 1. to 4. of the first paragraph of this section, the extent and complexity of IT applications, the different layers of IT infrastructure supporting those IT applications and the relevant IT processes.

For example, with regard to the controls around the suspense accounts noted in (d) above, there are also access controls for the suspense accounts (i.e., who has access to process transactions to this account). This would be an example of a general IT control that would be identified for the purpose of this requirement.

See question **O4** for an example of how the above steps are applied for non-complex commercial software.

Furthermore, Appendix 6 of ISA 315 (Revised 2019) provides examples of GITCs to address certain risks arising from the use of IT.

N2 - What controls over journal entries are within scope of paragraph 26(a)(ii) of ISA 315 (Revised 2019)?

Paragraph 26(a)(ii) of ISA 315 (Revised 2019) (in the control activities component) requires you to identify "controls over journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments."

Professional judgment is used to determine the journal entries that are relevant for the purpose of identifying the controls in paragraph 26(a)(ii)[16] of ISA 315 (Revised 2019). In today's environment where there are significant automated processes, you will need to distinguish controls over those journal entries that need to be focused on for the purpose of paragraph 26(a)(ii) of ISA 315 (Revised 2019).

Return to **Figure 1.**

Paragraph 25 of ISA 315 (Revised 2019) requires you to "understand the entity's information system and communication relevant to the preparation of the financial statements…" for significant classes of transactions, account balances and disclosures, including "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 statement…"[17] In obtaining this required understanding, you would have obtained knowledge about the entity's information system, and therefore be able to identify journal entries, and the controls over those journal entries, whether the journal entries are standard or non-standard, or automated or manual. The identification of the journal entries and their related controls is therefore a judgment based on the nature and circumstances of the entity, including its information system.

The focus of paragraph 26(a)(ii) is on controls over journal entries that address a risk(s) of material misstatement at the assertion level, and that could be susceptible to unauthorized or inappropriate intervention or manipulation.

16 Paragraph 26(a)(ii) in ISA 315 (Revised 2019) relates to the *controls over journal entries* which are required to be understood as part of understanding the entity's system of internal control. Paragraph 26(a)(ii) in ISA 315 (Revised 2019) addresses both fraud and error and focuses on the controls over journal entries that address risks of material misstatement at the assertion level. Paragraph 33(a) in ISA 240 requires the auditor to test the appropriateness of journal entries and is specifically focused on the risks of material misstatement due to fraud. The ISA 240 requirement is targeted at *testing journal entries* and is responsive to the risk of management override of controls.

17 ISA 315, paragraph 25(a)(i)

These controls include:

- Controls over non-standard journal entries – whether the journal entries are automated or manual that are used to record non-recurring, unusual transactions or adjustments.
- Controls over standard journal entries – where the journal entries are automated or manual and are susceptible to unauthorized or inappropriate intervention or manipulation. In the case of journal entries that are automated, this could arise because of, for example, individuals without the appropriate authority have access to the source code or being able to make inappropriate changes to configurations (i.e., the journal entry, although automated, could be subject to manipulation). Conversely, controls over standard journal entries that are automated, such as controls over system-generated journal entries that are directly and routinely processed to the general ledger, would not warrant the focus of paragraph 26(a)(ii), where there is judged to be little or no susceptibility to unauthorized or inappropriate intervention or manipulation and therefore do not give rise to a risk of material misstatement at the assertion level.

Your inherent risk (IR) assessments are made without consideration of the entity's controls. This helps avoid, for example, making inappropriately lower risk assessments based on assumptions or inadvertent reliance that controls are operating effectively, without having evaluated the design and tested the operating effectiveness of those controls.

N3 - Which general IT controls (GITC) are required to be identified in relation to the controls over journal entries for the purpose of D&I (i.e., determining whether a control has been effectively designed and implemented)? For example, is a GITC required to be identified for each control over journal entries identified in Paragraph 26(a)(ii) in ISA 315 (Revised 2019), and D&I performed for that GITC?

Paragraph 26 (a)(i)-(iv) of ISA 315 (Revised 2019) requires specific controls to be identified that are subject to D&I, including controls over journal entries (see **N2** for the scope of the journal entries and controls subject to this requirement). If any of these 'identified controls' (i.e., controls subject to paragraph 26(a)(i)-(iv)) involve the use of IT or rely on IT, you are required (under paragraph 26(b)) to identify the related IT application, and any other aspects of the IT environment that may be subject to risks from the use of IT.[18] You are then required to identify the related risks arising from the use of IT and the GITCs addressing such risks, and then perform D&I over those GITCs.

Return to **Figure 1**.

When identifying the GITCs that will be subject to D&I, supporting application material explains that identifying risks arising from the use of IT relates only to the identified IT applications, or other aspects of the IT environment, for the controls in the control activities component (as identified in paragraph 26(b) in ISA 315 (Revised 2019)).

Not every control over a system-generated journal entry that has been identified in paragraph 26(a)(ii) of ISA 315 (Revised 2019) has to have a related GITC for which D&I is required. But rather, GITCs are considered in terms of how they relate to the relevant risks arising from the use of IT for the IT applications, or other aspects of the IT environment, for the identified controls in paragraph 26(a)(i)-(iv) in ISA 315 (Revised 2019). The identification of those GITCs subject to D&I is a judgment based on the nature and circumstances of the entity, including its information systems.

18 *Risks arising from use of IT* is a defined term in paragraph 12(i) of ISA 315 (Revised 2019).

Example 1

The LCE has different layers of IT used in their IT environment, from the IT applications themselves to the IT infrastructure that supports those applications such as the network, operating system, databases and their related hardware and software. The LCE may have set up their systems so that each employee must enter a password to access their operating system (network layer access) which then accesses all the entity's IT applications (application layer access). The auditor identified the control to set up passwords to log into the individual operating systems (network layer control) as a GITC that has a risk arising from the use of IT, instead of the controls to set up passwords to each individual application the entity uses (application layer control).

N4 – Why do you need to separately assess inherent risk for risks of material misstatement at the assertion level? (ISA 315.31 and .34)

A separate assessment of inherent risk enhances the quality of your risk assessment process and will therefore help focus the auditor's efforts when responding to the assessed risk appropriately. In designing your procedures in response to the assessed risks of material misstatement, you are required to consider the reasons for the assessment of the risk of material misstatement (RoMM) at the assertion level, including inherent risk and control risk, and design and perform procedures as appropriate.

Return to **Figure 1**.

Your inherent risk (IR) assessments are made without consideration of the entity's controls. This helps avoid, for example, making inappropriately lower risk assessments based on assumptions or inadvertent reliance that controls are operating effectively, without having evaluated the design and tested the operating effectiveness of those controls.

While you are always required to assess inherent risk for identified risks of material misstatement at the assertion level, you are required to assess control risk (CR) only if you plan to test the operating effectiveness of controls or when substantive procedures alone do not provide sufficient appropriate audit evidence at assertion level. If you do not plan to test the operating effectiveness of controls, your assessment of control risk is such that the assessment of the risk of material misstatement is the same as your assessment of inherent risk.

Although making separate assessments of inherent risk and control risk is a new requirement (it can no longer be done simultaneously) in ISA 315 (Revised 2019), many auditors have already been doing separate assessments of inherent risk and control risk. With that said, if your firm's audit methodology under extant ISA 315 (Revised) had the assessments done simultaneously, this change will apply to you.

Aspects of the process for assessing inherent risks are discussed in question N5.

N5 – Why are "inherent risk factors," "likelihood and magnitude of misstatement" and "spectrum of inherent risk" important in making a separate assessment of inherent risk? (ISA 315.19(c)and .31-.32)

These concepts help provide you with more focus and quality in your risk assessment process. As a result, your response to the identified and assessed risks are also more focused on the identified and assessed risks, contributing to a quality audit.

Return to **Figure 1**.

Inherent risk factors, which is new in ISA 315 (Revised 2019)) are 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. Inherent risk factors include complexity, subjectivity, change, uncertainty, or susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk.[19]

You are required[20] to take the inherent risk factors into account when obtaining an understanding of the entity and its environment and the AFRF and use them to help identify where there may be risks of material misstatement. You then are required[21] to take into account how, and the degree to which, the inherent risk factors affect the susceptibility of relevant assertions to misstatement when assessing inherent risk for the identified risks of material misstatement (i.e., use them to help determine whether an identified risk is on the spectrum of inherent risk).

You are not required to document how every inherent risk factor was taken into account in relation to each class of transaction, account balance or disclosure. However, audit documentation needs to be sufficient to enable an experienced auditor, having no previous connection with the audit, to understand significant matters arising during the audit, the conclusions reached thereon, and significant professional judgments made in reaching those conclusions.[22] In "taking a matter into account," the auditor consciously thinks about something when judging a situation. This means when obtaining the required understanding, the auditor is actively thinking about how the inherent risk factors may influence the entity's financial reporting but only taking action when the inherent risk factor is applicable. This is an iterative process.

For each identified risks of *material* misstatement at the assertion level, you:

- Assess inherent risk by assessing the likelihood and magnitude of misstatement, taking into account how, and the degree to which, those inherent risk factors affect the susceptibility of those relevant assertions to misstatement.
- Take into account how, and the degree to which, the risks of material misstatement at the financial statement level affect the assessment of inherent risk.
- Determine whether the assessed risks of material misstatement are significant risks (i.e., those risks that are close to the upper end of the spectrum of inherent risk).

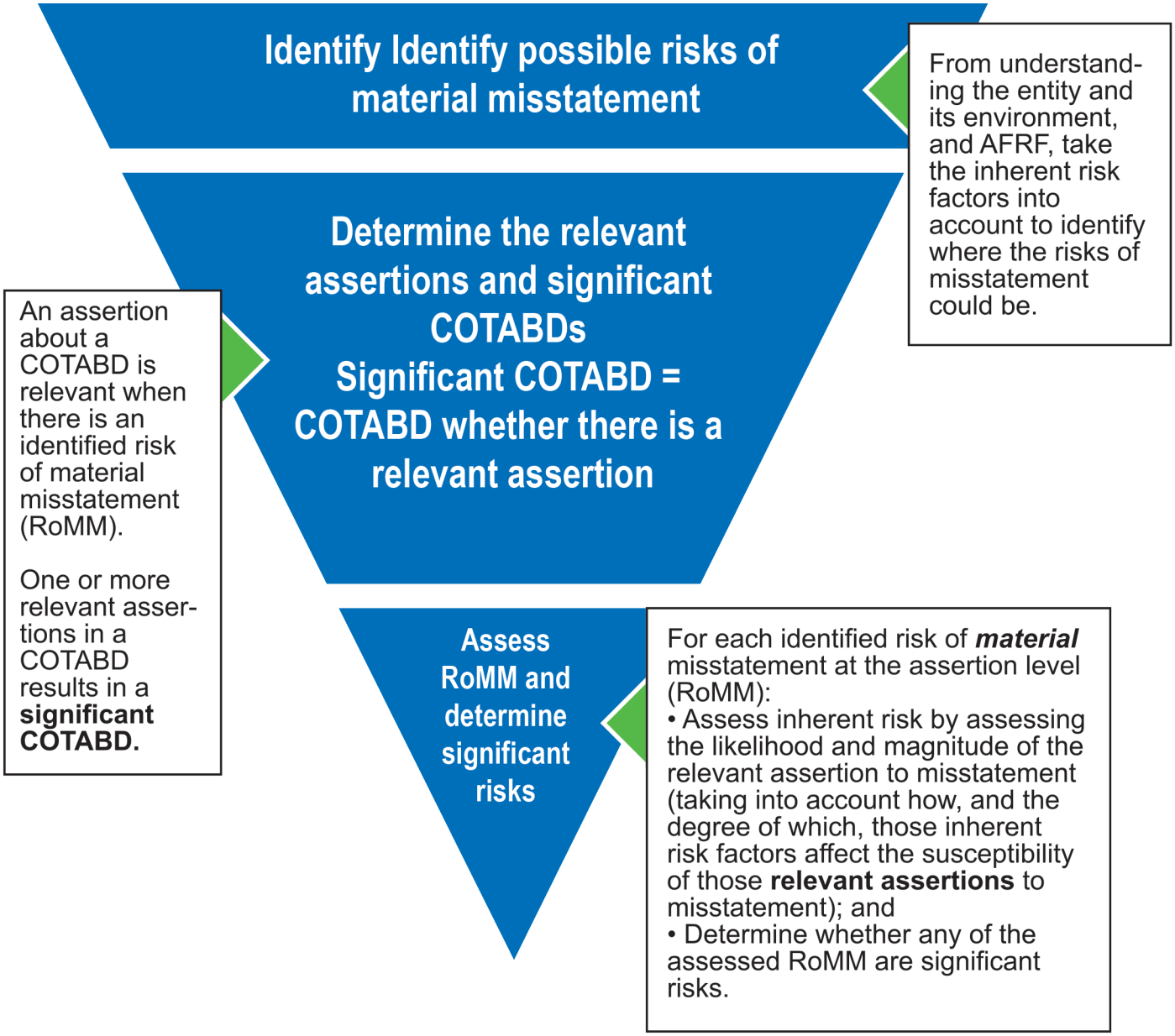
19 Appendix 2 of ISA 315 (Revised 2019) provides descriptions of inherent risk factors and matters to consider in understanding and applying them.

20 ISA 315.19(c).

21 ISA 315.31(a).

22 ISA 230, *Audit Documentation*, paragraph 8(c).

FIGURE 2 – IDENTIFYING AND ASSESSING RISKS OF MATERIAL MISSTATEMENT AT THE ASSERTION LEVEL



* COTABD: Classes of transactions, account balances and disclosures.

The Spectrum of Inherent Risk

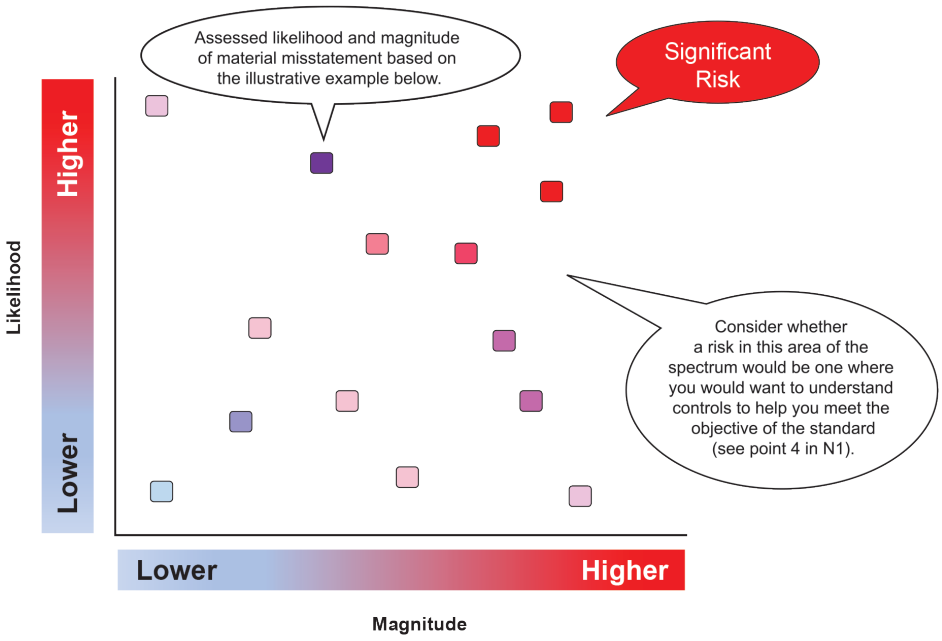
The degree to which inherent risk varies on a spectrum is referred to as the spectrum of inherent risk. Figure 3 shows an example of how the spectrum of inherent risk may be viewed.

For each identified risk of material misstatement at the assertion level, you are required to assess the likelihood and magnitude of material misstatement. It is the combination of likelihood and magnitude that will determine where inherent risk is assessed on the spectrum of inherent risk.

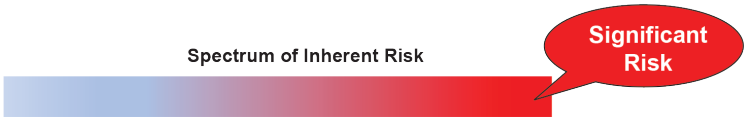
Your consideration of the likelihood takes into account the possibility that a misstatement may occur, based on consideration of how the inherent risk factors affect the risk of material misstatement (for example the greater the complexity is, the higher on the spectrum of inherent risk the identified ROMM will likely be).

Your consideration of the magnitude of a misstatement takes into account both the qualitative and quantitative aspects of the possible misstatement. For example, determining whether a risk of misstatement related to classification is material may involve the evaluation of qualitative considerations, such as the effect of small classification misstatement on the LCE's compliance with debt or other contractual covenants. A debt covenant may include a requirement for the LCE to maintain, at least, a minimum specified amount of working capital. A small misstatement affecting working capital could have significant ramifications for the LCE if the correction of the misstatement results in working capital being less than the minimum specified in the debt covenant. Therefore, the risk of material misstatement related to classification may exist, even if the amount of misstatement is of lower quantitative magnitude.

FIGURE 3: EXAMPLE OF ASSESSING LIKELIHOOD AND MAGNITUDE OF MISSTATEMENT IN DETERMINING WHERE INHERENT RISK IS ASSESSED ON THE SPECTRUM OF INHERENT RISK



☐ Each square represents a different inherent risk assessment for an identified risk of material misstatement. It indicates a combination of the assessed magnitude and likelihood of misstatement used to assess that inherent risk, taking into account the inherent risk factors. Each combination is used to determine where on the spectrum of inherent risk an identified risk of material misstatement is assessed:



In assessing inherent risk, you exercise professional judgment to determine the significance of the combination of the likelihood and magnitude of a misstatement.[23] The judgment about where in the range inherent risk is assessed may vary based on the nature, size and complexity of the entity and takes into account the assessed likelihood and magnitude of the misstatement and inherent risk factors.

Illustrative example of how matters referred to in Figures 2 and 3 may be applied

(This example is illustrative in nature and includes only certain facts and circumstances to demonstrate the application of certain requirements in ISA 315 (Revised 2019).)

An LCE's major asset is its real estate property of vacant land, which is being held for future development and eventual sale. The LCE prepares financial statements in accordance with a financial reporting framework that uses a cost model to account for acquisition, construction or development over time of real estate property. The financial reporting framework requires the entity to test for recoverability whenever events or changes in circumstances indicate that the carrying amount may not be recoverable. An impairment loss is recognized when the carrying amount is not recoverable and the carrying value exceeds fair value.

The LCE holds most vacant land in its holdings in geologically stable regions. However, some of its real estate property (approximately 10 per cent) is on shorelines and hillsides where erosion may occur. There have been some significant events resulting from climate change in some regions over the past years in those shoreline and hillside regions. In addition, some municipalities/regions are looking at re-zoning some shoreline and hillside areas. The LCE has determined that there are events or changes in circumstances indicating that the real estate property carrying amount may not be recoverable.

Susceptibility of assertions to misstatement

The auditor identifies the valuation assertion related to real estate property as having a susceptibility to material misstatement. This could impact the carrying value of the vacant land recorded on the balance sheet and the impairment loss recorded on the income statement and the related disclosures.

Identifying risks of material misstatement and relevant assertions

Given that the vacant land is the major asset of the LCE and the various events and conditions that indicate possible change to the recoverable amount of the real estate property, the auditor identifies a risk of material misstatement related to estimating the recoverable amount and, when applicable, the fair value.

Therefore, the auditor identifies the valuation assertion related to real estate property as being a relevant assertion, given there is a risk of material misstatement related to it.

The auditor identifies the carrying value of the vacant land recorded on the balance sheet and the impairment loss recorded on the income statement and the related disclosures as significant classes of transactions, account balances and disclosures because they contain relevant assertions.

Assessing risks of material misstatement – inherent risk

For the risk of material misstatement related to estimating the recoverable amount and, when applicable, the fair value, the auditor assesses the inherent risk by assessing the likelihood and magnitude taking into account how the inherent risk factors affect susceptibility of the valuation assertion to misstatement and the degree to which it does.

23 ISA 315.A208.

Because of the change driving further consideration of the recoverable amount, the inherent risk factors that primarily affect the susceptibility of the valuation assertion to misstatement (which the auditor determined for this particular example) are complexity (of the calculation of fair value (or recoverable amount), subjectivity (of the inputs into the calculation of the fair value (or recoverable amount) and uncertainty (as to what may happen in the future with regard to the value of the asset an its recoverable amount).

Given the changes in events and conditions, the auditor determines that there is a higher degree of complexity, subjectivity and uncertainty.

Although the likelihood of a material misstatement may be higher (given the complexity, subjectivity and uncertainty), the magnitude of the potential misstatement may not be as material, given that only 10 percent of the real estate property may be subject to risk. Accordingly, the risk of material misstatement is assessed as higher on the spectrum of inherent risk but not a significant risk.

Assessing risks of material misstatement – significant risk (change in case facts)

If the case facts above were different — for example, if the real estate property on shorelines and hillsides where erosion may occur made up 75 per cent of the entity's vacant land holdings (instead of approximately 10 per cent as outlined above) — the magnitude of the potential misstatement might be more material. The assessment of likelihood of misstatement has not changed; therefore, the auditor determines the risk of material misstatement related to estimating the recoverable amount and, when applicable, fair value (i.e., valuation is a relevant assertion, and the carrying value of property and impairment loss are significant COTABDs) as being close to the upper end of the spectrum of inherent risk (i.e., see "Significant Risk" highlighted in **Figure 3**).

N6 – Why do you need to perform a risk assessment stand-back, and how does it relate to the requirement to perform substantive procedures for each material class of transactions, account balances and disclosures in ISA 330.18? (ISA 315.36, ISA 315.37)

Risk assessment is an iterative process. A risk assessment stand-back is intended to drive an evaluation of the completeness of the identified risks of material misstatement. The stand-back is focused on whether there is anything in the auditor's understanding that may indicate that there may be further risks of material misstatement that have not been identified in the procedures already performed.

In addition, if new information comes to light during the course of the audit, which (1) may change the identified risks of material misstatement because this information is inconsistent with the audit evidence on which you originally base your identification, or (2) may cause the identification of a new risk of material misstatement, you are also required to reconsider the original risk assessments made and the planned responses to those risks.

This could have significant implications for the nature, timing, and extent of procedures you perform in responding to the identified risks of material misstatement.

When performing the risk assessment stand-back, you may find one or more material classes of transactions, account balances or disclosures for which you had not determined to be significant because you had not identified any risks of material misstatement related to the assertions in those classes of transactions, account balances or disclosures. Such material classes of transactions, account balances or disclosures should be reconsidered to confirm that there are no risks of material misstatement. Even if no further risks of material misstatement are identified, ISA 330 (paragraph 18) still requires substantive procedures on these material classes of transactions, account balances or disclosures.

Return to **Figure 1**.

Questions to ask when performing a stand-back

Questions you may consider asking yourself in evaluating whether your original determination remains appropriate include, for example, whether there have been any new information relating to:

- Aspects of the entity and its environment (e.g., business acquisition that changes the organizational structure, change in business model such as a launch of a new product, new regulatory requirements, changes in the industry)
- The entity's accounting policies (e.g., changing inventory costing method from average costing to first-in, first-out)
- How and the degree to which the inherent risk factors affect susceptibility to misstatement (e.g., more use of complex spreadsheets to develop a provision or higher uncertainty related to the outcome of an event)
- Internal control components (e.g., loss of key management employees, or new software module implemented)

If new information is obtained which is inconsistent with the audit evidence on which you originally based the identification or assessments of the risks of material misstatement, consider whether you need to revise materiality. If you revise materiality, this may also impact your identification of risks of material misstatement.

However, it has been clarified that not all assertions within a material class of transactions, account balance or disclosure are required to be tested. Rather, in designing the substantive procedures to be performed, you consider the assertion(s) in which, if a misstatement were to occur, there is a reasonable possibility of the misstatement being material. This may assist you in identifying the appropriate nature, timing and extent of the procedures to be performed. For example, the LCE may have a land and buildings held at cost, with no indication of impairment, for which you did not identify a risk of material misstatement. In performing substantive procedures on this balance, you may decide to design the procedures to test the existence assertion.

Explanations of Certain Other Requirements

O1 – Why are you required to perform analytical procedures when identifying and assessing risks of material misstatement? (ISA 315.14b)

Analytical procedures:

- Help identify inconsistencies, unusual transactions or events, and amounts, ratios, and trends that may assist you in identifying risks of material misstatement, especially risks of material misstatement due to fraud
- Help identify aspects of the entity of which you were unaware that assist in identifying the risks of material misstatement
- Help understand how inherent risk factors, such as change, affect susceptibility of assertions to misstatement, which may assist the auditor in assessing the risks of material misstatement

Return to **Figure 1**.

Analytical procedures used as risk assessment procedures do not need to be performed in accordance with the requirements in ISA 520, *Analytical Procedures*[24] which deals with analytical procedures used as substantive procedures and those performed near the end of the audit. However, the requirements and application material in ISA 520 may provide useful guidance when performing analytical procedures as part of the risk assessment procedures. Analytical procedures may be simple comparisons of information, such as comparing current year balances to balances in the prior period.[25] However, the types of analytical procedures used previously may not necessarily be effective in identifying and assessing risks of material misstatement in the current year. Based on the knowledge obtained when understanding the entity and its environment, the AFRF and the entity's system of internal control, you may create expectations of how you believe balances should have moved. For example, new significant transactions, events or conditions affecting the entity's business or financial reporting may have arisen in the current year for which you would expect to see changes, or not, year on year. Consider asking yourself, for example, the extent to which a class of transaction, account balance or disclosure should have changed from a prior period, taking into account your updated understanding.

When practicable, you may want to consider waiting to perform analytical procedures as risk assessment procedures until the accounting has been completed such that the information is no longer preliminary. For example, when the LCE has performed its period-end procedures and developed various estimates (e.g., depreciation, allowance for doubtful accounts, etc.).

However, even preliminary information can help corroborate or contradict outcomes of inquiries about results of operations / financial performance and financial position. Analytical procedures based on preliminary information are more likely to result in meaningful comparisons when the information for the current year is at roughly the same stage of completion as the information used in the prior period.

24 ISA 520, *Analytical Procedures*.

25 ISA 315.A29.

O2 – Why do you need to use a combination of inquiry, observation and inspection in performing risk assessment procedures, including when obtaining evidence about the design and implementation of identified controls in the control activities component?
(ISA 315.13, .14, .19(a)-(b), .21-.26 and .A177)

Observation and inspection may corroborate or contradict responses to inquiries of management and others regarding your understanding of the entity and its environment, the AFRF used and the entity's system of internal control, including the control activities component. This combination assists in obtaining audit evidence that provides an appropriate basis for the identification and assessment of risks of material misstatement.

How management has designed and implemented controls in the control activities component provides a preliminary understanding of how the entity identifies business risks and how it responds to them. It may also influence the auditor's identification and assessment of the risks of material misstatement in different ways and provide a basis for your design and performance of substantive procedures. The implementation of a control is determined by establishing that the control exists, and that the entity is using it as it was designed. However, inquiry alone to obtain audit evidence about the design and implementation of identified controls in the control activities component is not sufficient.

(See question **N5** for controls specified in ISA 315.26 for which you are required to evaluate design and determine implementation.)

Return to **Figure 1**.

Risk Assessment Procedures (Inquiry, Observation and Inspection)

Although you are required[26] to perform all the types of risk assessment procedures (inquiries of management and other appropriate individuals within the entity, analytical procedures, observation and inspection) in obtaining the required understanding of the entity and its environment, the AFRF and the entity's system of internal control, you are not required to perform all of them for each aspect of that understanding. Other procedures may be performed as part of obtaining your understanding of the entity and may be helpful in identifying and assessing risks of material misstatement. Examples include making inquiries of others outside the entity, such as the entity's external legal counsel or external supervisors, or of valuation experts that the entity has used.

Understanding the Entity and its Environment

For example, the results of your inquiries may indicate that the entity has no new related parties. Inspection of the list of significant suppliers compared to the previous year may reveal one or more new significant suppliers. In obtaining an understanding, for example, of the nature, amounts, timing and extent of the transactions of the LCE with these new suppliers, you may identify unusual terms of trade with a supplier and other factors indicating it is a previously unidentified related party. As a result, you may assess the risk of material misstatement as higher than when you only considered the inquiries as a basis for your risk assessment.

26 ISA 315.14.

Understanding the Applicable Financial Reporting Framework

For example, the results of your inquiries may indicate that the entity continues to have the same terms of trade (e.g., FOB shipping point) with their new U.S. customers. When inspecting certain master agreements with these new U.S. customers, you note that the majority of the terms of trade are FOB shipping destination. As a result, you may identify a risk of material misstatement related to occurrence or cut-off of revenue, or you may assess the inherent risk higher than when you only considered the inquiries as a basis for your risk assessment.

Understanding the System of Internal Control, Including the Control Activities Component

For example, in response to your inquiries, the owner-manager may state that nothing has changed with respect to the nature and extent of the processes and procedures used to help ensure accurate and complete financial reporting. However, observations and inspection of reports may indicate that the reports from the entity's IT system have not been accessed and reviewed by the owner-manager when in fact the owner-manager stated they review such reports on a monthly basis. A follow-up conversation with the owner-manager may corroborate the issues found in your observations. As a result, you may assess the risk of material misstatement as higher than when you only considered the inquiries as a basis for your risk assessment.

Design and Implementation of Controls

Evaluating the design of an identified control involves your consideration of whether the control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting, material misstatements. The implementation of a control is determined by establishing that the control exists, and that the entity is using it. This cannot be done through inquiry alone. Additional procedures such as observing the application of the control while it is being performed or inspecting documents and reports may corroborate the inquiry about how the control is implemented, or it may provide you with new information that could impact your risk assessment and related response.

For example, the owner-manager may use certain IT-generated reports in performing a control that address a significant risk. You may make inquiries to obtain an understanding of how these reports are generated and the nature, timing and extent of their use. However, it may be only by observing the process for the generation and use of these reports that you are able to identify that the control owner is generating or using the report in a different way compared to what was explained to you. As a result, you may adjust your identification of possible risks of material misstatement, or design more or different procedures regarding how these reports are used in obtaining audit evidence and consider whether this constitutes a deficiency in accordance with ISA 265.

Entity policies and procedures (and controls) 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 conditioned by the entity's culture. Audit evidence about elements of the control environment in LCEs 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. You may consider observing the application of specific controls and speaking with more than one person at the entity to corroborate initial inquiries.

O3 – Why are you required to obtain an understanding of each of the five components of internal control even when your approach to the audit is primarily substantive?
(ISA 315.21-.27)

You need to obtain this understanding to be able to identify and assess risks of material misstatement at the financial statement level and assertion level. Without such understanding, you may, for example, fail to

- Identify a risk of material misstatement,
- Appropriately assess the identified risk of material misstatement, or
- Appropriately respond to an identified risk when designing and performing your further audit procedures.

Return to **Figure 1**.

(Note: To view the requirements of ISA 315 (Revised 2019) related to obtaining an understanding of the entity's system of internal control in flowchart format, refer to **Appendix A** of this *Tool*.)

ISA 315 (Revised 2019) provides information on "how" to obtain an understanding of the five components of internal control. You obtain an understanding by:

- Understanding specific elements within a component of internal control; and
- Evaluating whether the controls in that component of internal control are appropriate to the nature and circumstances of the entity.

Based on the results of the evaluation of the appropriateness of the controls for that entity (i.e., your evaluation of each of the components of the entity's system of internal control), you are required to determine whether one or more control deficiencies have been identified. If you have identified one or more control deficiencies, you may consider the effect of those control deficiencies on the design of further audit procedures in accordance with ISA 330.

ISA 315 (Revised 2019) recognizes that the way in which the entity's system of internal control is designed, implemented and maintained varies with an entity's size and complexity. For example, LCEs may use less structured or simpler controls (i.e., policies and procedures) to achieve their objectives.[27] For LCE's, those simpler controls may be appropriate in the circumstances.

In addition to providing information on "how" to obtain an understanding of the five components of internal control, ISA 315 (Revised 2019) now also provides information on "why" you need to obtain an understanding of each component of the entity's system of internal control relevant to the preparation of financial statements in the application material.

Set out below is a brief overview of "why" you need to obtain an understanding of each of the components, discussed in the context of the audit of an LCE. Specific matters that may require clarification are noted with suggestions as to how they may be addressed.

Control Environment

You are required to obtain an understanding of the LCE's control environment because the control environment (for example tone at the top) can affect risks of material misstatement (including risks of fraud) at the financial statement level, which may also affect risks of material misstatement at the assertion level.

27 ISA 315.A92.

This is because the control environment provides an overall foundation for the operation of the other components of the system of internal control.[28] It may have a pervasive influence on the effectiveness of controls in the other components and on the preparation of the financial statements. For example, if the owner-manager of a business sets a tone at the top that stresses honesty and integrity, places a high priority on controls and expects compliance with established policies and procedures, this may help with effective functioning of the entity's controls to detect and correct any misstatements and therefore reduce the ability for risks of material misstatement. As another example, even an LCE's informal human resources policies (e.g., policies and procedures around hiring competent and experienced employees) are likely to be a key determinant in whether personnel have the characteristics needed to help ensure high-quality financial reporting. You would use this understanding as part of your evaluation of whether management 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.

Evidence regarding the quality of the control environment may be obtained through inquiry of the owner-manager about various aspects of how that role is performed (i.e., oversight responsibilities and culture) and observations throughout the audit regarding upper management's activities and interactions with other personnel. Also, through inquiry of other personnel, you may obtain varying perspectives on the quality of the control environment required to be understood. When evaluating the control environment, this information obtained when understanding the control environment is considered to help determine whether the control environment is appropriate to the nature and circumstances of the entity or whether a deficiency exists. Note that it is an evaluation of the control environment overall and how it supports the other components of the entity's system of internal control, and not a detailed evaluation of the specific controls within the control environment (where they exist).

The Entity's Risk Assessment Process

Like all entities, an LCE faces business risks. These risks result, for example, from significant conditions and events that could adversely affect whether the LCE is able to achieve its objectives. The owner-manager (and perhaps the board of directors) will have a process, likely informal, to identify, assess and address business risks. You obtain an understanding of this process to understand where the entity identifies its risks and whether the LCE has responded to those risks and evaluate whether their risk assessment process is appropriate in the circumstances, considering the nature and complexity of the LCE.

For example, if the LCE is a manufacturer, there is a risk of deterioration in product quality. If the LCE's management does not address this risk in any way, the effects on the financial statements may include, for example, inventory valuation issues, increased problems in collecting accounts affecting the allowance for doubtful accounts and a need to increase estimates related to warranties. Based on this understanding, in evaluating the entity's risk assessment process you may identify a control deficiency and may need to consider its impact on the audit.

Also, management's assessment of the LCE's business risks will impact its assessment of the entity's ability to continue as a going concern.

Even though evidence of their risk assessment may not be formally documented, inquiries of the owner-manager and other appropriate personnel will help you understand how, and how often, business risks are considered. When evaluating the entity's risk assessment process, consideration is given to whether what the entity has is appropriate to the nature and circumstances of the entity or whether a deficiency exists (for example, for smaller, less complex entities in some cases it may be appropriate that there is not formalized risk assessment process).

28 ISA 315.A97.

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

You obtain an understanding of this component, which includes if, how and when monitoring is undertaken, because the entity's monitoring will affect, for example, whether misstatements (material or not) are prevented or detected.

An LCE may not have a formal process for monitoring its system of internal control. However, risks of inaccurate financial reporting may be lower, for example, when the owner-manager is actively involved in monitoring aspects of operations such as collection of accounts, timely payment to suppliers and compliance with the provision of loan covenants. This may involve use by the owner-manager of reports generated from commercial software.

Obtaining an understanding of the monitoring process is likely to entail inquiries of the owner-manager or other personnel involved in that process. You may observe or inspect documentation that shows the nature and frequency of monitoring activities. This understanding will help you 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, or whether a deficiency exists (for example, the entity undertakes no monitoring but even in smaller, less complex entities some kind of monitoring would be expected as a deficiency may exist).

The Information System and Communication

(Note: To view the requirements of ISA 315 (Revised 2019) related to the auditor's understanding of the IT environment and the Identification of GITCs in flowchart format, refer to **Appendix B** of this *Tool*. See question **O4** for a discussion of internal control matters to consider when the LCE uses commercial software.)

Information system relevant to the preparation of the financial statements

You obtain an understanding of the information system because misstatements may result from occurrences at any point in the flow of information relevant to financial reporting. Therefore, you may consider the following in obtaining that understanding:

- Policies in the information system regarding the nature of data or information relating to transactions
- Other events and conditions to be captured
- The information processing to maintain the integrity of that data or information
- The information processes, personnel and other resources used in the information processing.

This includes information not only from the general ledger and subsidiary ledgers, but also information from other sources, such as spreadsheets used to calculate revenue recognized or external to the entity (such as interest rates) where these are used in, for example, fair value calculations.

While information systems of LCEs may not be complex, risks of material misstatement may arise, for example, if personnel do not have the competencies or other resources needed to perform their duties or if there is inadequate segregation of duties. Based on this understanding, in evaluating the entity's information system you may identify a control deficiency and may need to consider its impact on the audit.

In an LCE, there may not be policies and procedures manuals or formal documentation of the information system (although this is good practice even in small organizations). Again, inquiry and observation (for example by performing a walk-through) of how the various relevant processes are performed may provide you with an understanding of the information system. This would include consideration of the entity's IT environment (e.g., how it is using commercial software to process its information).

Auditors may sometimes confuse the information system component of internal control with the control activities component. As described below under "control activities," these components are different (but interrelated), and making the distinction between them is important. The controls in the control activities component are identified from the work done in understanding the entity's information system.

Communications relevant to the preparation of the financial statements

You obtain an understanding of communications because they can affect, for example, the accuracy and completeness of financial reporting.

Communications in an LCE may be informal. Nevertheless, the risk of inaccurate financial reporting may be lower, for example, if there is clear and timely communication of matters related to financial reporting, including roles and responsibilities. Communications by the owner-manager to relevant personnel about business decisions, such as changing policies on extending credit to customers, may also have a bearing on accurate accounting. As another example, the owner-manager may be aware of side agreements with customers or suppliers but has not communicated this information to accounting personnel. This may lead to inaccurate booking of accruals.

In addition, timely communications from other personnel to the owner-manager about accounting problems identified, or changes in circumstances that affect their ability to fulfill their responsibilities, may also help lower the risk of inaccurate financial reporting.

Inquiries about and observation of communication processes, and review of relevant documentation, if available, may provide you with an understanding of the communications process. This understanding will help you evaluate whether the entity's communication appropriately supports the preparation of the entity's financial statements in accordance with the AFRF.

Control Activities

You obtain an understanding of the control activities component because controls in the control activities component are designed to ensure the proper application of policies (which are controls) in all the other components of the entity's system of internal control.[29] Controls in the controls activities component may therefore be particularly important in addressing risks of material misstatement.

Distinction between the information systems component and the control activities component

The requirements around the information systems component are meant to give you a base on which to understand how information flows through the information system, the accounting records, the financial reporting process used to prepare the financial statements and disclosures, and the entity's resources, including the IT environment. The control activities component includes controls such as authorizations and approvals, reconciliations, verifications, physical or logical controls (including controls over access to computer programs and data files), and segregation of duties. For the control activities component, you are required to evaluate the design and determine the implementation of the specific controls identified that meet the requirements. This requirement applies even when your procedures to respond to assessed risk are primarily substantive. You are not required to evaluate the design and determine the implementation of all controls in the information systems and communications component, but you are required to evaluate whether the entity's information system and communication appropriately supports the preparation of the financial statements (see question **N1**).

29 ISA 315.A147.

O4 – How may your approach to identifying, evaluating the design and determining the implementation of General IT Controls (GITCs) take into account that an LCE uses non-complex commercial software for accounting and financial reporting?
(ISA 315.26(b)-(c); A170; Appendix 5 and Appendix 6)

When an LCE uses non-complex commercial software, your risk assessment procedures regarding GITCs may require less effort than for the audit of an entity with a sophisticated IT environment. Procedures regarding design and implementation of GITCs may focus on managing access to the system versus change management controls or IT operational controls.

(See question **N5** — GITCs are among the controls in the control activities component specified in ISA 315.26.)

Return to **Figure 1**.

Broadly, the following aspects of IT are required to be understood for the purposes of understanding the information system:

- The IT environment relevant to the information system (newly defined (see new definition above)). Paragraphs A140–A141 in ISA 315 (Revised 2019) explains 'why' this understanding is required; and
- The entity's use of IT (i.e., IT applications relevant to the flows of transactions and processing of information in the information system). Paragraphs A142–A143 in ISA 315 (Revised 2019) explain further about the auditor's understanding of the use of IT when obtaining an understanding of the information system.

According to paragraph 26(b) of ISA 315 (Revised 2019), the auditor is only required to identify the IT applications and other aspects of the IT environment that are subject to risks arising from the use of IT. Some LCEs use an "off-the-shelf" commercial accounting package where the source code cannot be changed by the entity. Therefore, IT risks relevant to the preparation of the entity's financial statements will likely be very limited. It is also possible that the LCEs' GITCs may not be formalized.[30]

ISA 315 (Revised 2019) acknowledges that the extent of the auditor's understanding of the IT processes, including the extent to which the entity has GITCs in place, will vary with the nature and the circumstances of the entity and its IT environment. Also, ISA 315 (Revised 2019) contains much more extensive guidance on matters for you to consider in obtaining an understanding of an entity's IT environment and controls.

For instance, Appendix 5 provides examples of typical characteristics of IT environments based on the complexity of IT applications used in the entity's information system. This includes a table comparing the typical characteristics of:

- Non-complex commercial software
- Mid-size and moderately complex commercial software and IT applications
- Large or complex IT applications (e.g., ERP (enterprise resource planning) systems).

30 ISA 315.A241

Also, Appendix 6 in ISA 315 (Revised 2019) includes a table illustrating examples of GITCs to address risks arising from the use of IT for different IT applications for the three levels of complexity of commercial software. For example, you may identify some automated controls that relate to the LCE's single non-complex commercial software for financial reporting that contains standard reports generated by the software. The LCE has no ability to change the program, given the lack of source code. The IT infrastructure supporting the IT application relates to a single network, a single operating system, and a single database. The IT operations do not involve data backup, as manual backups are done by the finance team and there are no job-scheduling operations. As a result, you identify the processes related to access (and not to change or IT operations) as subject to risks arising from the use of IT. You identify the following risks arising from the use of IT and the GITCs to mitigate such risks:

IT process	Example risks arising from the use of IT	Example GITCs
Mangage Access	User-access privileges: Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.	Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles / roles, critical financial reporting transactions and segregation of duties.
		Access of terminated or transferred users is removed or modified in a timely manner.
		User access is periodically reviewed.
		Privileged-level access (e.g., configuration, data and security administrators) is authorized and appropriately restricted.
	System settings: Systems are not adequately configured or updated to restrict system access to properly authorized and appropriate users.	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout).

Even for an audit of an LCE, your evaluation of the entity's information system may include, for example, considering whether the entity has invested in an appropriate IT environment and necessary enhancements. You may also consider whether a sufficient number of appropriately skilled personnel have been employed when the entity uses commercial software (even where there is no or limited ability to make modifications).

Another consideration is that controls you identify may depend on system-generated reports. IT applications that produce those reports may be subject to risks arising from the use of IT. When taking a substantive approach to your audit, you may decide to directly test the inputs and outputs of the report-generation process. In that case, you may not identify the related IT applications as subject to risks arising from IT.[31] Therefore, the controls over these system-generated reports (part of the control activities component) may not require evaluation as part of your risk assessment process.

31 ISA 315.A169.

O5 – Can the nature and extent of your documentation take into account that the entity and its processes are less complex for the audit of an LCE? (ISA 315.38)

For audits of financial statements of LCEs, the form and extent of documentation may be simple and relatively brief. However, your documentation needs to be sufficient to enable an experienced auditor, having no previous connection to the audit, to understand, for example, the nature, timing and extent of risk assessment procedures you performed to comply with ISA 315 (Revised 2019), and the results of those procedures.

Return to **Figure 1**.

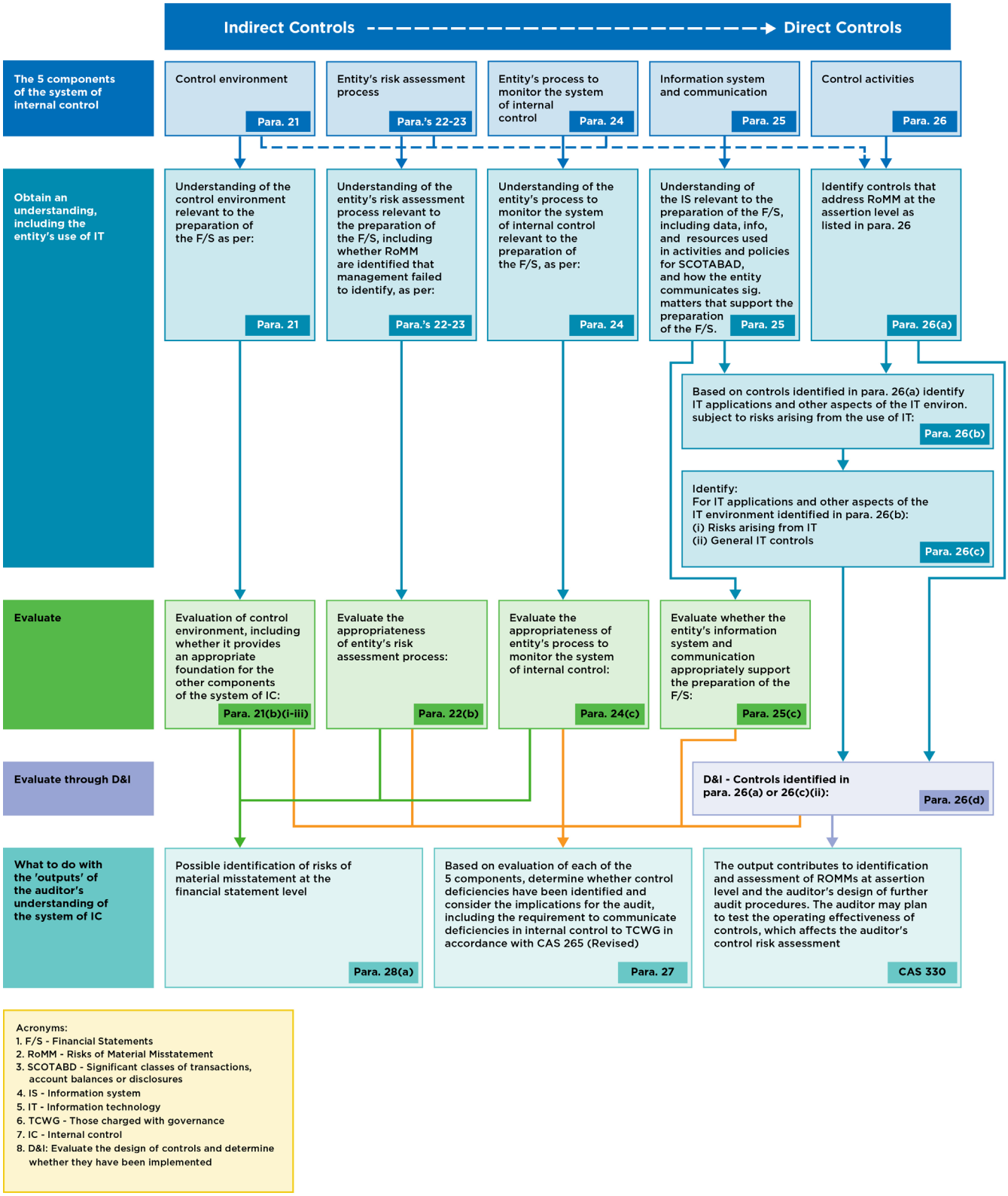
Some auditors have expressed a view that there is a lack of clarity regarding the nature and level of granularity of the documentation required for risk identification and assessments.

The extent of documentation is left to the auditor's judgment – these are principles-based standards. ISA 315 (Revised 2019) notes that your documentation is influenced, for example, by the nature, size and complexity of the entity and its system of internal control, availability of information from the entity, and the audit methodology and technology used in the course of the audit. It is not necessary to document the entirety of your understanding of the entity and matters related to it.[32] Key elements of understanding documented may include those on which you based the assessment of the risks of material misstatement. However, you are not required to document every inherent risk factor that you took into account in identifying and assessing the risks of material misstatement at the assertion level (as explained in question **N3**). In audits of LCEs, audit documentation may be incorporated in the auditor's documentation of the overall strategy and audit plan.

32 ISA 315.A241.

Appendix A

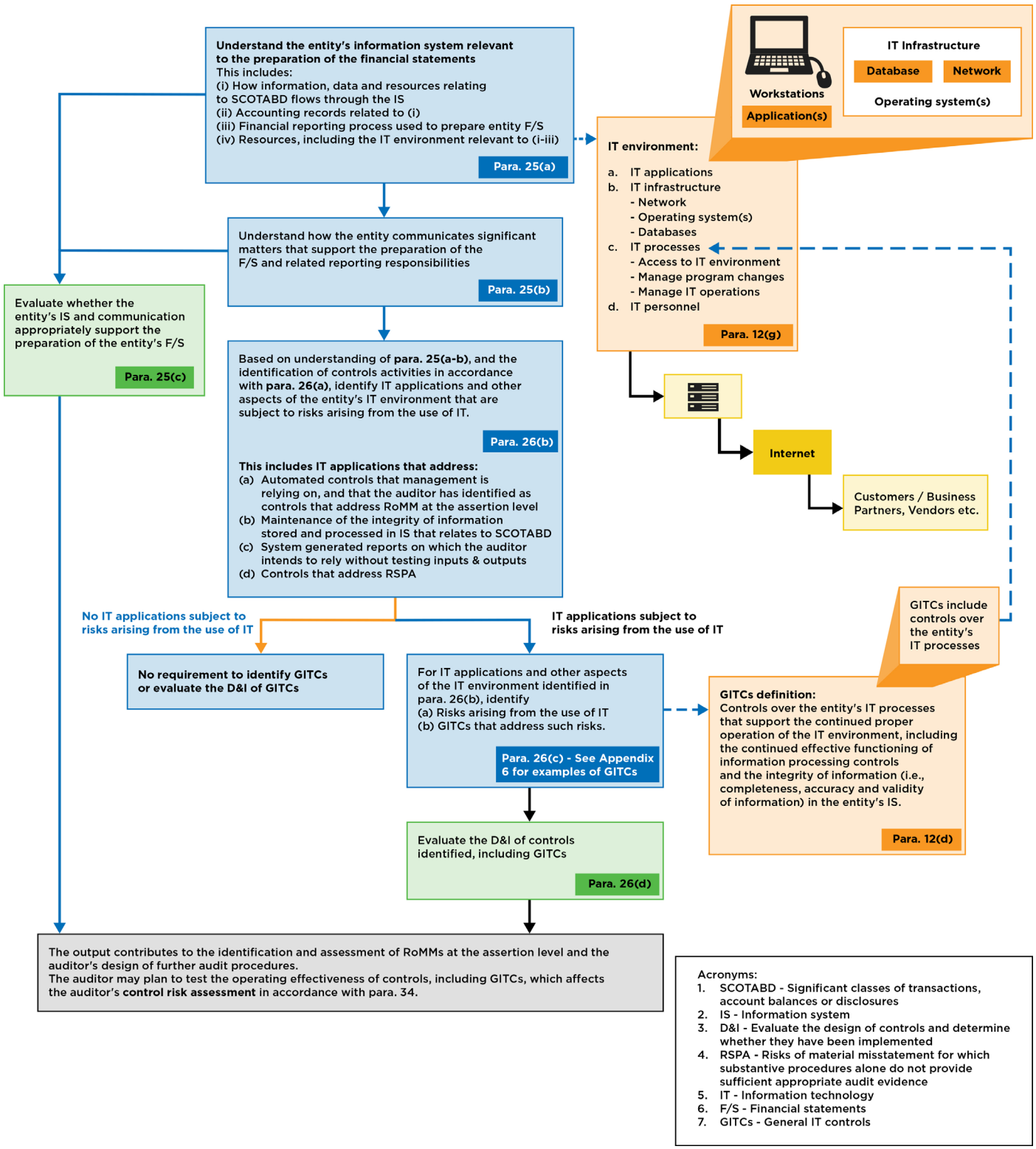
Understanding the Components of the Entity's System of Internal Control[33]



33 This figure is an extract from *Understanding of Internal Control Flowchart* of the International Auditing and Assurance Standards Board, published by the International Federation of Accountants in July 2018 - with updated paragraph numbers.

Appendix B

Understanding the Entity's Use of IT[34]



34 This figure is an extract from *Understanding of IT Environment Flowchart* of the International Auditing and Assurance Standards Board, published by the International Federation of Accountants in July 2018 - with updated paragraph numbers.

For further information, please email ChristopherArnold@ifac.org.

International Federation of Accountants®

529 Fifth Avenue, 6th Floor
New York, NY 10017
www.ifac.org