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

First-Time Implementation Guide

July 2022

IAASB
International Auditing and Assurance Standards Board

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

First-Time Implementation Guide

This First-Time Implementation Guide has been prepared by the Staff of the IAASB. The objective of this First-Time Implementation Guide is to help understand and apply the changes in International Standard on Auditing (ISA) 315 (Revised 2019).

The contents of this document focus on the more substantial changes made, however not every change is highlighted or addressed.

This publication does not amend or override ISA 315 (Revised 2019), the text of which alone is authoritative. Reading this publication is not a substitute for reading ISA 315 (Revised 2019). In conducting an audit in accordance with ISAs, auditors are required to comply with all the requirements that are relevant to the engagement – this publication does not address all requirements within ISA 315 (Revised 2019) but rather focuses on those requirements where there have been more substantial changes.

The revised standard and Basis for Conclusions (explaining the Board's rationale for the significant changes made) were published in December 2019.

What Does ISA 315 (Revised 2019) Address?

1. ISA 315 (Revised 2019), like ISA 315 (Revised), *Identifying and Assessment of Material Misstatement through Understanding the Entity and Its Environment*, covers the auditor's procedures to:

   (a) Understand the entity and its environment, the applicable financial reporting framework and the entity's system of internal control, to be able to identify and assess risks of material misstatement.

   (b) Identify risks of material misstatement; and

   (c) Assess risks of material misstatement.

See Fact Sheet: Introduction to ISA 315 (Revised 2019)

Why did ISA 315 (Revised) get changed?

2. The project to revise ISA 315 (Revised)[1] commenced in early 2016 to respond to key findings from the IAASB's ISA Implementation Monitoring Project.[2] The post-implementation review was completed in 2013, and key and significant findings in relation to ISA 315 (Revised) included that:

   - Inconsistency existed in the nature and number of significant risks identified in practice.
   - Obtaining an understanding of the system of internal control was difficult to apply in practice.
   - Information Technology (IT) risks were not sufficiently addressed in the standard.

   The post-implementation review also highlighted the challenges of applying ISA 315 (Revised) when auditing small- and medium-sized entities (SMEs).

---

1 ISA 315 (Revised), *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment*

2 *Clarified International Standards on Auditing–Findings from the Post-Implementation Review*

When is ISA 315 (Revised 2019) effective?

3. The previous version of ISA 315 (ISA 315 (Revised)) has been replaced by ISA 315 (Revised 2019) for periods beginning on or after December 15, 2021.

Have other related standards changed as a result of ISA 315 (Revised 2019)?

4. ISA 315 (Revised 2019) has been enhanced to form a stronger foundation for the audit, in particular better quality risk identification and assessment is expected to enhance the procedures required by other standards such as ISA 330[3] and ISA 540 (Revised).[4] Conforming and consequential amendments were also made to a number of other ISAs resulting from the changes made to ISA 315 (Revised), including ISA 330, ISA 240[5] and ISA 540 (Revised). These changes, where substantial (most were more conforming in nature), are highlighted throughout this first-time implementation guide where they are relevant.

5. ISA 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements* (effective for periods beginning on or after December 15, 2009) addresses the auditor's responsibilities with respect to risk identification and assessment in relation to fraud.[6] ISA 330 (effective for periods beginning on or after December 15, 2009) addresses the requirements for the auditor's responses to the assessed risks of material misstatement, at the overall and assertion levels. Except for conforming and consequential amendments made as part of the project to revise ISA 315 (Revised), the requirements of these standards remain the same.

What are the overarching audit concepts used in ISA 315 (Revised 2019)?

6. ISA 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*, deals with the overall objectives of the auditor in conducting an audit of financial statements. ISA 200 sets out the overall objectives of the auditor and explains the nature and scope of the audit. The broader, fundamental concepts for an audit, including the audit risk model, can be found in ISA 200.

What Has and Hasn't Changed – Overarching Audit Concepts in ISA 200

Concept	Unchanged	Changed
Obtaining evidence	Obtaining sufficient appropriate audit evidence to reduce audit risk to an acceptably low level.	-
Audit risk model	Audit risk is a function of the risks of material misstatement and detection risk.[7] The overall audit risk model has not changed.	-

[3] ISA 330, *The Auditor's Responses to Assessed Risks*

[4] ISA 540 (Revised), *Auditing Accounting Estimates and Related Disclosures*

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

[6] In 2022 the IAASB commenced a project to revise ISA 240 more comprehensively, including to focus on how the more robust risk identification and assessment procedures in ISA 315 (Revised 2019) can be built into that standard.

[7] ISA 200, paragraph 13(c)

Concept	Unchanged	Changed
Inherent risk, control risk, detection risk	The concepts of inherent risk, control risk and detection risk as described in ISA 200 have not changed.	• A separate assessment of inherent risk and control risk is now required. • The concept of the *spectrum of inherent risk* has been introduced to assist with the assessment of inherent risk. The spectrum of inherent risk assists the auditor in making a judgment, based on the likelihood and magnitude of a possible misstatement, on a range from lower to higher risk, for the purpose of assessing risks of material misstatement. Inherent risk factors have been introduced to help auditors consider risks of material misstatement on the spectrum of inherent risk.
Risk of material misstatement	The definition of the risk of material misstatement[8] has not changed: *The risk that the financial statements are materially misstated prior to the audit. This consists of two components, described as follows at the assertion level:* *(i) Inherent risk…* (ii) *Control risk…*	Although the definition of the risk of material misstatement has not changed, in the application material to ISA 200 the 'threshold' for the identification of a possible misstatement has been clarified and explained. By including this clarification in ISA 200 (rather than ISA 315 (Revised 2019)), it supports the definition of risk of material misstatement in ISA 200. The clarification explained in the application material to ISA 200 is that a risk of material misstatement exists where there is a *reasonable possibility* of both a misstatement occurring (i.e., its likelihood), and being material if it were to occur (i.e., its magnitude).(refer to the new paragraph A15a[9] in ISA 200 in the Conforming and Consequential Amendments) Based on this clarification in ISA 200, the term 'reasonably possible' is used within ISA 315 (Revised 2019) as it relates to the

[8] ISA 200, paragraph 13(n)

[9] This paragraph will be renumbered once the conforming and consequential amendments are included within each relevant ISA in the 2022 IAASB Handbook.

Concept	Unchanged	Changed
		threshold for identifying risks of material misstatement.
Professional skepticism	Auditors are required to exercise professional skepticism when designing and performing audit procedures.	There are enhanced procedures to encourage behavioral change for auditors when undertaking audit procedures, as well as strengthened documentation requirements (see section on Professional Skepticism later in this document). Where matters related to professional skepticism have been highlighted, they are indicated by the use of this symbol: 
Professional judgment	The auditor is also required to exercise professional judgment in planning and performing risk assessment procedures. This overall concept has not changed, but various enhancements have been made throughout to assist the auditor in making judgments.	-
Considerations specific to smaller entities	The concept of scalability (i.e. being able to apply the ISAs to entities of varying sizes and complexities) is inherent within the IAASB's standards, and the IAASB always focuses on what more can be done to assist with all entities being able to apply its standards. The IAASB has continued to distinguish the auditor's considerations in relation to scalability and proportionality within separate paragraphs within the revised standard (clearly headed as "Scalability" considerations).	• The revised standard focuses on complexity rather than size (i.e., 'less complex entities' rather than 'smaller entities' in line with the IAASB's approach to such entities). • Scalability has been illustrated through the use of contrasting examples throughout the standard (i.e., illustrating both ends of the complexity spectrum) rather than only focusing on 'smaller entities.'
Considerations specific to "public sector entities"	Considerations for public sector entities have been maintained.	These paragraphs have been updated where appropriate (i.e., to reflect unique public sector considerations).

Nature and Extent of Work to be Performed

7. ISA 315 (Revised 2019) clarifies that the nature and extent of risk assessment procedures required 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). It further explains that the auditor uses professional judgment to determine the nature and extent of the risk assessment procedures to be performed to meet the requirements of the standard.[10]

Iterative Nature of the Standard

8. 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 throughout the requirements to identify and assess the risks of material misstatement. In obtaining the understanding required by this ISA, the auditor may develop initial expectations of risks, which may be further refined as the auditor progresses through the risk identification and assessment process.

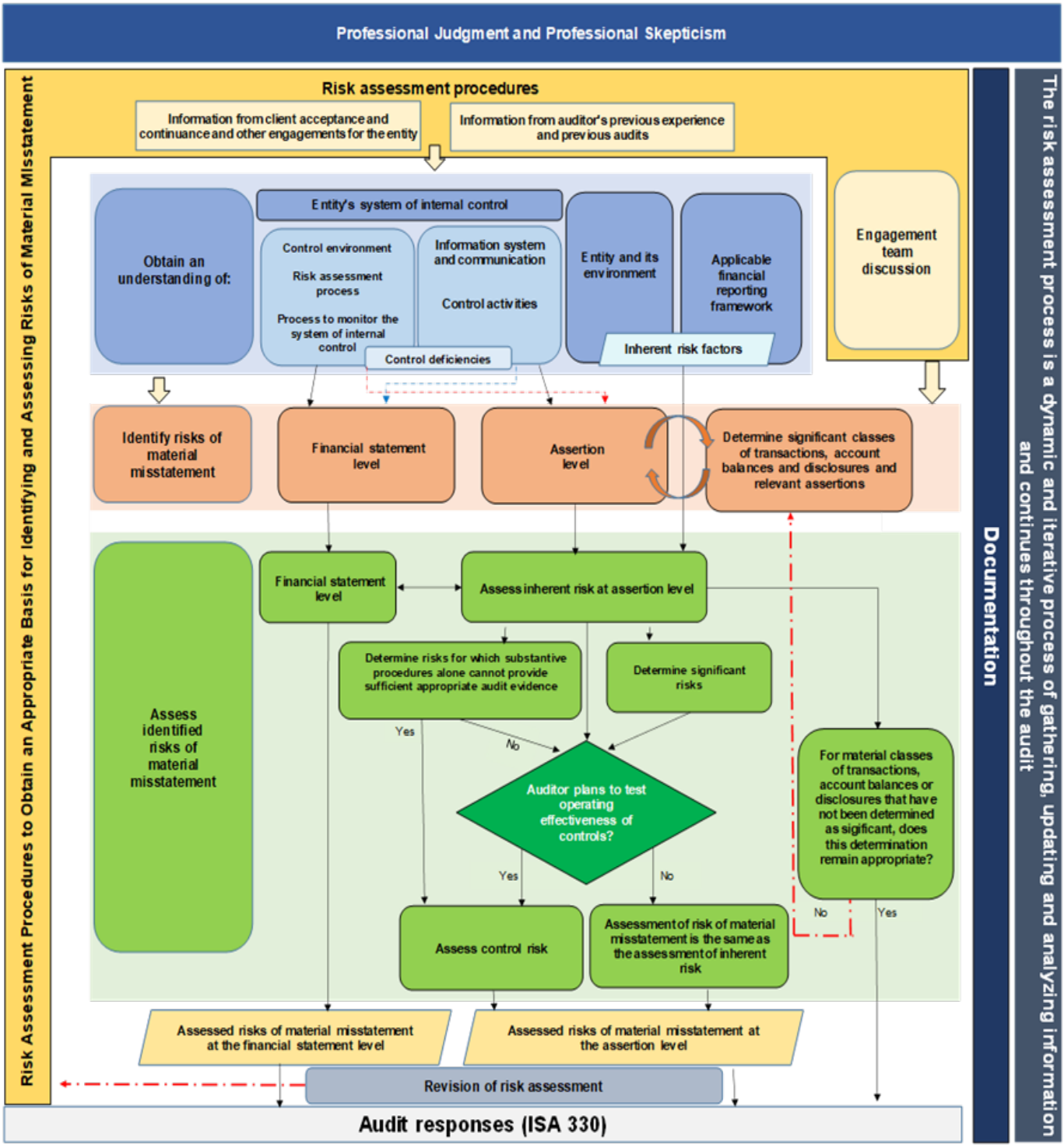
9. The flowchart that follows illustrates the iterative nature of the standard. In addition, where the execution of certain requirements that are presented earlier within the standard have dependencies upon the execution of other requirements presented later within the standard, application material has been added to make these connections. For example:

   - Paragraph A49 of ISA 315 (Revised 2019) explains that the auditor may develop initial expectations about the classes of transactions, account balances and disclosures that may be significant classes of transactions, account balances and disclosures. This in turn forms the basis for the scope of the auditor's work when understanding the information system (see paragraph 25 of ISA 315 (Revised 2019)).
   - Paragraph A127 of ISA 315 (Revised 2019) further notes that work performed on the information system (understanding and evaluation) may further influence the auditor's expectations about significant classes of transactions, account balances and disclosures.
   - Paragraph A128 of ISA 315 (Revised 2019) explains that understanding the flows of information in the information system may also assist in identifying those specific controls that are required to be further understood (i.e., in the 'control activities' component).
   - Paragraph A129 of ISA 315 (Revised 2019) further explains that some controls can only be identified once the possible risks of material misstatement have been assessed (e.g., after significant risks have been determined).

10. The following sets out an overview of ISA 315 (Revised 2019):

[10] ISA 315 (Revised 2019), paragraph A16

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



Explaining "Why" a Procedure is Required

11. ISA 315 (Revised 2019) has focused on explaining why certain procedures are required (these "why" paragraphs can be found within the application material).

12. These explanations are intended to address the rationale for certain requirements where there may have been misunderstanding, misapplication or inconsistent application of the requirements. The Board agreed that by including an explanation as to why these procedures need to be done, it would reduce the risk of inconsistent application of the related requirements. In particular, the "why's" have been added to explain why the understanding of the various components of the entity's system of internal control is required, particularly in circumstances where it is intended that a primarily substantive approach to the audit will be undertaken.

Automated Tools and Techniques (ATT)

13. ISA 315 (Revised 2019) focuses on obtaining audit evidence as *a basis for* the identification and assessment of risks of material misstatement.

14. The procedures for obtaining audit evidence as set out in ISA 500, *Audit Evidence*, i.e., inspection, observation, external confirmation, recalculation, reperformance, analytical procedures and inquiry, continue to apply, regardless of whether those procedures are performed manually or using technology. ISA 315 (Revised 2019) is not prescriptive as to *how* these procedures are performed. Instead, risk assessment procedures performed leveraging the use of technology have been described in the application material as automated tools and techniques (ATT) in recognition that ATT may not be available to all auditors in the same way.

15. Where relevant within the application material, specific considerations have been included for the use of ATT under the heading "automated tools and techniques."

See FAQ: *The Use of Automated Tools and Techniques in Identifying and Assessing the Risks of Material Misstatements*, which sets out questions and answers related to using ATT in the identification and assessment of ROMMs

Appendices

16. Appendices have the same authority as the application and other explanatory material (i.e., they form part of the standard). The purpose and intended use of each Appendix is explained either in the title of the appendix or in introductory paragraph(s). Each Appendix is aimed at providing useful guidance for the auditor in designing and performing risk assessment procedures.

17. In ISA 315 (Revised 2019), the appendices have largely been used to further explain matters more directly related to the entity that are considered helpful to the auditor in undertaking the procedures required by ISA 315 (Revised 2019). In contrast, matters related more directly to the auditor's actions about how to apply the requirements are contained within the application material.

18. Various matters related to the entity have been relocated from the application material of ISA 315 (Revised) to the appendices in ISA 315 (Revised 2019) including:

    (a) Matters related to understanding the entity and its business model (Appendix 1);

    (b) Understanding aspects of the entity's system of internal control (Appendix 3); and

    (c) Considerations for understanding an entity's internal audit function (Appendix 4).

19. In addition, several new appendices have been developed to assist with the execution of the standard:

Appendix No	Subject	Content
2	**Understanding Inherent Risk Factors**	• Describes how each of the inherent risk factors included within ISA 315 (Revised 2019) (i.e., complexity, subjectivity, change, uncertainty and susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk) arises. • Provides examples of events or conditions that may give rise to the existence of risks of material misstatement.
5	**Considerations for Understanding Information Technology**	Provides further matters for the auditor's consideration in understanding the entity's use of IT in its system of internal control, including: • Matters to consider when understanding the entity's use of IT in the components of the entity's system of internal control. • Examples of typical characteristics of information systems with different complexities. • Considerations around scalability. • Supporting material for identifying IT applications that are subject to risks arising from the use of IT
6	**Considerations for Understanding General IT Controls**	Developed to provide matters for consideration when the auditor is understanding general IT controls including: • Describing the nature of general IT controls. • Examples of general IT controls that may exist. • Examples of how general IT controls may address examples of risks arising from the use of IT, including for different IT applications based on their nature.

Objective of the Auditor

20. The overall objective of the auditor when performing procedures to identify and assess risks of material misstatement remains the same–i.e., to identify and assess the risks of material misstatement, whether due to fraud or error, at the

Para. 11

financial statement and assertion levels, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement.

New Definitions and Concepts in ISA 315 (Revised 2019)

21. Several new definitions have been introduced to help with clarity of the requirements. These new definitions have been set out in this guide where relevant (in dark blue boxes). Where definitions have been revised, this has also been explained.

Para. 12

22. There are also other new concepts that have been introduced, such as the *spectrum of inherent risk*,[11] also designed to assist with risk identification and assessment, and these have been explained where relevant throughout this guide (see paragraph 84(b) below).

Changes to the Risk Assessment Procedures and Related Activities

Risk Assessment Procedures–Nature and Extent

23. It has been clarified that the purpose of undertaking risk assessment procedures is to provide an *appropriate basis for* the identification and assessment of the risks of material misstatement, and the responses thereto (see paragraph 13 of ISA 315 (Revised 2019)).

Para. 13

24. It has also been emphasized in the revised standard that the evidence obtained in performing risk assessment procedures is audit evidence. The intention with this change is to help auditors understand the nature and extent of what needs to be done – i.e., enough evidence is needed to support an appropriate basis for the auditor's decisions thereafter to respond to the assessed risks of material misstatement.

25. The important concept of professional skepticism has also been reinforced in the requirement to perform risk assessment procedures more broadly, by highlighting that the risk assessment procedures are to be designed in a manner that is not biased towards obtaining corroborative audit evidence or excluding contradictory audit evidence.

Information from Other Sources

26. Broadly, although restructured, the requirements related to considering information from acceptance or continuance activities, and where other engagements have been performed for the client by the engagement partner, remain the same.

Para's 15 & 16

27. The auditor also still needs to consider information from previous experience with the entity and previous audits, however the auditor need not only consider the *relevance* of the information but must now also consider the *reliability* of such information.

Engagement Team Discussion

28. The matters for discussion at the engagement team discussion remain broadly the same, as well as the need to communicate to those engagement team members not involved in the discussions.

Para's 17 & 18

[11] ISA 315 (Revised 2019), paragraph 5

Changes to the Required Understanding

New Relevant Definition	Description	Further Explanatory Material
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[12] insofar as they affect inherent risk.	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. (Para. A7) 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. (Para. A8)

29. In ISA 315 (Revised 2019), there are broadly 3 distinct areas for the auditor's understanding:

- The entity and its environment.
- The applicable financial reporting framework.
- The entity's system of internal control.

In the previous version of the standard, ISA 315 (Revised), the applicable financial reporting framework was not separately distinguished (it was included as part of the understanding of the entity and its environment) – this has now been separated and has a distinct focus.

[12] ISA 240, paragraphs A24–A27

Changes to Understanding the Entity and Its Environment

Para. 19

30. To recognize the evolution and increasingly complex nature of the environment in which entities are operating, the required understanding of the entity and its environment now emphasizes the relevant aspects of the entity's business model (see paragraphs A62–A67 of ISA 315 (Revised 2019)). This focus is extended to also include the auditor's understanding of how the entity measures its performance. These changes are intended for the auditor to really understand how the entity operates, and measures its performance, from management's point of view, as that may better help the auditor understand where risks of material misstatement could arise.

31. The auditor's consideration of the inherent risk factors is first introduced when obtaining an understanding of the entity and its environment (see paragraph 34 below).

Changes to Understanding the Applicable Financial Reporting Framework

Para. 20

32. The risks of material misstatement become apparent as management applies the financial reporting requirements to the circumstances of the entity. Therefore, this has become an increasingly important area for the auditor in ISA 315 (Revised 2019) because risks of material misstatement could arise from how the applicable financial reporting framework is applied to the entity's circumstances.

33. How the applicable financial reporting framework is applied could be impacted by many factors, including the inherent risk factors (see below), the competence of those interpreting and applying the requirements as well as the amount of interpretation needed to apply the requirements. Some or all these factors could lead to risks of material misstatement as the applicable financial reporting framework is applied.

Inherent Risk Factors

Para's 19(c) & 31(a)

34. The intention of the inherent risk factors is to help auditors understand inherent risk, and assists the auditor in focusing on those aspects of events or conditions that affect an assertion's susceptibility to misstatement. Appendix 2 to ISA 315 (Revised 2019) describes each of the inherent risk factors and provides examples of events and conditions that may indicate the existence of risks of material misstatement in the financial statements. Application material has been added to further guide the auditor in taking the inherent factors into account, including explaining why they have been introduced (see paragraphs A85–A89 of ISA 315 (Revised 2019)).

35. 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. However, the auditor is not required to document every inherent risk factor that was taken into account in identifying and assessing the risks of material misstatement at the assertion level (see paragraph A241 of ISA 315 (Revised 2019).

36. Taking the inherent risk factors into account when obtaining an understanding of the entity and its environment, and the applicable financial reporting framework, is intended to facilitate a more focused and robust risk identification. Accordingly, when the auditor is understanding the entity and its

environment, the inherent risk factors may help in identifying where there may be risks of possible misstatement.

37. As the auditor obtains an understanding of the matters required to be understood relating to the entity and its environment, the inherent risk factors help the auditor draw a linkage between the information obtained and those areas where a risk of material misstatement in the financial statements could possibly exist.

38. To assist with identifying where possible misstatements could arise from the application of the applicable financial reporting framework, the inherent risk factors are also required to be taken into account when considering whether there are aspects of the financial reporting framework that could lead to a possible risk of material misstatement. For example, the requirements in the applicable financial reporting framework for accounting estimates may require management to use judgment in formulating the accounting estimate using assumptions about the future. In some cases, these estimates may involve significant uncertainty and may be complex to calculate, in which case the inherent risk factors of complexity, subjectivity and uncertainty relative to accounting estimates in the financial statements are relevant. This in turn could result in the identification of risks of material misstatement within the accounting estimate.

39. Inherent risk factors are also taken into account when the auditor is assessing inherent risk. By taking the inherent risk factors into account in assessing inherent risk, the auditor considers the degree to which the inherent risk factors affect the susceptibility of relevant assertions to misstatement (i.e., may help the auditor's consideration whether the assessment of inherent risk for the identified risk(s) of material misstatement at the assertion level should be higher or lower on the spectrum of inherent risk).

Changes to Understanding the Entity's System of Internal Control

New Relevant Definition	Description	Further Explanatory Material
Controls	Policies or procedures that an entity establishes to achieve the control objectives of management or those charged with governance. In this context: (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.	Controls are embedded within the components of the entity's system of internal control. (Para. A2) 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. (Para. A3) Procedures may be mandated, through formal documentation or other communication by management or those charged with governance, or may result from behaviors that

New Relevant Definition	Description	Further Explanatory Material
	(ii) Procedures are actions to implement policies.	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. (Para. A4) 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. (Para. A5)

40. Although the approach to understanding the entity's system of control is broadly the same as was required under ISA 315 (Revised) (i.e., understand the 5 components of the system of internal control), many changes have been made about what this understanding entails for each component. The application material in ISA 315 (Revised 2019) explains why the understanding of the various components of the entity's system of internal control is required (see paragraphs A97-A98 and A124-A125).

The Auditor is sill required to understand the 5 components of the entity's system of internal control

41. Part of the IAASB's efforts to help clarify what needs to be done to "obtain an understanding," is to present the requirements for each of the components in a consistent way – in a tabular format. The intention of the tables is that the requirements in each of these tables should be read together. The auditor achieves the objective of the requirement set out in the first line of the table, by performing the requirements in the left and the right-hand sides of the table. This presentation is to help auditors apply these requirements to the nature and circumstances of the entity being audited. However, the tabular format could be removed, and the requirements read in a more linear way – and this would have the same intended outcome.

42. The required understanding in the table for each component of the system of internal control is intended to delineate the two principal aspects that need to be done to obtain the requisite understanding:

    (a) Of the matters that the auditor should know about relevant to that component; and

    (b) An evaluation of those matters in context of that component and the nature and circumstances of the entity. For the control activities component, this evaluation is slightly different and is further explained in paragraph 59 below. In performing the evaluation for the relevant component, the scalability described in paragraph A92 of ISA 315 (Revised 2019) should be noted, i.e., that the way in which the entity's system of internal control is designed, implemented

and maintained varies with its size and complexity. For example, less complex entities may use less structured or simpler controls to achieve their objectives (and that may be appropriate to that entity).

43. Various clarifications have been made when referring to specific concepts or terms. The intention is that these words are used consistently so that there is no confusion as to what the concept or term means when applying it (the same principle also applies to any conforming and consequential amendments made):

(a) **The entity's system of internal control** – refers to the whole system made up of the 5 components as described in the definition in paragraph 12(m) of ISA 315 (Revised 2019).

(b) **Controls** – see new definition above. Controls are the *policies and procedures* embedded within the components of the entity's system of internal control. ISA 315 (Revised 2019) recognizes that these may not be formalized or documented but may still be evident through communications or implied through actions and decisions. Paragraphs A156–A157 of ISA 315 (Revised 2019) set out considerations for audits of less complex entities where controls may operate in a less formal way (e.g., through direct application by the owner-manager). However, notwithstanding the policies and procedures in some entities may be less formalized, an understanding of those policies and procedures are required (to the extent needed to meet the requirements of each component of the entity's system of internal control)[13] because this understanding informs the identification and assessment of the risks of material misstatement, and the responses thereto.

(c) **"Identified control"** – this term is used to distinguish that the control being referred to is one that is required to be identified in the control activities component.

(d) **Control Activities Component** – this term is only used to describe the name of the component of the system of internal control that sets out the specific individual controls to be identified (i.e., the term "control activities" has otherwise been removed), and for which the auditor is required to evaluate whether the control is designed effectively and determine whether the control has been implemented (hereafter referred to as D&I).

(e) **Indirect controls** – controls that are not sufficiently precise to prevent, detect or correct misstatements at the assertion level, but support other controls and so have an 'indirect' effect on those controls operating properly (see paragraphs A95 and A96of ISA 315 (Revised 2019)).

(f) **Direct controls** - controls that are sufficiently precise to prevent, detect or correct misstatements at the assertion level (see paragraphs A95 and A123 of ISA 315 (Revised 2019)).

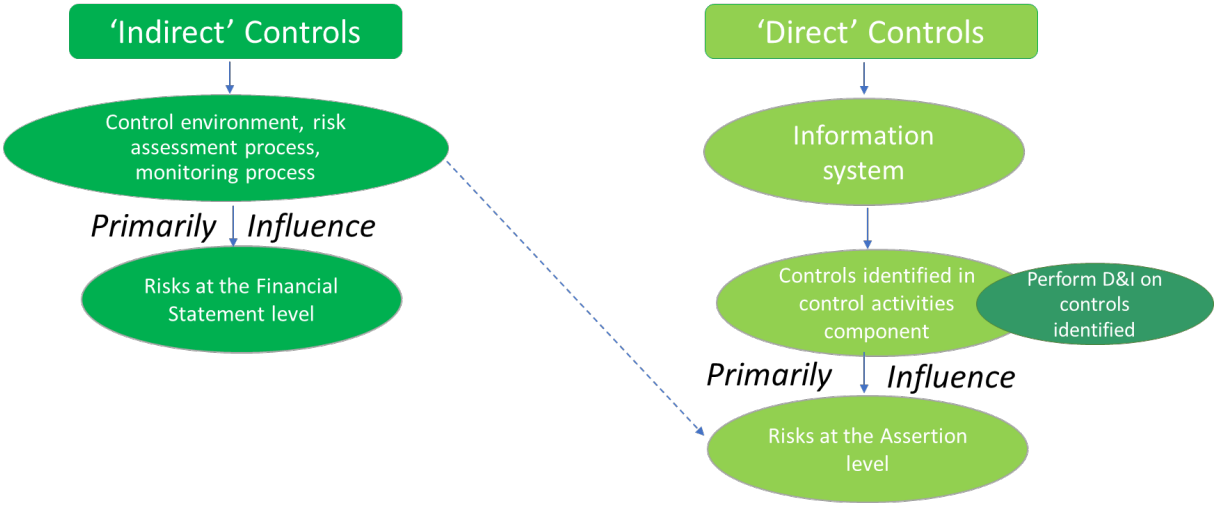
Distinction Between Indirect and Direct Components of the System of Internal Control

44. The 5 components of internal control have been split into two types that align with the nature of the controls within each component, and may affect the auditor's identification and assessment of risks of material misstatement, as well as responding to the assessed risks:

[13] ISA 315 (Revised 2019), paragraph A17

(a) In the control environment, the entity's risk assessment process and the entity's process to monitor the system of internal control components, the controls are primarily *indirect controls* (although there may be some direct controls these are likely less in these components).

(b) In the information system and communication, and control activities components the controls are primarily *direct controls*.



45. The indirect controls influence the effectiveness of the direct controls (for example, the control environment is foundational to the whole system of internal control, and if it is not functioning as expected this would impact how effective all the entity's controls may be). Paragraphs A97–A98 and A124–A125 of ISA 315 (Revised 2019) further explains why an understanding of all the components of the system of internal control are required.

46. Further clarity about what exactly needs to be done in relation to the components of the system of internal control that primarily include direct controls (i.e., in the information system and communication, and control activities components) has been included in the revised standard. Also, understanding Information Technology (IT) in relation to the entity's system of internal control has been clarified and enhanced (see section below on "Information Technology Considerations").

Individual Changes Within Each Component of the System of Internal Control

47. Each component has been revised to make clear "*what*" needs to be understood (i.e., on the left side of the table for the requirements of each component of the system of internal control), together with the requisite evaluation on the right side of the table, to have 'obtained' the relevant understanding.

48. The objective of the evaluation, where required, for each of the components of the entity's system of internal control, is to determine whether there is a deficiency(ies) in that component (in the context of the nature and circumstances of the entity) that may impact the auditor's identification and assessment of risks of material misstatement (as well as the design of further audit procedures in accordance with ISA 330). The requirement to determine whether there are any deficiencies identified now addresses all the work performed to understand the entity's system of internal control (see paragraph 27 of ISA 315 (Revised 2019)).

Control Environment

49. The specific matters required to be understood for the control environment are now included in the requirement (paragraph 21(a) of ISA 315 (Revised 2019)), whereas previously some of these matters were only referred to within the application material. The evaluation of the component is now also more specific about those matters to be evaluated and paragraph A103 of ISA 315 (Revised 2019) explains why the evaluation is required (and emphasizes the foundational nature of the control environment component).

Para. 21

The Entity's Risk Assessment Process

50. Although the specific matters required to be understood for the entity's risk assessment process are similar to what was required under ISA 315 (Revised), an evaluation of the process the entity has in place while considering the nature and circumstances of the entity is now required (as explained in paragraph 42(b) above). Paragraph A111 of ISA 315 (Revised 2019) explains why the auditor evaluates whether the entity's risk assessment process is appropriate, including that it assists with understanding how the entity has identified risks that may occur, and how those risks have been assessed and addressed.

Para. 22

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

51. The focus is on the entity's *process* to monitor the entity's system of internal control – this was previously understanding the major activities that the entity used to monitor internal control. As with the other components of internal control in ISA 315 (Revised 2019), an evaluation of the process the entity has in place while considering the nature and circumstances of the entity is also now required (as explained in paragraph 42(b) above). Paragraph A120 of ISA 315 (Revised 2019) explains that considering the sources of information the entity uses to monitor controls assists with understanding whether the process itself is appropriate for that entity.

Para. 24

The Information System and Communication

52. To help clarify the scope of the understanding, ISA 315 (Revised 2019) requires that the information processing activities for each significant class of transactions, account balance and disclosure is required to be understood. Although the required determination of significant classes of transactions, account balances and disclosures is only addressed later in the standard, based on the risk assessment procedures performed to obtain an understanding of the entity and its environment, and the applicable financial reporting framework, the auditor may have a preliminary expectation of the significant classes of transactions, account balances and disclosures. If the determination at the later stage results in additional (or different) significant classes of transactions, account balances or disclosures, the auditor would need to then obtain the relevant understanding of that part of the information system.

Para. 25

53. In addition to understanding the data and information, ISA 315 (Revised 2019) now also requires that any resources within the information system also be included (paragraph A133 of ISA 315 (Revised 2019) addresses aspects about human resources that may be relevant (such as the competence of individuals undertaking the work, whether there are adequate resources and whether there is appropriate segregation of duties). IT resources and related matters are explained separately below.

54. The application material sets out that the auditor's understanding can be obtained through inquiries, inspection, observation or selecting transactions and tracing them through the applicable process in the information system (i.e., performing a walk-through) (see paragraph A136 of ISA 315 (Revised 2019)).

55. The focus on information obtained from outside of the general and subsidiary ledgers (in particular in relation to disclosures) is maintained (see paragraphs A138–A139 of ISA 315 (Revised 2019)).

56. This component of the system of internal control also requires an evaluation of whether the entity's information system and communication appropriately support the preparation of the entity's financial statements (as explained in paragraph 42(b) above).

Control Activities

57. The control activities component now lists the specific controls that the auditor is required to identify and perform D&I thereon. Previously the controls required to be understood for the purpose of this component was more of an overarching requirement based on the understanding of the entity's system of internal control as a whole. Clarity has now been provided about which controls are required to be understood (including that D&I are required ONLY for these controls).

Para. 26

58. The following sets out the controls required to be identified by paragraph 26(a)(i)-(iv) of ISA 315 (Revised 2019):

    (a) Controls that address significant risks (see paragraphs 86–89 below);

    (b) Controls over journal (see paragraphs 60–63 below);

    (c) Controls for which the auditor plans to test the operating effectiveness of controls, either because the auditor has decided that is the most efficient audit approach or because substantive procedures alone would not provide sufficient appropriate audit evidence (examples of such controls are provided in paragraph A163 of ISA 315 (Revised 2019); and

    (d) Other controls the auditor considers appropriate based on the auditor's professional judgment (see paragraph 64 below).

59. Paragraphs A175–A179 of ISA 315 (Revised 2019) further explains the auditor's procedures when undertaking D&I. The auditor is required to identify specific controls (in the control activities component) and perform D&I on these controls as it assists with the auditors understanding about management's approach to addressing certain risks and therefore provides a basis for the design and performance of further audit procedures that are responsive to those risks as required by ISA 330. Paragraph A180 explains those circumstances where D&I is sufficient for 'testing operating effectiveness' (i.e., for automated controls).

Controls over journal entries

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

Para. 26(a)(ii)

61. Professional judgment is used to determine the journal entries that are relevant for the purpose of identifying the controls in paragraph 26(a)(ii)[14] of ISA 315 (Revised 2019). In today's environment where there are significant automated processes, the auditor 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).

62. Paragraph 25 of ISA 315 (Revised 2019) requires the auditor 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…"[15] In obtaining this required understanding, the auditor would have obtained knowledge about how transactions are processed, 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.

63. 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. These controls include:

    (a) Controls over non-standard journal entries – where the journal entries are automated or manual and are used to record non-recurring, unusual transactions or adjustments.

    (b) 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 having 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.

Other controls the auditor considers appropriate

64. Paragraph A165 of ISA 315 (Revised 2019) explains the 'other controls to be identified based on the auditor's judgment' may include:

Para. 26(a)(iv)

[14] 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.

[15] ISA 315 (Revised 2019), paragraph 25(a)(i)

(a) Controls that address risks that are assessed as higher on the spectrum of inherent risk (not determined to be a significant risk);

(b) Controls related to reconciling detailed records to the general ledger; or

(c) Complementary user entry controls, if using a service organization.

Control Deficiencies

65. Control deficiencies may be identified when obtaining an understanding of each component of the entity's system of internal control (in particular, through the various evaluations required, it may be found that the entity's policies or procedures are not appropriate to the nature and circumstances of the entity). Application material in paragraph A182 in ISA 315 (Revised 2019) explains that the auditor may consider the effect of these deficiencies identified on the further audit procedures the auditor undertakes in ISA 330 (i.e., what impact on the audit approach the deficiency may have).

Para. 27

66. In addition, in accordance with ISA 265[16] the auditor is required to determine whether one or a combination of deficiencies constitutes a significant deficiency (which is further addressed in ISA 265).

Information Technology Considerations

New Relevant Definitions	Description	Further Explanatory Material
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*.	N/A
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).	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

[16] ISA 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*

New Relevant Definitions	Description	Further Explanatory Material
		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. (Para. A6)
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.	N/A
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).	N/A

67. ISA 315 (Revised 2019) has substantially changed and enhanced the requirements and application material in relation to the auditor's considerations about IT. This takes into account the increasing

use and complexity of IT for many entities. Paragraph A170 in ISA 315 (Revised 2019) explains that 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 circumstances of the entity and its IT environment, as well as based on the nature and extent of the controls identified by the auditor. It is also noted that as the entity's IT environment and IT systems become more complex, the work performed will likely involve team members with specialized IT skills.[17] Scalability, in particular where the IT systems are less complex, has also been focused on – see further explanation in paragraph 73 below.

68. The main changes with regard to IT can be found in the auditor's required understanding of the information system and control activities components.

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

    (a) 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

    (b) 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.

70. 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[18] (see new definition for *risks arising from the use of IT* above) for the identified controls in the control activities component (i.e., those controls as set out in paragraph 58 above). These identified controls are focused on information processing controls (newly defined – see new definition above) that directly address the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information).[19,20] From this, the auditor is then required to identify the related risks arising from the use of IT and the entity's general IT controls that address such risks[21] (*general IT controls* are newly defined, see new definition above). D&I is required for these 'identified' general IT controls.

71. Application material set out in paragraphs A166–A174 in ISA 315 (Revised 2019) further explains identifying IT applications and other aspects of the IT environment and related risks arising from the use of IT. Appendix 5 to ISA 315 (Revised 2019) also provides example characteristics of IT applications and other aspects of the IT environment, and guidance related to those characteristics. Appendix 6 further explains 'considerations for understanding general IT controls.'

---

17 ISA 315 (Revised 2019), paragraph A171

18 ISA 315 (Revised 2019), Paragraph 26(b)

19 ISA 315 (Revised 2019), paragraph A148

20 The auditor is not required to identify and evaluate all information processing controls related to the entity's policies that define the flow of transactions and other aspects of the entity's information processing activities for the significant classes of transactions, account balances and disclosures (paragraph A148 of ISA 315 (Revised 2019)).

21 ISA 315 (Revised 2019), Paragraph 26(c)

72. When identifying the general IT controls that will be subject to D&I (for example, general IT controls related to those identified controls in paragraph 26(a)(i)-(iv) in ISA 315 (Revised 2019) (such as controls over journal entries)), supporting application material:

    (a) Explains that controls identified by the auditor may depend on system-generated reports, in which case the applications that produce those reports may be subject to risks arising from the use of IT. Alternatively, the auditor may not plan to rely on controls over those systems generated reports and rather plan to directly test the inputs and outputs of those reports, in which case the auditor may not identify related IT applications as being subject to risks arising from the use IT (see paragraph A169 in ISA 315 (Revised 2019)). Depending on the nature of the controls over journal entries, there may be a combination of controls that can be tested directly or the auditor may plan to test general IT controls that provide for the consistent operation of an automated control instead of testing the automated control directly.

    (b) Makes clear the extent of the understanding of the IT processes will vary with the nature and circumstances of the entity and its IT environment (see paragraph A170 in ISA 315 (Revised 2019) and examples thereafter).

    (c) Explains when the other aspects of the IT environment subject to risks arising from the use of IT may be relevant (see paragraph A172 in ISA 315 (Revised 2019)).

    (d) Explains that identifying risks arising from the use of IT relates only to the identified IT applications for the controls in the control activities component (as identified in paragraph 26(b) in ISA 315 (Revised 2019)), and that when considering general IT controls these are considered more broadly (i.e., not necessarily for each control identified in paragraph 26(a)) (see examples in application material in paragraphs A173-A174 in ISA 315 (Revised 2019)).

    Therefore, for example in the case of controls over journal entries, 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 general IT control for which D&I is required. But rather, general IT controls are considered in terms of how they relate to the relevant risks arising from the use of IT for the IT applications for the identified controls in paragraph 26(a)(i)-(iv) in ISA 315 (Revised 2019). The identification of those general IT controls subject to D&I would be a judgment based on the nature and circumstances of the entity, including its information system.

73. 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 circumstances of the entity, its IT environment and the nature and extent of the controls identified by the auditor. Examples to illustrate the scalability (i.e., for an entity using commercial software and for an entity with multiple IT applications and IT processes that are complex) have been provided (see paragraphs A170-A171 in ISA 315 (Revised 2019)). Appendix 5 (paragraph 15) also focuses on scalability of IT applications and risks arising from the use of IT.

Changes to the Identification and Assessment of the Risks of Material Misstatement

New Relevant Definitions	Description	Further Explanatory Material
Relevant assertion	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).	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. (Para. A9)
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.	N/A

74. ISA 315 (Revised 2019) has separated the requirements for identifying risks of material misstatement from the requirements for assessing those risks. The changes in this section are aimed at developing a framework for auditors to identify and assess risks of material misstatement in a robust manner.

Identifying Risks of Material Misstatement

75. As noted above, the audit risk model has not changed. The auditor is still required to identify risks of material misstatement at both the financial statement and assertion levels. The identification of risks of material misstatement continues to be performed before the consideration of any related controls (i.e., the inherent risk) (see paragraph A186 in ISA 315 (Revised 2019)). The assertions remain the same, and the auditor may still use different assertions as long as all aspects of the assertions set out in the standard have been covered (see paragraphs A189–A191 in ISA 315 (Revised 2019)).

Para. 28

76. Risks of material misstatement at the financial statement level refer to risks that relate pervasively to the financial statements as a whole, and potentially affect many assertions (e.g., if management are not competent this will affect the financial statements pervasively). ISA 315 (Revised 2019) places a bigger focus on risks at the financial statement level and better explains the link between risks of material misstatement at the financial statement level and the assertion level. This is because the auditor needs to determine whether the risks identified have a pervasive effect on the financial statements and would therefore require an overall response in accordance with ISA 330.[22] Financial statement level risks may also affect individual assertions and so may also help in determining audit procedures to address those identified risks.

[22] ISA 300, *Planning an Audit of Financial Statements*

77. The identification of financial statement level risks is also influenced by:

    (a) The auditor's understanding of the entity's system of internal control, in particular the evaluation and identification of deficiencies in the indirect components (see paragraphs 42(b) and 49-51 above).

    (b) Susceptibility to misstatement due to fraud risk factors that affect inherent risk (see paragraph A197 in ISA 315 (Revised 2019))

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

79. In identifying the risks of material misstatement at the assertion level, the auditor is now required to also determine relevant assertions and related significant classes of transactions, account balances and disclosures. Both of these concepts are newly defined – see new definitions above.

Para. 29

80. Relevant assertions are intended to focus auditors on those assertions for a class of transactions, account balance or disclosure for which the nature or circumstances are such that there is both a reasonable possibility of occurrence of a misstatement(s) and being material if it were to occur. As noted in paragraph 6 above, application material has been added to the definition of "risk of material misstatement" in ISA 200 to further explain this threshold.

81. By definition, a significant class of transactions, account balance or disclosure is one where there is one or more relevant assertion(s). Determining significant classes of transactions, account balances and disclosures helps clarify the auditor's work in relation to understanding the information system, as well as developing the auditor's responses that are required by ISA 330. With respect to disclosures, the application material in paragraph A204 of ISA 315 (Revised 2019) explains matters that may drive disclosures to be significant.

Assessing Risks of Material Misstatement at the Financial Statement Level

82. ISA 315 (Revised 2019) has clarified the purpose of assessing risks *at the financial statement level*, i.e., that the requirement to assess the risks of material misstatement at the financial statement level is twofold: to determine whether such risks affect the assessment of risks at the assertion level; and to evaluate the nature and extent of their pervasive effect on the financial statements.

Para. 30

Assessing Risks of Material Misstatement at the Assertion Level

83. The introduction to ISA 315 (Revised 2019) describes the *spectrum of inherent risk* as the "degree to which inherent risk varies."[23] Assessing inherent risk at the assertion level represents a judgment within a range, from lower to higher, on the spectrum of inherent risk (see paragraphs A208-209 in ISA 315 (Revised 2019)). The auditor may designate these assessed risks of material misstatement within categories along the spectrum of inherent risk – these categories may be described in different ways so long as the auditor's assessment of inherent risk is appropriate such that the response to those assessed risks is responsive to the assessed inherent risk and the reasons for that assessment.

[23] ISA 315 (Revised 2019), paragraph 7

84. The approach to assessing inherent risk *at the assertion level* has been enhanced. Although more granular than the requirements in the previous version of the standard (ISA 315 (Revised)), it is intended to facilitate a greater consistency in the assessment of the risks of material misstatement. The auditor is required to:

Para. 31

(a) *Assess the likelihood and magnitude of misstatement*—the relative degrees of likelihood and magnitude of a possible misstatement help determine where on the spectrum of inherent risk the identified risk of misstatement is assessed. The likelihood and magnitude of a possible misstatement is influenced by the inherent risk factors (either individually or in combination), but also recognizes that inherent risk may be higher for some assertions than others. In considering the magnitude of a misstatement, the auditor considers the size, nature or circumstances of the possible misstatement (i.e., takes into account quantitative and qualitative aspects).

(b) *Determine where on the spectrum of inherent risk the possible misstatement is assessed*—the greater the degree to which a class of transactions, account balance or disclosure is susceptible to material misstatement, the higher on the spectrum of inherent risk the assessment of inherent risk is going to be, and vice versa. The auditor uses professional judgment in determining the significance of the combination of the likelihood and magnitude of a misstatement.

- For an assessed risk to be higher on the spectrum of inherent risk, it does not need both magnitude and likelihood to be assessed as high – rather the intersection of the magnitude and likelihood will determine whether the assessed risk is higher or lower on the spectrum of inherent risk. For example, a higher inherent risk assessment could result from a lower likelihood of the risk occurring but a very high magnitude.[24]
- The standard does not specify categorizations along the spectrum of inherent risk but does recognize that these may be used by auditors.[25]

85. Assessing inherent risks in this way assists the auditor in developing an appropriate response to the risks of material misstatement. For example, the higher on the spectrum of inherent risk the identified risk is assessed, the more persuasive the audit evidence will need to be to respond to the assessed risk. In addition, this way of assessing inherent risk also helps to determine significant risks (see below).

Significant Risks

86. Rather than focusing on the responses to risks (as the definition in ISA 315 (Revised) does),[26] the definition of significant risk in ISA 315 (Revised 2019) has been revised to focus on when the assessment of inherent risk is close to the upper end of the spectrum of inherent risk. It is envisioned therefore that this could relate to one or more risks, and may differ period to period, depending on the nature and circumstances of the entity. Therefore, two entities within the same industry would not necessarily have the same significant risks.

Para. 32

[24] ISA 315 (Revised 2019), paragraph A213

[25] ISA 315 (Revised 2019), paragraph A214

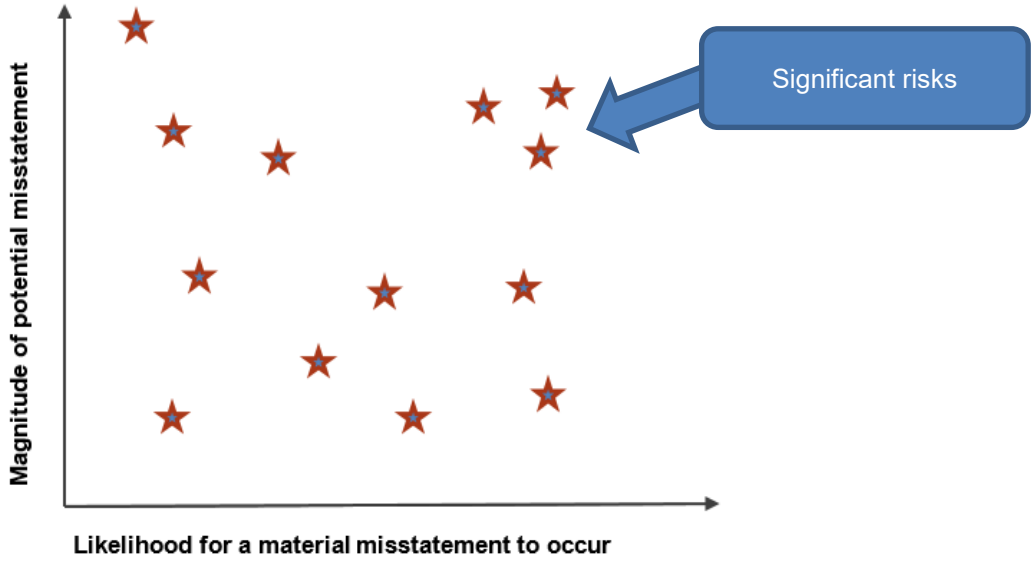
[26] ISA 315 (Revised) defines “significant risk” as “an identified and assessed risk of material misstatement that in the auditor’s judgment, requires special audit consideration.”

87. The revised definition for a significant risk encompasses two elements. A risk is determined to be significant where:

    (a) The assessment of inherent risk is close to the upper end of the spectrum of inherent risk due to the degree to which the inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur. The combination of likelihood and magnitude means that a significant risk could potentially have a low likelihood but the magnitude could be very high if it occurred. Although these risks are considered less likely to be a significant risk (compared to risks where both the likelihood and magnitude are high), they have not been explicitly excluded; or

    (b) The risk is to be treated as a significant risk in accordance with the requirements of other ISAs (e.g., fraud risks).

88. Unless required to be designated as a significant risk by another ISA, the determination of significant risks is a matter of professional judgment. Paragraph A221 in ISA 315 (Revised 2019) provides some examples of those matters where significant risks may be more prevalent.



89. Although the responses to risks are no longer driving the auditor's determination of what a significant risk is, once a risk has been determined as significant, ISA 315 (Revised 2019) and other ISAs still contain specified responses for those risks that have determined to be significant. For example, as explained in paragraph 58 above (control activities component), controls related to significant risks are required to be identified and D&I performed.

Control Risk

90. ISA 315 (Revised 2019) no longer facilitates the option of assessing inherent and control risk together, i.e., they are required to be assessed separately (although control risk is not identified the auditor's understanding of the components of the entity's system of internal control assists the auditor in the assessment of control risk).

91. There is also a stronger link of the assessment of control risk with the work undertaken in obtaining an understanding of the components of the entity's system of internal control. The auditor's

understanding of the entity's system of internal control informs the auditor's expectations about the operating effectiveness of controls and whether the auditor plans to test the operating effectiveness of controls in designing and performing further audit procedures in accordance with ISA 330.

92. Any plans to test the operating effectiveness of controls is based on an expectation that controls are operating effectively, and this forms the basis of the auditor's assessment of control risk. Accordingly, if, based on the work undertaken in the control activities component (see paragraph 58 above), the auditor does not plan to test the operating effectiveness of controls, the assessment of control risk is such that the assessment of the risks of material misstatement is the same as the assessment of inherent risk (i.e., control risk is 'maximum'). Therefore, if the auditor plans to undertake a primarily substantive approach to the audit, once the understanding of the components of the system of internal control has been obtained and the relevant work done for that purpose (as required by paragraphs 21 – 27 of ISA 315 (Revised 2019)), there is no need for further testing of controls.

93. ISA 315 (Revised 2019) also emphasizes that if the auditor plans to test the operating effectiveness of the control, and the control is automated, there may be a need to test the operating effectiveness of the related general IT controls that support the functioning of that automated control (see paragraph A229 in ISA 315 (Revised 2019)).

Evaluating Audit Evidence Obtained from Risk Assessment Procedures

Para. 35

94. To reinforce professional skepticism within the standard, a new requirement to evaluate whether the audit evidence obtained from risk assessment procedures provides an appropriate basis for the identification and assessment of the risks of material misstatement has been added (paragraph 35 in ISA 315 (Revised 2019)).

New Stand-back – Classes of Transactions, Account Balances and Disclosures that are Not Significant but are Material

Para. 36

95. With the intention to enhance and improve the completeness of the risk identification process, a new stand-back is required once the auditor is nearing the end of the process (paragraph 36 in ISA 315 (Revised 2019)).

96. The auditor is required to evaluate the completeness of the significant classes of transactions, account balances and disclosures identified by the auditor. This is done by focusing on those classes of transactions, account balances and disclosures that are material (either quantitatively or qualitatively) but have not been identified as significant (i.e., no identified risks of material misstatement and therefore no relevant assertions).

97. It should be noted that paragraph 18 in ISA 330, also targeted at 'material' classes of transactions, account balances and disclosures still remains (i.e., requires substantive procedures for all material classes of transactions, account balances and disclosures). The interaction of the new stand-back in ISA 315 (Revised 2019) and the requirement in ISA 330 is further explained in paragraphs A233–A235 of ISA 315 (Revised 2019). As part of the project to revise ISA 315 (Revised), the IAASB reconsidered the interaction of the new requirement in ISA 315 (Revised 2019) and paragraph 18 of ISA 330 and whether the latter was still needed, despite these paragraphs serving a similar purpose to safeguard against imperfect risk identification and assessment. The Board agreed to maintain paragraph 18 of ISA 330 but made changes to:

- Clarify that ISA 330 paragraph 18 applies to classes of transactions, account balances or disclosures that are '*quantitatively or qualitatively material*' to align with the scope of ISA 315 (Revised 2019),
- Explain, in the application material,[27] the interaction of the requirement with the new concept of significant classes of transactions, account balances and disclosures.
- Clarify that not all assertions in respect of classes of transactions, account balances or disclosures affected by this requirement are required to be tested. It is explained in paragraph A42a in the conforming and consequential amendments to ISA 330 that when designing substantive procedures to be performed, the procedures are focused on those assertion(s) where, if a misstatement were to occur, there is a reasonable possibility of the misstatement being material.

Documentation

98. Based on the clarifications and enhancements made in ISA 315 (Revised 2019), the IAASB agreed that more would be required to be documented (in terms of the requirements of ISA 230[28]), in particular the requirement to document 'significant judgments'[29] that will be made by the auditor in identifying and assessing the risks of material misstatement. However, to focus on some of the key changes made, in particular in relation to controls and significant risks, new and enhanced documentation is required for:

    (a) Key elements of the auditor's understanding of the entity and its environment, the applicable financial reporting framework and each of the components of the entity's system of internal control (the specific paragraphs where the aspects are required to be documented have been noted). The documentation should include the source of the information as well as the risk assessment procedures performed.

    (b) D&I of controls in the control activities component.

    (c) The identified and assessed risks of material misstatement at the financial statement and assertion levels. This also includes significant risks and risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. The rationale for significant judgments made also need to be documented.

    (d) Paragraph A238 in ISA 315 (Revised 2019) also notes various matters that could be documented to demonstrate the exercise of professional skepticism by the auditor.

[27] ISA 315 (Revised 2019), paragraph A233

[28] ISA 230, *Audit Documentation*

[29] ISA 230, paragraph 8(c)

The objective of the IAASB is to serve the public interest by setting high-quality auditing, assurance, and other related standards and by facilitating the convergence of international and national auditing and assurance standards, thereby enhancing the quality and consistency of practice throughout the world and strengthening public confidence in the global auditing and assurance profession.

The IAASB develops auditing and assurance standards and guidance for use by all professional accountants under a shared standard-setting process involving the Public Interest Oversight Board, which oversees the activities of the IAASB, and the IAASB Consultative Advisory Group, which provides public interest input into the development of the standards and guidance.

IAASB
International Auditing
and Assurance
Standards Board

529 Fifth Avenue, New York, NY 10017
T + 1 (212) 286-9344 **F** +1 (212) 286-9570
www.iaasb.org