

ISA 315 (Revised)¹—Issues and Recommendations

Objective of the IAASB Discussion

The objective of this agenda item is to obtain the Consultative Advisory Group's (CAG) views on the second draft of the proposed revisions to ISA 315 (Revised) as set out in **Agenda Item G.2 (Requirements)** and **G.3 (Application Material)**.

1. What has changed since we last met?

The ISA 315 Task Force presented papers to the September, October and December 2017 IAASB meetings after presenting to the CAG in September 2017. Changes to the Task Force views and resultant changes to the Requirements and Application Material have been presented in this paper. **Text presented in blue represents matters that were presented to the Board in December 2017**, and have been included to assist the CAG in understanding the journey of the ISA 315 Task Force.

2. What does the Task Force ask of the CAG?

The Task Force would appreciate the CAG's reaction to the changes made to date, and whether there are any other changes that should still be considered. *Specific matters for CAG consideration can be found on page 21.*

3. Why is the paper so long?

Since the last CAG meeting in September 2017, the Task Force presented papers to 3 separate Board meetings. As noted earlier, text presented in blue represents matters that were presented to the Board in the December 2017 IAASB meeting. In addition, the content of the issues paper presented to the Board in October 2017, is presented in Appendix 2 of this paper.

I. Structure of this Paper and Format of the IAASB Discussion

1. This paper sets out Task Force views about proposed changes to ISA 315 (Revised) in both the requirements and related application material. The proposed changes are presented as follows:
 - **Agenda Item G.2:** sets out the Task Force's views on all the proposed changes to the requirements (marked to extant ISA 315 (Revised)).
 - **Agenda Item G.3:** sets out proposed changes to the application material (marked to extant ISA 315 (Revised)). In considering the application material, the CAG is asked to note that the considerations specific to public sector will be updated after planned outreach with public sector representatives in March 2018. The Task Force will continue to consider the scalability of the standard as it further refines the proposed changes (scalability is discussed further in paragraphs 11 and 67–69 of this paper). In addition, the Task Force continues to consider the application material related to information technology considerations as well as general IT controls.

The substantive issues being raised for the purposes of the March 2017 IAASB meeting are included in this paper and Agenda Items G, G.2 and G.3. The Appendix to Agenda Item G provides a project history, including links to the relevant CAG documentation.

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

2. In addition, in working through the changes to the standard, the ISA 315 Task Force (the ‘Task Force’) will continue to consider whether additional non-authoritative guidance should be developed (e.g., for small and medium practices (SMPs) to illustrate what needs to be done, by way of examples).
3. The Task Force has to still consider conforming amendments arising from the proposed changes to ISA 315 (Revised), which will be presented at the June 2018 IAASB meeting for discussion, with the exception of conforming amendments relating to ISA 330,² paragraph 18 (see paragraph 62 of this paper). The Task Force has identified likely conforming amendments to ISA 200³ (also see paragraph 10 of this paper), ISA 330 and ISA 540 (Revised)⁴ to date in its work to revise ISA 315 (Revised). In relation to conforming changes to ISA 540, the Task Force will work with the ISA 540 Task Force with regard to sequencing of the changes as the ISA 540 Task Force finalizes that standard.
4. The Task Force’s activities including outreach and coordination with other IAASB Task Forces or Working Groups, can be found in Appendix 1 to this paper. Matters that crossover the project to revise ISA 540, including the outcomes of the joint meetings with the ISA 540 Task Force, can be found in paragraph 5 below, and coordination with the Data Analytics Working Group (DAWG) can be found in paragraphs 70–72 of this paper.
5. The Task Force continues to coordinate with the ISA 540 Task force as both projects progress. In particular, matters of coordination the Task Forces have focused on include:
 - Alignment of the use of inherent risk factors, and the requirements about obtaining an understanding of the system of internal control (see paragraph 37 of this paper), within each standard.
 - Spectrum of risk—the ISA 315 Task Force continues to work through how this can be explained in ISA 315 (Revised) (see further explanation in paragraphs 8–9 of this paper). As noted in The ISA 540 Task Force’s IAASB Agenda Paper (Agenda Item 2 , paragraphs 11 to 12), the ISA 540 Task Force will also continue to monitor the changes and align changes to ISA 540 (Revised) accordingly
 - Conforming amendments that may still be needed once ISA 540 (Revised) is finalized and the ISA 315 (Revised) Exposure Draft is published—in the coordinated work being undertaken by the two Task Forces it is expected that the conforming changes will be minimal but the ISA 315 Task Force still needs to further consider any changes that may be needed to ISA 540 once it is finalized. These matters will be brought to the Board for discussion in June 2018.

II. Matters Relating to the Proposed Changes in ISA 315 (Revised)

6. This section describes significant changes made since the September 2017 CAG meeting.

Title, Scope, New Introductory Paragraphs and Objective (Requirements: paragraphs 1 through 3⁵ of ISA 315 (Revised))

7. There have been no changes made to the title, scope and objective since previously presented.

² ISA 330, *The Auditor’s Responses to Assessed Risks*

³ ISA 200, *Overall Objectives of the independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*

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

⁵ The effective date of the revised standard will be further considered at the time of exposure.

8. ISA 315 (Revised) substantially builds off the concepts in ISA 200, which defines and describes audit risk, the risks of material misstatement (including that they may exist at the overall financial statements level or the assertion level), describes the concepts of control risk and inherent risk, and describes that some risks are higher than others (i.e., introducing the concept that there is a 'spectrum of risk'). ISA 330 requires the auditor to design and implement overall responses to address the assessed risks of material misstatement at the financial statement level to design and perform further audit procedures to address assessed risks of material misstatement at the assertion level, and further describes what this involves.
9. To provide context for the requirements and guidance in ISA 315 (Revised) relating to the identification and assessment of the risks of material misstatement, the Task Force had referenced certain paragraphs from ISA 200 and ISA 330 in the revised application material proposed to the Board in December 2017. The Board found these generally to be useful in explaining key concepts. However, some concerns were expressed about the nature of some of these paragraphs as it appeared in some cases that those paragraphs were addressing matters within the scope of ISA 330 (which deals with how to respond to the identified risks of material misstatement). Accordingly, the Task Force has removed this text from the application material and instead reorganized this material as introductory paragraphs to ISA 315 (Revised). The Task Force is of the view that this provides context for the requirements and application material, in particular introducing some of the concepts that are key to understanding the standard, such as 'spectrum of risk.'
10. The Task Force has not yet specifically considered conforming or consequential amendments to ISA 200 beyond the prior acknowledgement that ISA 200, paragraph A42,⁶ will require amendment to clarify that ISA 315 (Revised) requires separate assessments of inherent risk and control risk. The paragraphs of ISA 200 that deal with audit risk and related concepts are included in Appendix 3 to this paper for the Board's reference. The Task Force is interested in Board views as to whether the draft introductory paragraphs draw an adequate connection to these concepts in ISA 200 and whether any further consequential amendments to ISA 200 should be considered by the Task Force beyond those planned for paragraph A42.
11. In developing the introductory paragraphs, the Task Force also has the view that it is important to emphasize the scalability of the standard in the way it is applied, i.e., that the nature and extent of what is required to be performed in ISA 315 (Revised) depends on the nature and complexity of the entity, as well as the entity's system of internal control, including its IT environment.

Definitions

Task Force Views on the Proposed Changes

[Assertions](#) (Definition: paragraph 4(aa) of ISA 315 (Revised); Application Material – paragraph A0a–A0aa of ISA 315 (Revised))

12. To respond to Board comments that the proposed changes should be further considered, given that the concept of assertions was thought to be fairly well-understood by auditors, but possibly less well so by other stakeholders, the Task Force decided to revert to the extant definition and to elevate part of the description of the concept of assertions from extant paragraph A127. As a result, the definition of assertions now includes that assertions are inherent in representing that the financial statements are in accordance with the applicable financial reporting framework.

⁶ The project to revise ISA 540 has also proposed amendments to this paragraph (see Agenda Item 2)

13. Explanatory material has been added to differentiate written representations from management (obtained by the auditor in accordance with ISA 580⁷) from representations by management as referred to in the definition of assertions, because it had been noted that there was concern about whether the representations were the same or different.

Controls (Definition: paragraph 4(ca) of ISA 315 (Revised); Application Material – paragraphs A0b–A0c of ISA 315 (Revised))

14. The Board provided comments that controls are broader than just formalized ‘policies and procedures,’ including observations that controls could include aspects of governance (such as tone at the top) and other aspects of the entity’s systems (such as the risk assessment process in some entities) which are established, but not always formally documented policies or procedures. In response, the Task Force broadened the proposed definition of controls and presented a revised definition for Board discussion at the October 2017 IAASB meeting. Although a Board member noted concern about the use of the word ‘informal’ in the definition, the Task Force is of the view that in small-and medium- entities (SME’s) some controls may not be ‘formally’ documented but nevertheless still exist and may be relevant to the audit. This term therefore acknowledges those types of controls thereby contributing to the scalability of the definition (this has been further revised based on the IAASB discussions in December 2017– see discussion below).
15. To address concerns about describing policies as including “informal expectations” the Task Force has revised the definition to recognize that policies may include statements that may be documented, explicitly stated in communications or implied through actions and decisions, which may make it clearer that policies have authority even if delivered through some kind of communication or action (i.e., still recognizing that it does not have to be formal written policies). The revised definition reflects the description of ‘controls’ in the *2013 Committee of Sponsoring Organizations Internal Control – Integrated Framework* (COSO Framework 2013).
16. Explanatory material has also been added to clarify that procedures may be enforced through the actions permitted by the design of the IT application used by the entity.

General Information Technology (IT) Controls and Application Controls (Definition: paragraph 4(a) and 4(caa) of ISA 315 (Revised))

17. In response to Board comments at the October and December 2017 meetings, the Task Force has proposed adding a definition of General IT Controls. The definition included in Agenda Item G.2 is taken from the extant Glossary. As this definition refers to “application controls” and this term is also used in the application material of ISA 315 (Revised), the Task Force is of the view that including the definition of “application controls in information technology” from the Glossary would also be helpful. The Task Force however is of the view that both of these definitions may benefit from modernization. If the Board supports the addition of these terms to the definitions, the Task Force will seek to update them to more closely reflect current state IT environments.

Qualitative Inherent Risk Factors (QIRFs) (Definition: paragraph 4(cb) of ISA 315 (Revised); Application Material – paragraph A0d–A0g of ISA 315 (Revised))

18. An important consideration for the Task Force is the interaction of the concept of qualitative inherent risk factors (QIRFs) in ISA 315 (Revised) with the factors described in the exposure draft of ISA 540,

⁷ ISA 580, *Written Representations*

Auditing Accounting Estimates and Related Disclosures (ED-540) (complexity, the need for the use of judgment by management, and estimation uncertainty). The ISA 315 Task Force met twice with the ISA 540 Task Force to discuss matters of mutual interest, in particular in light of the responses to ED-540. In particular, the Task Forces jointly considered how the QIRFs align with the factors presented in ED-540 and have made changes to align the factors and the terms used to describe them, as presented below. The ISA 315 Task Force has agreed to further consider how it can to make it clearer in ISA 315 (Revised) about how the QIRF's align between ISA 315 (Revised) and ISA 540, by providing relevant examples about the application of the QIRFs to accounting estimates in ISA 315 (Revised) that will demonstrate the alignment of the QIRFs in ISA 315 with those being used in ISA 540. It was also agreed that the ISA 540 Task Force would further consider how they could make stronger links between the factors in ED-540 and the QIRFs.

19. The Task Forces also considered the US Public Company Accounting Oversight Board's (PCAOB) recent Proposed Auditing Standard, *Auditing Accounting Estimates, Including Fair Value Measurements* where risk factors specific to accounting estimates have been proposed that would relate⁸ to the IAASB's proposals for the QIRFs and the factors in ED-540. Notwithstanding that the PCAOB may use these factors for slightly different purposes, the Task Forces agreed that on balance the concepts are broadly aligned conceptually. In further deliberating whether to align the terms between ISA 315, ED-540 and the PCAOB proposals, the Task Force agreed that the concept of subjectivity was broadly the consequence of inherent ambiguity and gives rise to the need for judgment by management. The Task Forces also agreed that estimation uncertainty was a particular class of uncertainty. Accordingly, the ISA 315 Task Force agreed that the term 'ambiguity' should be changed to 'subjectivity.' A comparison of the concepts as used in ED-540 and by the PCAOB in its proposal is presented below:

ISA 315 (Revised)	ED-540 ⁹	PCAOB PROPOSAL
Complexity	Complexity	Complexity (of the process for developing the accounting estimate, and the number and complexity of significant assumptions)
Ambiguity <u>Subjectivity</u>	Judgment <u>Subjectivity</u>	Subjectivity
Change	- ¹⁰	-
Uncertainty	Estimation Uncertainty	Degree of uncertainty of estimates

⁸ AS 2110.60 provides additional risk factors to consider specific to accounting estimates, including uncertainty, complexity, subjectivity and degree of uncertainty.

⁹ See further discussion of the QIRF's used in ED-540 and proposed changes in that project in Agenda Item 2.

¹⁰ In ISA 540, change and the susceptibility to fraud have been recognized as other relevant factors that the auditor may consider in identifying and assessing the risks of material misstatement.

ISA 315 (Revised)	ED-540 ⁹	PCAOB PROPOSAL
Susceptibility to Fraud	.10	-

20. In further considering how to incorporate the QIRFs into the requirements and application material, the Task Force has considered in greater depth what these represent and how they are used in the process of identifying and assessing the risks of material misstatement. In addition, the Task Force has deliberated on how other factors (that affect inherent risk but were not included in the QIRFs) are included in the auditor’s considerations when gathering information and identifying and assessing the risks of material misstatement.
21. In the view of the Task Force, inherent risk factors are characteristics of events and conditions that affect susceptibility to misstatement of an assertion about a class of transactions, account balance or disclosure, before consideration of controls. Inherent risk factors can either be quantitative (numerical) or qualitative. The current definition, and use, of QIRFs does not take account of the quantitative aspects of such events and conditions. Accordingly the definition for QIRFs (and use throughout ISA 315 (Revised)) has been changed to “inherent risk factors” to facilitate the auditor’s consideration of the full range of possible types of inherent risk factors that may be identified as characteristics of events and conditions. New application material to the definition provides further examples of quantitative and qualitative factors. In addition, the Task Force has also revised Appendix 2 that sets out examples of events and conditions that may indicate risks of material misstatement to place these examples in the context of the inherent risk factors. Further consideration will still be given to whether additional matters need to be added to Appendix 2 in ISA 315 (Revised) to better reflect the changes that have been made to the definition of inherent risk factors. In the remainder of this paper we refer to inherent risk factors rather than QIRFs.
22. The Board has also continued to question whether susceptibility to fraud should be described as an inherent risk factor, and the Task Force continued to deliberate this. In particular, concern has been raised that:
- Fraud risk factors relate to both inherent risk and control risk but the inherent risk factors) are required to be used in the identification of inherent risks; and
 - There does not appear to be a clear linkage between susceptibility to fraud as an inherent risk factor and the procedures performed in accordance with ISA 240 to evaluate fraud risk factors in relation to the identification of risks of material misstatement related to fraud.
23. In its deliberations, the Task Force agreed that identified and assessed risks of material misstatement the assertion level include risks due to error and risks due to fraud. In further considering what creates susceptibility to risks due to fraud, the Task Force has agreed that ‘behavioral’ aspects (of those responsible for the preparation of the financial information) should also be considered (the other four QIRFs are attributable to the entity or the nature of the item and do not affect management behavior).
24. In regard to management behavior, the Task Force concluded that an inherent risk factor should capture characteristics of events or conditions relating to classes or transactions, account balances or disclosures that provide an incentive or pressure or an opportunity for intentional *or unintentional* management bias, believing this to be consistent with the concept of inherent risk. Accordingly, the Task Force has agreed that ‘susceptibility to fraud’ should be changed to ‘susceptibility to management bias,’ which broadens the risk factors to incorporate characteristics of events or conditions that interact with management behaviors

that can affect risks of material misstatement due to error or fraud. Further application material has been added to clarify that this inherent risk factor relates to the characteristics of events or conditions that indicate an incentive or pressure, or create an opportunity, for management to not maintain neutrality in preparing financial information. The Task Force is of the view that this factor overlaps and is not conflict in with the use of fraud risk factors, in the context of the fraud triangle, in identifying risks of material misstatement due to fraud.

25. The application material has been updated as enhanced to reflect the matters noted above, and has also been added to clarify that the inherent risk factors do not operate independently but rather interact with one another, for example complexity and subjectivity are strongly influenced by change and uncertainty. The Task Force has also reconsidered how the inherent risk factors have been described in the application material and changes made accordingly.

Relevant Assertions (Definition: paragraph 4(cc) of ISA 315 (Revised))

26. In relation to Board comments regarding the ‘threshold’ for determining relevant assertions, the Task Force agreed that ‘more than a remote likelihood’ may not be appropriately understood as this term is not used in the ISAs, and that it would be better to consider the term ‘reasonable possibility’, (which is also used in US PCAOB Auditing Standard (AS) 2110¹¹ in the context of significant accounts and disclosures.) Accordingly, the definition has been amended to refer to a ‘reasonable possibility’ that a misstatement may be material (which encompasses the likelihood and magnitude of misstatement). Application material has been added to explain what is meant by ‘reasonable possibility.’ The Task Force also made it clear that if it is remote that a misstatement may occur, then the related assertion would not be considered a relevant assertion.
27. In response to December 2017 Board comments, explanatory material has now been elevated into the definition of relevant assertions to clarify the meaning of ‘reasonable possibility.’
28. The Task Force also agreed it would be helpful to emphasize that the determination of a relevant assertion is based on inherent risk (i.e., controls are not taken into account). In light of this addition, and upon further reflection, the Task Force is of the view that the definition of relevant assertion is consistent with that of the PCAOB. The Task Force believes that the difference in wording between the proposed ISA 315 (Revised) definition and the corresponding PCAOB definition is useful to draw out the relationship between a relevant assertion and a significant class of transactions, account balance or disclosure.

Significant Class of Transactions, Account Balance or Disclosure (Definition: paragraph 4(da) of ISA 315 (Revised))

29. The Task Force agreed with Board comments encouraging the Task Force to consider consistency of terms used by other standard setters for similar concepts, and has changed ‘relevant’ class of transactions, account balance or disclosure to ‘significant’ class of transactions, account balance or disclosure.

¹¹ AS 2210, *Identifying and Assessing the Risks of Material Misstatement*

Significant Risks (Definition: paragraph 4(e) of ISA 315 (Revised); Application Material – paragraph A0h of ISA 315 (Revised))

30. In light of the discussion related to ED-540 and the ‘spectrum of risk,’ the Task Force agreed that a risk is assessed as ‘significant’ when it is at the highest end of the spectrum of inherent risk. Accordingly, the Task Force has revised the definition of significant risk to acknowledge this point.
31. The ISA 315 Task Force has also been coordinating with the ISA 540 Task Force on the changes being made in ISA 315 (Revised), so that material being developed in ISA 315 (Revised) to support the spectrum of inherent risk concept would also prospectively support the changes being proposed in ISA 540. The ISA 315 Task Force agreed to further progress its concept of the spectrum of inherent risk such that the 540 Task Force can consider how best to incorporate it in ISA 540 to replace the low/not low risk thresholds and in order to recognize how scalability can be demonstrated in identifying, assessing and responding to the risks of material misstatement at the assertion level for accounting estimates.
32. The definition of significant risk has also been amended to clarify that the inherent risk factors affect the likelihood of a misstatement occurring as well as the potential magnitude of that misstatement. This brings consistency with the revised requirement that addresses the auditor’s assessment of inherent risk in paragraph 26 of ISA 315 (Revised).

Requirements—Risk Assessment Procedures and Related Activities (Requirements: paragraphs 5–10 of ISA 315 (Revised); Application Material – paragraphs A1–A24 of ISA 315 (Revised))

Task Force Views on the Proposed Changes to the Requirements

33. The Task Force has further considered the use of the phrase of ‘sufficient and appropriate’ throughout the proposals made in December 2017 in light of Board concerns about the use of these terms. The Task Force continues to have the view that it is important in paragraph 5, which described the various aspects of obtaining an understanding, to clarify why this understanding is obtained. In further considering the ‘why,’ the Task Force agreed that the purpose of obtaining the required understanding of the various aspects is to provide sufficient appropriate audit evidence for the identification and assessment of risks. This further confirms that risk assessment procedures performed provide audit evidence, which is consistent with ISA 500,¹² which has been highlighted in the application material.
34. Further to this change, the Task Force also amended the requirement in paragraph 9 that addresses the use of audit evidence from prior periods to emphasize that the auditor needs to evaluate whether such evidence remains relevant and reliable to be used as audit evidence in the audit for the current period.
35. With regard to the application material, the Task Force has:
 - Highlighted the iterative nature of the risk identification and assessment process.
 - Highlighted that the depth of understanding required will vary according to the nature and circumstances of the entity.
 - Clarified the various sources of information available to the auditor, including data provided by the entity.

¹² ISA 500, *Audit Evidence*, paragraph A10 states that audit evidence is obtained... from performing risk assessment procedures; and further audit procedures...

- Provided further guidance about the auditor’s considerations about information obtained from client acceptance and continuance, and other engagements performed for the entity being audited, in relation to the identification and assessment of risks of material misstatement.
36. To focus the engagement team on the importance of appropriately exercising professional skepticism during the risk identification and assessment process, application material has been developed relating to the identification and further consideration of inconsistent or contradictory information during the engagement team discussion (see paragraph A21a of ISA 315 (Revised) in **Agenda Item G.3**). The application material also emphasizes the importance of a robust understanding to be able to appropriately undertake the risk identification and assessment process, and the importance of the engagement team discussion in this regard.
37. Further explanation about the use of automated tools and techniques can be found in paragraphs 70–72 of this paper.

The Understanding of the Entity and Its Environment, and the Applicable Financial Reporting Framework (Requirements: paragraphs 11–11A of ISA 315 (Revised); Application Material – paragraphs A24a–A49f of ISA 315 (Revised))

38. To respond to Board comments from the September and October 2017 Board meetings, the Task Force has made changes to paragraph 11 of ISA 315 (Revised) as follows:
- To focus the auditor’s consideration of internal and external measures used by the entity on those that are ‘relevant’, it is limited to those measures that are relevant to the audit from the perspective of the auditor’s identification and assessment of risks of material misstatement. The application material has also been revised, as appropriate, to make clear the kinds of information that would only be relevant to listed entities.
 - Added back organizational structure, ownership and governance to the requirement so as not to lose the robustness of the auditor’s required understanding in these areas.
 - Developed application material to explain what a ‘business model’ is, including the types of matters the auditor may want to understand.
39. The Task Force has also:
- Restructured the requirement that focuses on the auditor’s understanding of the applicable financial reporting framework to clarify the context of the understanding, and enhanced this requirement to also include understanding the reasons for changes to the entity’s accounting policies, (included in the extant requirement and which the Task Force believes is an important aspect to the auditor’s understanding).
 - Added that the required understanding needs to be “appropriate’ to enable the auditor to be able to understand the classes of transactions, account balances and disclosures to be expected in the financial statements.
40. To respond to Board comments from the December 2017 Board meeting, the Task Force has made changes to paragraph 11 of ISA 315 (Revised) as follows:
- Restructured the paragraph to make clear that the understanding is obtained to provide an appropriate basis for the auditor to understand the classes of transactions, account balances and disclosures to be expected in the financial statements.

- Clarified that the understanding required of the applicable financial reporting framework, and of changes to accounting policies, is in the context of the nature and circumstances of the entity and its environment.
 - Clarified how the inherent risk factors are addressed when obtaining an understanding of the entity and its environment and the applicable financial reporting framework. In December 2017 this was presented as a separate sentence at the end of the requirement but concern was expressed that it was not clear what needed to be done. In the view of the Task Force, the auditor considers the characteristics of events and conditions (i.e., the inherent risk factors) as the understanding of the entity and its environment and of those events and conditions is obtained in conjunction with the auditor's consideration of how the requirements of the applicable financial reporting framework apply in that context. Understanding how the inherent risk factors affect the susceptibility of an assertion to misstatement enables the auditor to consider which assertions about which classes of transactions, account balances or disclosures may be subject to potential risks of material misstatement, and to help identify and assess the risks of material misstatement. Accordingly, the auditor's consideration of the applicable financial reporting framework has been enhanced to take into account events or conditions that may indicate risks of material misstatement and how such events or conditions are subject to, or affected by, the inherent risk factors.
41. In relation to the application material, the Task Force has:
- Explained the importance of the inherent risk factors in the auditor's understanding.
 - Built in a challenging mindset by the auditor as they are obtaining their understanding, thereby promoting professional skepticism.
 - Fully explained those aspects of the business model and business risks that are relevant for the auditor.
 - Restructured the existing content in the extant ISA 315 (Revised) for the auditor's understanding of the applicable financial reporting framework as set out in the revised requirement in paragraph 11(b) of ISA 315 (Revised).
 - Moved certain matters related to the auditor's understanding of the entity and its environment to a new appendix (Appendix 1 of ISA 315 (Revised)) consistent with its December 2017 proposals.
 - Provided further guidance about the depth and breadth of understanding required, as well as provide context for why the understanding is obtained (i.e., to help the auditor develop expectations for the identification of potential risks of material misstatement).
42. Further explanation about the use of automated tools and techniques when obtaining an understanding of the entity and its environment can be found in paragraph 70–72 of this paper.

The Required Understanding of the Entity's Internal Control (Requirements: paragraphs 12–21B of ISA 315 (Revised); Application Material – paragraphs A50–A109g of ISA 315 (Revised))

Task Force Views on Proposed Changes

43. The Task Force has further deliberated, and changes have been made in, the requirements that address each of the components of internal control to address the Board's concerns of that the revisions proposed in the September 2017 Agenda Papers were overly focused on identification of relevant controls and not sufficiently focused on requiring an understanding the components. The Task Force extensively debated

the nature of each component of internal control over financial reporting, and proposed changes to the requirements and application material to more clearly set out the understanding required by the auditor in relation to each component for the purpose of the audit. In doing so, the Task Force separated the ‘understanding’ required from the identification of ‘controls relevant to the audit,’ as some components may not necessarily have controls that are relevant to the audit.

44. Proposals for changes to ISA 315 (Revised) require the auditor to identify the risks of material misstatement at the financial statement level, and at the assertion level for significant classes of transactions, account balances and disclosures and assess those risks by assessing inherent risk and control risk. The auditor’s understanding of internal control over financial reporting provides the basis for the required risk assessments, and is obtained through understanding the five components of internal control. Although an understanding of each component is required, ‘controls relevant to the audit’ has been clarified to be those controls that meet the criteria in paragraph 20 in ISA 315 (Revised) and that either directly address, or assist in addressing, the risks of material misstatement at the assertion level.

Understanding the System of Internal Control

45. Changes have been made to paragraph 12 of ISA 315 (Revised), which provides the set-up for the understanding to be obtained relating to each component of internal control to further clarify which paragraphs achieve ‘understanding each component.’ The Task Force has also agreed to not change the current understanding of the system of internal control as it relates to ‘financial reporting’ to ‘financial reporting objectives,’ as this may have unintended consequences.
46. In relation to each of the components of internal control, the following additional changes to the requirements proposed for the September 2017 IAASB discussion have been made:
- *Control environment*—matters required to be understood in relation to this component have been elevated from Appendix 1 of extant ISA 315 (Revised), and updated for consistency with the principles for this component set out in COSO Framework 2013,¹³ to help auditors identify what needs to be understood in relation to the control environment, and evaluate whether these aspects provide an appropriate foundation for the other components of internal control. The requirement for further consideration of any deficiencies identified and whether these deficiencies result in a significant deficiency, including the impact on the audit, has now been separated as a new, distinct requirement.
 - *The Entity’s Risk Assessment Process*—this component has been rearticulated to recognize that consideration should still be given to how management or those charged with governance identify and address risks in the absence of a formal risk assessment process. The Task Force is of the view that, absent a formal process, a risk assessment would be undertaken in most entities to some extent, and the auditor should still understand what management does in such cases. The specific matters that the auditor should obtain an understanding of have been articulated, therefore whether there is a formal process or not, it is clear the types of matters that need to be considered relating to this component. In addition, the proposed requirement to consider the appropriateness of the risk assessment process, or the absence thereof, in light of the nature and size of the entity has been broadened to all entities and not only those without a formalized process.

¹³ The Committee of Sponsoring Organizations of the Treadway Commission’s (COSO) *Internal Control – Integrated Framework (2013)*

- *The Information System and Communication*—changes have been made to focus on the flow of information through the information system from initiation of a transaction to the preparation of the financial statements, including the related accounting records and documents. Also, it has been clarified that the significant classes of transactions, account balances and disclosures are used in determining the scope of the understanding required. In response to Board comments in October 2017 related to the proposals for revisions in respect of IT, the Task Force considered how to appropriately set boundaries for the understanding of the entity's use of IT, particularly as it relates to the information system. Accordingly, a new requirement in 18(d) has been proposed for the auditor to identify the entity's IT environment including IT applications and underlying IT infrastructure to the extent it is relevant to the aspects of the information system that are required to be understood in paragraph 18(a)-(c). No significant changes have been made to the 'communication' requirement.
 - *Control Activities*—The Task Force is of the view that an understanding of the control activities component is achieved through the identification of controls relevant to the audit, and the evaluation of the design and implementation of such controls. The Task Force has further clarified its thinking related to the understanding of the component. It is the view of the Task Force that, because this component primarily comprises controls over the information system (including application controls and general IT controls), the understanding of the control activities component is captured in the auditor's process to identify the controls relevant to the audit within the component and to evaluate their design and implementation. Paragraph 19A has been updated accordingly to clarify this thinking. With regard to the types of controls in the control activities component, these have been relocated to the application material to provide supporting guidance on the types of controls that may exist and to inform the auditor's identification of those relevant to the audit. The Task Force will continue to consider how this guidance corresponds to the categories of controls set out in other frameworks.¹⁴
47. The Task Force has also abbreviated the name of the "Information System, Including Related Business Processes, and Communication" component to the "Information System and Communication" component as this still reflects the nature of the component but is easier to use for reference purposes throughout the standard. The related business processes still form part of this component, which is made clear in both the specific requirement in paragraph 18 of ISA 315 (Revised) and the related application material (in paragraph A90a of ISA 315 (Revised)).

Controls Relevant to the Audit

48. The Task Force has clarified that "obtaining an understanding of internal control relevant to the audit" (as per extant paragraph 12) has been replaced with the above requirements to understand each of the components of internal control to the extent specified, to identify controls relevant to the audit and evaluate the design of the controls and determine whether the controls have been implemented (D&I), based on a clarification of the concept of controls relevant to the audit. Changes that have been made to explain and clarify what the auditor the auditor is required to do to understand each component of internal control are described above, and the Task Force has also clarified the concept of "controls relevant to the audit" as follows:

¹⁴ For example, the COSO Framework 2013 sets out the types of controls in this component as including authorizations and approvals, verifications, physical controls, controls over standing data, reconciliations and supervisory controls.

- In the view of the Task Force, controls within the *control environment*, *the entity's risk assessment process*, and *the entity's process to monitor the system of internal control* components are typically more 'indirect' in nature (i.e., controls that do not directly impact an assertion related to a class of transactions, account balance or disclosure). Such indirect controls are more likely to affect the auditor's risk assessment at the financial statement level. However, there may be instances where controls in these components address risks directly at the assertion level. For example a monitoring activity relating to a control over a specific account balance, in which case these controls may be identified by the auditor as 'relevant to the audit' (see below for the implications of determination).
- The *information system and communication* component addresses the flow of information relevant to financial reporting from initiation of a transaction (or occurrence of an event or change in a condition) through the capture of that information, its processing and transfer to the general ledger and its inclusion in the financial statements. Information is relevant to financial reporting if it is relevant to the recognition, measurement, presentation or disclosure of significant classes of transactions, account balances or disclosures. Controls within this component are the policies and procedures that define those flows in a manner that results in financial statements that meet the requirements of the applicable financial reporting framework. Therefore the changes to the standard and restructuring of the application material (paragraphs A96a to A96d of ISA 315 (Revised)) that are proposed are intended to clarify what comprises, and how to obtain, the required understanding of those controls. In particular, application material has been added to explain that the auditor:
 - Obtains understanding of the flows of information and the related accounts and records that comprise the information system relevant to financial reporting, as designed or operated in practice, and
 - Evaluates their design effectiveness and confirms that the auditor's understanding reflects how they have been placed into operation.

This confirmation may be obtained through tracing information about transactions, other events or conditions, through the processes, records or accounts designed or operated in practice, to confirm that understanding (e.g., by performing a walk-through).

- Controls in the *control activities* component, and controls in other components in certain circumstances, are relevant to the audit if they are:
 - Required to be identified as relevant to the audit (i.e., because the standard requires the controls to be identified as relevant—see paragraph 20 in ISA 315 (Revised)); or
 - General IT controls, in the circumstances described by paragraph 21A of ISA 315 (Revised).
49. For each control identified as a control relevant to the audit, the auditor continues to be required to evaluate the D&I.
50. In relation to general IT controls, in addition to changes presented to the Board in October 2017, a link has been made to the auditor's understanding of matters related to IT that has been obtained in understanding the five components of internal control in order to identify risks related to IT. In addition, if general IT controls are determined to be relevant to the audit based on the revised requirement, this is also scoped in to the requirement to perform D&I.

51. In response to December 2017 Board comments for the Task Force to consider the appropriate placement of the requirements related to the auditor's identification of controls relevant to the audit and the evaluation of the design and implementation of the controls, the Task Force has:
- Created a separate section that addresses "Controls Relevant to the Audit", that includes paragraphs 20-21B.
 - Added Paragraph 13 to highlight that the performance of the requirements in the "Controls Relevant to the Audit" section are necessary to the auditor's understanding of the system of internal control (i.e., paragraph 13 together with paragraph 12 highlight all requirements that comprise the auditor's understanding of the system of internal control).
52. The Task Force has further considered how any identified deficiencies for each of the indirect aspects (i.e., the control environment, risk assessment process and monitoring process) should be considered and aligned the respective requirements in each component accordingly. The articulation of the relevant requirements have also been made consistent with the way the requirements are set up in ISA 265.¹⁵
53. With regard to understanding the entity's risk assessment and monitoring processes, the Task Force continues to believe that it is important to understand these processes, even if they are not formalized. In particular, in smaller entities management may have less formalized processes in place to consider how the entity's risks may identified and addressed, and controls and processes monitored. However, concern had been expressed by the Board about how this had been expressed in the draft discussed in December 2017. Changes have therefore been made to focus on the nature of the processes, including the formality of such processes, and the application material further enhanced in order to evaluate whether the entity's processes are appropriate to the nature, size and circumstances of the entity (highlighting that there may be less formality in the case of smaller, non-complex entities).
54. The Task Force has clarified certain aspects of obtaining an understanding of the information system, including:
- Clearly separating the requirement to understand the flow of transactions and information in paragraph 18(a), from the requirement to understand the accounting and other supporting records in paragraph 18(b).
 - Clarifying the requirement in paragraph 18(d) to be an understanding of the IT environment, which includes the understanding of the IT applications and underlying IT infrastructure. Clarifications have also been made in the application material.
 - Introducing a requirement in paragraph 18A to evaluate the design of the information system and to determine whether it has been placed in operation. This requirement recognizes that evaluating the design and implementation of the policies and procedures that define the flows of information and the financial reporting process within the information system, should be differentiated from the evaluation in paragraph 21B of individual controls, primarily controls over the information system, that are identified as relevant to the audit.. Application material has been added to address techniques for performing this evaluation (for example, by undertaking a walk-through or using automated techniques).

¹⁵ ISA 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*

55. With regard to the requirements within the newly created 'controls relevant to the audit' section, the Task Force has:
- Updated the application material to support each of the requirements in paragraph 20. Ongoing coordination with the ISA 540 Task Force will assist in determining the need for any further guidance related to accounting estimates.
 - Reinstated and updated the extant requirement related to understanding risks arising from the entity's use of IT. The Task Force has done so taking into consideration the December 2017 Board comments that greater clarity and supporting guidance were needed related to the condition in the proposed requirement to identify general IT controls relevant to the audit (i.e., "based on the auditor's understanding of the risks related to IT"). Upon reflection, the Task Force believes a discrete requirement to identify the risks arising from IT may assist in addressing scalability in the auditor's identification of general IT controls; this requirement can facilitate a risk-based approach based on the nature and complexity of the entity's IT environment. For example, for small entities with unmodified packaged software, the risks arising from IT may be acceptably low, in which case there may not be general IT controls relevant to the audit, particularly when the auditor does not intend to test the operating effectiveness of any application controls.
 - Clarified the requirement in paragraph 21B to evaluate the design and implementation of controls relevant to the audit, in particular to clarify the meaning of "relating controls to what could go wrong at the assertion level." The Task Force is of the view that this requirement involves mapping the individual controls relevant to the audit to the potential risks of material misstatement that each control was designed to address, and that this exercise supports the auditor's ability to evaluate the design of the control in the context of the related risks. Accordingly the term "what could go wrong" has been replaced with "potential risks of material misstatement."
56. The Task Force has reinstated the explicit requirement for the identification of risks arising from IT in paragraph 21. If the Board is supportive of the Task Force direction, the Task Force will seek to provide supporting application material with a focus on scalability. In addition, the Task Force plans to develop application material, using the assistance of an IT audit specialist, for each of the criteria that drive general IT controls relevant to the audit in paragraph 21A.
57. Changes have also been made to the application material as follows:
- The description about 'limitations of internal control' and various other matters related to the components of internal control have been moved a new appendix in line with the December 2017 Task Force proposal to do so (Appendix 3 in ISA 315 (Revised) related to understanding the entity's internal control).
 - Enhancements have been made to the application material relating to the control environment to emphasize that deficiencies in the control environment may lead to risks of material misstatement at the financial statement level.
 - Some additional guidance has been added relating to the auditor's understanding of IT. As noted above, the Task Force intends to pursue the development of further guidance in support of the requirements in paragraph 21 and 21A.

- Application material has been added to clarify the reasons for the auditor's evaluation of the design and implementation of controls relevant to the audit. This includes the influence of these procedures on the auditor's identification and assessment of risks of material misstatement, including as well as on the design and performance of further audit procedures.

Identifying and Assessing the Risks of Material Misstatement (Requirements: paragraphs 25–31 of ISA 315 (Revised); Application Material – paragraphs A121A–A151 of ISA 315 (Revised))

Task Force Views on the Proposed Changes to the Requirements

58. In light of the new concepts being introduced, the Task Force continues to work through the process to identify and assess the risks of material misstatement, in particular how to articulate this process within the standard so that it is able to be effectively applied by auditors from different sized firms, and so that there is a more consistent approach to identifying and assessing risks, in particular significant risks. The Task Force will also continue to consider application material as appropriate to support the revised requirements.
59. Paragraphs 25 through 26 of Agenda Item G.2 set out the Task Force's view about how the process of identifying and assessing risks of material misstatement may flow. In particular, the Task Force believes that based on the information gathered in understanding the entity, the auditor makes a 'preliminary' identification of significant classes of transactions, account balances and disclosures, which is required to be made before consideration of any controls, and iteratively seeks to confirm this initial identification as the process proceeds. Application material has been added to further explain the flow, including how the inherent risk factors impact the assessment of risks. Also, further application material has been developed to assist with the determination of significant risks (i.e., those risks on the highest end of the spectrum of inherent risk).
60. In relation to the assessment of control risk, a stronger link back to the work performed in relation to D&I has been made, with enhanced application material to further explain how the D&I work interacts with the auditor's assessment of control risk. The Task Force has also simplified the requirement to make clear that if the auditor is not intending, or not required to test the operating effectiveness of controls, that control risk will be assessed as maximum. This allows auditors who intend to perform a primarily substantive audit not to have anything further to do in relation to controls (although it is likely to impact the nature and extent of substantive procedures to be performed).
61. The Task Force has continued to deliberate the requirement in ISA 330, paragraph 18 to design and perform substantive procedures on material balances irrespective of the assessment of the risk of material misstatement. The Task Force continues to consider how this interacts with the new requirement for the auditor to identify the significant classes of transactions, account balances and disclosures, and their relevant assertions. In the view of the Task Force, the concept of 'materiality' relates to the information needs of users. The concept of 'significance' relates to the risks. For classes of transactions, account balances and disclosures that are identified as 'significant,' these would always be material as they are linked to 'relevant assertions' which, by definition, means there is more than a remote possibility (before consideration of controls) of a misstatement that is material. In such cases, the auditor would already be required to identify and assess the risks at the assertion level related to these significant classes of transactions, account balances or disclosures, and respond accordingly in accordance with paragraphs 7 and 8 of ISA 330.
62. The Task Force also agreed that there could be some (likely rare) cases where a class of transactions, account balance or disclosure could be material but was not identified as significant, and therefore that

there would not automatically be a requirement to perform further audit procedures. However, because of the amounts reported are material, the Task Force believes that the auditor should perform further audit procedures to address ‘what could go wrong’ in relation to assertions about classes of transactions, account balances or disclosures. Identifying what could go wrong would also assist the auditor with focusing on appropriate further audit procedures. Accordingly, the Task Force has agreed that the current requirement in ISA 330, paragraph 18, should therefore remain, subject to proposed changes as follows:

ISA 330: <i>The Auditor’s Responses to Assessed Risks</i>
<p>Requirements:</p> <p>18. Irrespective of the assessed risks of material misstatement, the auditor shall design and perform substantive procedures for each class of transactions, account balance, and disclosure <u>that is quantitatively or qualitatively material</u>. (Ref: Para. A42–A47)</p>

63. In considering these matters, the Task Force also agreed that ISA 315 (Revised) should facilitate the auditor’s identification of classes of transactions, account balances and disclosures that are quantitatively or qualitatively material but have not been identified as significant. Accordingly, a new requirement has been added to require the auditor to identify these and reconfirm that there are no relevant assertions for these classes of transactions, account balances or disclosures. In the view of the Task Force, this will also help make the link to ISA 330 paragraph 18.
64. With regard to the application material for ISA 330, paragraph 18, the Task Force will consider whether other changes are needed in light of Board discussions on matters set out in paragraphs 61 to 63 above.
65. To support the revised requirements for the identification of inherent risk and the separate assessment of inherent and control risk, application material has been enhanced as follows:
- To further explain how considerations about the auditor’s understanding of the control environment impacts the auditor’s risk assessment at the financial statement level, and the potential implications for the audit.
 - Application material to support the process to identify relevant assertions, and significant classes of transactions, account balances and disclosures has been added, including how this feeds into the auditor’s identification and assessment of inherent risks.
 - Explaining how the auditor further considers the likelihood and magnitude of possible misstatements, and that the risk exists on a spectrum of inherent risk. The application material also explains that auditors may use different categorizations on the spectrum of inherent risk; however any further audit procedures to address identified risks need to be responsive to those risks. In the view of the Task Force, explaining the ‘spectrum’ of risk will help explain the interrelationship between significant and ‘low’ risk, and may help support the use of these terms in other ISAs.
 - Making clear that significant risks are at the highest end of the spectrum of inherent risk.
 - Further explaining what the consequences of identifying a risk as significant on the audit are, by setting out the possible implications for the audit.
 - Application material to assist the auditor in assessing control risk, including emphasizing that, if the auditor has not tested controls related to risks, the control risk remains at maximum.

- Clarifying when general IT controls may be relevant to the audit (taking into consideration the risks related to IT), and therefore when evaluation of their D&I is required, and explaining how the expected operating effectiveness of general IT controls factors into the assessment of control risk.

Risks for Which Substantive Procedures Alone Do Not Provide Sufficient Appropriate Audit Evidence
(Requirements: paragraph 30 of ISA 315 (Revised); Application Material – paragraphs A148–A150 of ISA 315 (Revised))

66. The Task Force has revised the requirement such that the auditor is required to determine whether any risks exist for which substantive procedures alone would not provide sufficient appropriate audit evidence, to make it an active requirement instead of the extant passive consideration of such risks. The requirement has also been positioned prior to the auditor’s consideration of control risk, as this determination would need to be made prior to assessing control risk. The ISA 315 Task Force will also continue to work with the ISA 540 Task Force on the examples to be developed as respondents to ED-540 have highlighted various aspects related to this requirement in the responses to ED-540.

Scalability of ISA 315 (Revised)

67. The Task Force continues to consider how to make the standard scalable to a wide variety of entities, all with different circumstances and complexities, while keeping the standard principles-based and able to be effectively implemented.
68. The Task Force has agreed (as with other IAASB projects currently underway) that scalability applies to all sized entities. It is the level of complexity in the nature of the entity and its financial reporting that is the driver of scalability. For example, there may be small entities that have complexities in their business model or their financial reporting, and may therefore require a more robust risk assessment process. Accordingly, and based on direction received from the Board in the December meeting, the Task Force has removed the “Considerations specific to smaller entities” throughout the standard. However, many of the matters previously in these sections have been retained and built into the text of the standard as appropriate. In doing so, the Task Force has introduced contrasting examples in certain cases for larger or more complex entities. In addition, as the Task Force has been developing new, and enhancing, application material, it has been mindful of providing scalability aspects as appropriate. The Task Force plans to continue to identify areas of the application material where scalability guidance can be included, particularly as it relates to an entity’s use of IT and the effect on general IT controls relevant to the audit.
69. The following sets out the paragraphs where the Task Force has the view that scalability has been included:

Agenda Item G.2: Paragraph reference and summary of content (Introductory paragraphs)	
1H – 1I	Emphasizing that the size and complexity of the entity may affect the risks of material misstatement and the controls necessary to address those risks.
Agenda Item G.3: Paragraph reference and summary of content (Application material)	
A24a	Describing the depth of the auditor’s required understanding of the entity and its environment – this will vary according to the nature and circumstances of the entity.

A16	<p>Explaining how analytical procedures as a risk assessment tool are scalable:</p> <ul style="list-style-type: none"> - For a less complex entity, the auditor may use a simple spreadsheet to compare information from an interim or month end period with balances from prior periods. - For a more complex entity, the auditor may extract data from the entity's information system, and further analyze this data by using visualization techniques.
A24	Providing guidance where an engagement team discussion may not be possible, for example, where an engagement is carried out by a single partner.
A31	Emphasizing that the auditor's understanding of the entity's organizational structure and ownership is dependent on the particular circumstances.
A31d, A49f	Providing guidance on the consideration of an entity's objectives, strategy or business model for smaller or less complex entities.
A50a, A53	Clarifying that the way in which internal control is designed, implemented and maintained, varies with an entity's size and complexity.
A80a	Explaining the nature of the control environment within smaller entities, and the possible consequences for the auditor.
A80 b–c	Describing the nature of audit evidence for elements of the control environment in smaller entities.
A89	Clarifying that smaller or less complex entities may not have established a formal risk assessment process, and the consequences for the auditor.
A89 b–d	Highlighting that the evaluation of the appropriateness of the entity's risk assessment process is a matter of judgment based the nature, size and complexity of the entity and that the absence of an established risk assessment process may be appropriate, depending on the circumstances.
A89j	Clarifying that in smaller entities, management's monitoring of control is often accomplished by the owner-manager's close involvement in operations and there may not be any other monitoring activities.
A89k	Emphasizing that even for some larger entities, there may not be a distinct process for monitoring the system of internal control.
A99i	Explaining that smaller entities may be limited in the extent to which segregation of duties is practicable, and the consequences thereof.
A90c, A92c	Describing the nature of the required understanding of the information system, and related business processes relevant to financial reporting, in smaller entities.

A97	Clarifying that the communication of financial reporting roles and responsibilities within smaller entities may be less structured and formal.
A99 a–b	Explaining the nature and extent of control activities in smaller entities
A125d	Acknowledging that, in relation to audits of smaller, non-complex entities, a greater proportion of assessed risks are likely to be at the lower end of the spectrum of inherent risk.
A150 a–b	A reminder that the control risk assessment remains at the maximum level when the auditor does not intend to test the operating effectiveness of controls that address the assessed inherent risks.
A153	Emphasizing that the nature and extent of audit documentation may differ for entities with non-complex businesses and processes relevant to financial reporting.

Data Analytics

70. The Task Force has, and will continue to, consider how the evolving use of automated tools and techniques could be presented in ISA 315 (Revised) to better reflect current practice for using these tools and techniques in identifying and assessing the risks of material misstatement. In working with the Data Analytics Working Group (DAWG) on relevant guidance and examples to be included, the Task Force has remained mindful of focusing on the use of data analytics as it relates to ISA 315 (Revised). The DAWG will continue to further explore other data analytics matters which have broader implications for ISAs than just ISA 315 (Revised).
71. For the purposes of ISA 315 (Revised), the DAWG has worked with the ISA 315 Task Force on application material to be included in the ISA 315 (Revised) Exposure Draft that relates to the use of data analytics in the risk assessment process. Examples and other application material related to Data Analytics were discussed by the ISA 315 Task Force at its January meeting. During this meeting the following paragraphs were identified and content specific to data analytics have been included in the application material of ISA 315 (Revised):

Agenda Item G.3: Paragraph reference and summary of content (Application material)	
A2	Emphasizing that technology may be used on large volumes of data, which may result in evidence that informs the identification and assessment of risks of material misstatement.
A4b	Clarifying that the auditor may use automated tools and techniques, including for analysis, recalculations, re-performance or reconciliations.
A16 & A31a	Describing how automated tools or visualization techniques may be used as risk assessment procedures.
A96b	Explaining the option to use automated techniques to assist in confirming that the information system has been placed into operation.

A100g	Describing that automated tools may be used to understand the nature and extent of journal entries
A150g	Clarifying that automated techniques may be used to confirm whether all significant classes of transactions and account balances have been identified by, for example, analyzing types of transactions and their volume.

72. The ISA 315 Task Force plans to work with the DAWG to obtain their insights on further enhancements to these examples, or opportunities for other examples in the application material, prior to June 2018.

Appendices to ISA 315 (Revised)

73. New appendices have been developed or updated as explained in this paper:

- Appendix 1 (NEW)—*Considerations for understanding the Entity and Its Business Model*. Matters previously located in the application material have been relocated consistent with its proposals at the December 2017 meeting where the Task Force expressed the view that these matters are not critical to the auditor’s understanding, but are still helpful.
- Appendix 2—*Events and Conditions That May Indicate Risks of Material Misstatement*. Existing material in Appendix 2 has been enhanced to categorize the events and conditions by the inherent risk factors.
- Appendix 3—*Understanding the Entity’s System of Internal Control*. Existing material in extant Appendix 1 has been relocated and updated and enhanced as appropriate to reflect Task Force discussions about changes that may be needed, as well as changes to reflect updates made to COSO Framework 2013. A section within the extant application material relating to ‘limitations of internal; control’ has also been relocated as in the Task Force’s view this is not critical understanding but is still helpful context.

Matters for IAASB CAG Consideration

1. CAG Representatives are asked for their views on:
 - (a) The new introductory paragraphs (paragraphs **1A–1K** in **Agenda Item G.2** and explained in paragraphs **9–11** above)—Do these paragraphs help provide context for the identification and assessment of the risks of material misstatement? Are there any other aspects to be included that may provide further context?
 - (b) Whether the revisions to obtaining an understanding of internal control (see **Agenda Item G.2** paragraphs **12–21B** and relevant explanation in paragraphs **43–57** above) assist with understanding the work effort in order to obtain an understanding of the entity’s system of internal control?
 - (c) Scalability as described in paragraphs **67–69** above – are there other areas where the Task Force should further consider scalability?

Task Force Activities Including Outreach and Coordination with Other IAASB Task Forces and Working Groups

1. The following sets out the activities of the Task Force including outreach with others and coordination with other IAASB Task Forces and Working Groups relating to the ISA 315 (Revised) project since December 2017. Further information about the project, including the members of the Task Force, can be found [here](#).

Task Force Activities since the December 2017 IAASB Discussion

2. The ISA 315 Task Force has met once in person, held one teleconference and one video conference since the last IAASB discussion in December 2017.

Outreach with Audit Inspection Bodies

3. Representatives from the ISA 315 Task Force, including the Chair, held a teleconference with representatives of the International Forum of Independent Audit Regulators' (IFIAR) Standards Coordination Working Group (SWCG) (including the Chair) to discuss the progress of the project and to address questions from representatives from IFIAR's SCWG.

Coordination with Other IAASB Task Forces and Working Groups

4. Representatives from the ISA 315 Task Force, including the Chair, held a teleconference with representatives of the Data Analytics Working Group (DAWG) to discuss the integration of the use of automated tools and techniques into the revisions of the application material of ISA 315 (Revised), and in particular, the use of technology as a means to perform risk assessment procedures.
5. The Chair of the Task Force and Staff held a teleconference with the Chairs of the ISA 540 Task Force and Staff to discuss matters that crossover both projects, in particular with regard to the consistency in approach and terms that are used in light of changes that are being made to both standards (see paragraph 5 of this paper).

IAASB OCTOBER AGENDA PAPER – INFORMATION TECHNOLOGY
(FOR INFORMATION PURPOSES)

Introduction and Background

1. ISA 315 (Revised) requires the auditor to identify and assess the risks of material misstatement (ROMM's) through risk assessment procedures. Most entities have an IT system in place for recording and processing financial information. These systems may range from non-customized off-the-shelf packages to highly customized and highly-integrated systems.
2. The overall objective and scope of an audit does not differ whether the entity operates in an entirely manual environment, a completely automated environment, or an environment involving some combination of manual and automated elements. However, an entity's use of IT affects the manner in which financial information is processed, stored and communicated and therefore affects the entity's information system and the manner in which the entity implements internal control relevant to financial reporting. At the March 2017 IAASB meeting, a brief introduction to IT in ISA 315 (Revised) was provided (see Appendix 2), but there have been no further Board discussions regarding changes relating to IT
3. Accordingly, the rest of this paper focuses on how ISA 315 (Revised) can be enhanced with regard to the entity's use of IT and the auditor's considerations when understanding the entity and its environment, the applicable financial reporting framework and internal control, and identifying and assessing the risks of material misstatement (ROMMs).
4. The Task Force has been working with a firm IT expert in developing its proposals.

Format of the Papers

5. This paper sets out the Task Force's initial views on changes to the auditor's understanding of each of the components of internal control. However, detailed drafting changes have not been presented (other than to certain definitions as explained later in this paper) as the Task Force is still deliberating the changes needed. This explanation has been provided as context for some of the changes relating to the auditor's considerations about IT that have been presented.
6. This paper then explains the changes that are being proposed and sets out the Task Force's views on IT-related matters.
7. **Agenda Item 5-B** sets out:
 - (a) Revised changes to the definitions relating to the system of internal control and controls, mainly to obtain views about whether the revised definition of controls addresses the concerns expressed by the Board in its discussions in September 2017. The Task Force was of the view that these changes were integral to some of the changes proposed relating to IT and have therefore progressed the changes relating to the definition of controls.
 - (b) The proposed changes to the existing requirements in ISA 315 (Revised), and proposed new or enhanced application material, for auditor considerations relating to IT. Application material in extant ISA 315 (Revised) has not been presented as no further changes to the existing application and other explanatory material have been considered by the Task Force—changes to all existing application material will be presented to the Board for discussion in December 2017. The new application material presented for discussion in **Agenda Item 5-B** is indicative of those areas

where the Task Force believes additional guidance is needed, and is looking for the Board's views on these matters. However, further refinement of the drafting of these paragraphs as application and other explanatory material may be needed.

Agenda Item 5-B does not reflect other changes to address issues and concerns from the September 2017 IAASB discussions, with areas not for discussion being unchanged from September 2017 (and greyed out in Agenda Item 5-B). In addition, the proposed changes relate to considerations about the entity's use of IT and the auditor's considerations thereof, and do not address matters related to the auditor's use of data analytics tools and techniques (these will be addressed in December 2017).

8. In developing changes to ISA 315 (Revised), including enhancing the auditor's considerations about IT, the Task Force is still working through broader revisions and enhancements to the application material, including:
 - Whether changes are needed to Appendix 1 of ISA 315 (Revised), which further explains the components of internal control, and whether those changes or some of the matters set out in Appendix 1, relating to IT but also more broadly, should be left in Appendix 1 or are better placed in application material.
 - How scalability can be more clearly illustrated in the application material.

I. Obtaining an Understanding of the Five Components of Internal Control and Other Changes

9. The Task Force has been deliberating how to clarify that obtaining an understanding of internal control is done through obtaining an understanding of the five components of internal control, and what this involves. Concern had been expressed that the changes proposed by the Task Force at the September 2017 IAASB meeting focused on controls in each component, and was therefore not clear what is meant by 'obtaining an understanding' versus 'identifying controls relevant to the audit.' In addition, it was also noted that it was still not clear when controls are 'relevant to the audit.'
10. The Task Force therefore continues to deliberate how it can be made clearer what the auditor actions should be in relation to obtaining an understanding of internal control. In considering changes, the Task Force continues to consider if, and how, explicit considerations relevant to IT can be built into obtaining the relevant understanding of each component of internal control.
11. With regard to the requirement for obtaining an understanding of:
 - *The control environment*, the Task Force is of the view that this component is significant because of the impact of the control environment on the other components of internal control, and is continuing to consider how this requirement can be enhanced. The Task Force continues to debate how more fundamental matters relating to the control environment more broadly (such as related to the responsibilities for internal control, including oversight by those charged with governance) can be encompassed in the requirement, with additional guidance to support the enhanced requirement that is broader than just IT.
 - *The entity's process to monitor controls*, the Task Force is considering how to describe the understanding required of the entity's process. In making changes, the Task Force will also continue to be mindful that the entity's monitoring process includes how the entity identifies and remediates deficiencies in controls, and how the entity monitors the effectiveness of its controls.

- *The information system, including related business processes*, the Task Force is reconsidering how to refocus the auditor’s understanding on the ‘flow of transactions’ through the information system for the identified relevant classes of transactions and account balances, and related policies and procedures that address accounting records, and the financial reporting process. The Task Force also plans to continue to consider clarifications to distinguish between this component and the control activities component.
12. Changes made to the definitions of ‘internal control’ and ‘controls’ (Agenda Item 5-B, paragraph 4)
- In relation to the definition of ‘*internal control*’:
 - It was agreed at the September 2017 IAASB meeting that internal control should be referred to as a ‘system of internal control’ as this presents all of the related aspects more fully than referring to it as a process. Changes have been made accordingly, but other changes to the definition to address Board comments or concerns will be further considered for the December 2017 Board meeting.
 - In relation to the definition of ‘*controls*’:
 - Although not specifically related to IT, the Task Force is of the view that this definition is integral to many of the discussions related to understanding the components of internal control, and would therefore value the Board’s further input on whether the revisions to the definition as presented at the September 2017 Board meeting address the concerns that have been raised.
 - The definition as presented at the September 2017 Board meeting was based on the description of ‘controls’ in the COSO Framework 2013,¹⁶ with changes as appropriate to put the concept into the context of the ISAs. However, it was highlighted by the Board that controls consist of more than ‘policies and procedures,’ for example aspects of governance (such as tone at the top) and other aspects of an entity’s systems (such as the risk assessment process) could be a ‘control’ but were not a policy or procedure necessarily.
 - After further deliberation, the Task Force agreed that it was important to highlight that controls are effected by people (including management and those charged with governance), and could encompass formal or informal policies (i.e., could be formal statements or implied through actions), and that procedures are actions to implement the policies. The Task Force has therefore revised the definition of ‘controls’ to embed these concepts, thereby clarifying that it is not only formal documented policies and procedures but could also include other aspects of the entity’s systems.¹⁷

¹⁶ “Embedded within the internal control process are controls, which consists of policies and procedures. Policies reflect management or board statements of what should be done to effect control. Procedures are actions that implement policies. Organizations select and develop controls within each component to effect relevant principles. Controls are interrelated and may support multiple objectives and principles.”

¹⁷ The US Public Company Accounting Oversight Board’s standards refer to “policies or actions” and COSO’s concept of internal control is “*effected by people* – i.e. not merely about policy and procedures manuals, systems and forms, but about people and the actions they take at every level of an organization to effect internal control.”

13. The Board questioned whether ‘control activities’ should be defined as there is still confusion about what this is. The Task Force is of the view that this is a component of internal control, with separate requirements and application and other explanatory material to explain what it is. Accordingly, the Task Force has agreed not to define this but has recognized that clarification is needed as to what the concept is and has been further considering how this component of internal control can be described (see paragraph 24 below).

I. How IT Impacts the Required Understanding

14. ISA 315 (Revised)¹⁸ requires the auditor to obtain an understanding of:
- (a) The entity and its environment;
 - (b) The applicable financial reporting framework; and
 - (c) The entity’s internal control. In obtaining an understanding of the entity’s internal control, the auditor is required to obtain an understanding of the five components of internal control:
 - (i) Control environment;
 - (ii) The entity’s risk assessment process;
 - (iii) The entity’s process to monitor controls;
 - (iv) The information system, including the related business processes relevant to financial reporting, and communication; and
 - (v) Control activities.
15. The Task Force has considered how IT impacts the required understanding of each of these areas and changes have been proposed. Overall, the Task Force is of the view that only limited amendments are needed to the requirements. However, additional guidance in the application and other explanatory material is essential to help auditors focus on the effects of IT in their considerations related to the various requirements in the standard. The Task Force is also of the view that considerations around IT are to be embedded into each relevant section, and should not be presented as separate “considerations about IT” so as to suggest that considerations around IT are a separate exercise.
16. Appendix 1 to this paper sets out a flowchart to illustrate how the information gathered when ‘obtaining an understanding of internal control’ (including IT-related information) is used in assessing control risk, and subsequently as a basis for further audit procedures under ISA 330.¹⁹ This also includes identifying general IT controls, and how this impacts the auditor’s assessment of control risk, to help explain the Task Force’s views relating to general IT controls.
17. The following sets out the Task Force’s views on the proposed changes presented in **Agenda Item 5-B** for discussion.
18. *Risk assessment procedures* (Agenda Item 5-B, paragraph 5)
- Changes are still to be considered relating to the requirement to address Board comments from the September 2017 discussions. However, the Task Force is of the view that additional

¹⁸ This paper has been developed on the basis of the proposals in Agenda Item 2-B from the September 2017 IAASB meeting.

¹⁹ ISA 330, *The Auditor’s Responses to Assessed Risks*

application material to this paragraph related to IT be added to make it more prominent that IT considerations are an integral part of the auditor's work and should not be considered a separate exercise. In particular, this emphasis is important for small- and medium- practices who may see IT considerations during an audit as a separate, and not integrated, exercise.

19. *Understanding the entity and its environment* (Agenda Item 5-B, paragraph 11)

- Most businesses today use IT for commercial purposes as well as internal information processing. A change has been proposed to the requirement to understand the business and operations of the entity to require an understanding about the extent to which the business model integrates the use of IT. The Task Force is of a view that this change recognizes that in today's environment, IT is often integral to the business and may be highly pervasive through the operations of the business.
- Application guidance has been proposed to enhance the auditor's considerations of IT when obtaining an understanding of the entity and its environment in order to recognize the importance of IT in today's environment. The proposed application material highlights that the understanding of the entity will help the auditor start to create expectations in relation to the extent to which IT is involved in the entity's financial reporting and the related effects on the audit (for example, recognizing that an entity where the business model involves web-based transactions or an entity utilizing blockchain technology in making and receiving payments will likely have effects on the audit, as well as recognizing that in many jurisdictions now there are laws or regulations around IT related matters such as data security).

20. *Understanding the system of internal control* (Agenda Item 5-B, paragraph 12)

- Application material has been proposed to further integrate IT considerations into obtaining an understanding of internal control more generally and to make clear that controls include general IT controls, and therefore when obtaining an understanding of general IT controls the same principles as set out in in the requirement will apply.

21. *Understanding the control environment* (Agenda Item 5-B, paragraphs 14, 14A)

- At this stage, taking into account further consideration by the Task Force of enhancements to the required understanding of the control environment as explained above, the Task Force has proposed changes to the application material to include additional considerations for the auditor relating to both the IT environment (such as governance over IT) and to IT (such as related to the technology platform used), as it is believed that the auditor's understanding of the control environment should encompass an understanding of governance over IT, and a high-level understanding of the current state of the entity's IT environment.

22. *Understanding the entity's risk assessment process* (Agenda Item 5-B, paragraph 15)

- Additional guidance has been developed explaining the types of IT matters that can be considered when obtaining an understanding of the entity's risk assessment process relating to both financial reporting risks and operational risks (i.e., may not only be direct risks to financial reporting). In addition, understanding the IT aspects of the business risks that the entity has identified may also help the auditor understand the entity's automated processes (including relating to data) that may be relevant to the audit.

23. *Understanding the entity's process to monitor controls* (Agenda Item 5-B, paragraph 22)

- Additional guidance has been developed about the types of matters that need to be considered related to IT when obtaining an understanding of the entity's monitoring process, including emphasizing that controls could be controls over automated controls in highly automated and complex IT systems, as well as controls that monitor access and segregation of duties.
 - It is also noted that further application guidance is to be developed recognizing that internal audit may use IT in undertaking their procedures, as well as to recognize the IT impacts on sources of information.
24. *Understanding the information system, including related business processes, relevant to financial reporting, and communication* (Agenda item 5-B, paragraph 18):
- Suggestions of matters that may need to be considered related to IT when obtaining an understanding of the information system, including related business processes, have been proposed in the application material to emphasize attributes related to entity's use of IT that could be considered. As the Task Force works through distinguishing between this component and the control activities component, some of the matters proposed may move to application material in the control activities component as relevant.
25. *Understanding control activities* (Agenda Item 5-B, paragraphs 20 and 21)
- The Task Force continues to explore how best to describe this category of internal control, in particular when controls are relevant to the audit (including general IT controls) and will present further changes for Board consideration in December 2017 (as noted above). Furthermore, the Task Force is still considering how to provide application material to provide guidance about how an understanding of control activities is obtained, in the context of the changes made in this, and the other components, of internal control.
 - In relation to IT related matters, in its deliberations the Task Force has agreed that there are a number of circumstances when general IT controls would be relevant to the audit, and these circumstances have been incorporated in the proposed revised requirement and supporting application material (although the requirement is subject to further refinements as noted in the prior bullet, and therefore the Board should focus on the concepts presented versus the drafting). The Task Force is also of the view that such an approach is helpful to illustrate scalability—in clarifying specific circumstances when general IT controls are relevant to the audit, in smaller entities with less complex IT systems, if the auditor is not going to rely on the automated controls as part of the audit, and if the automated controls do not meet the other proposed described circumstances, the auditor would not need to further consider the general IT controls.

Matters for IAASB Consideration

1. The IAASB is asked for views regarding the proposed changes to the definition of controls as explained in paragraph 12 above, specifically whether this is broad enough to capture other matters that Board members were concerned would be omitted by a more narrow definition.
2. The IAASB is asked for views regarding the proposed changes to ISA 315 (Revised) relating to enhancing the auditor's considerations of IT as explained in paragraphs 18–25 above. In particular, in relation to the proposed requirement to identify and understand general IT controls (as described in paragraph 25), do Board members have the view that describing circumstances

- that may be indicative of when general IT controls are relevant to the audit should be included in the requirement as presented? Are there other circumstances that should be included?
3. Are there other matters related to IT that the Task Force should be considering in finalizing the proposals for discussion at the December IAASB meeting?

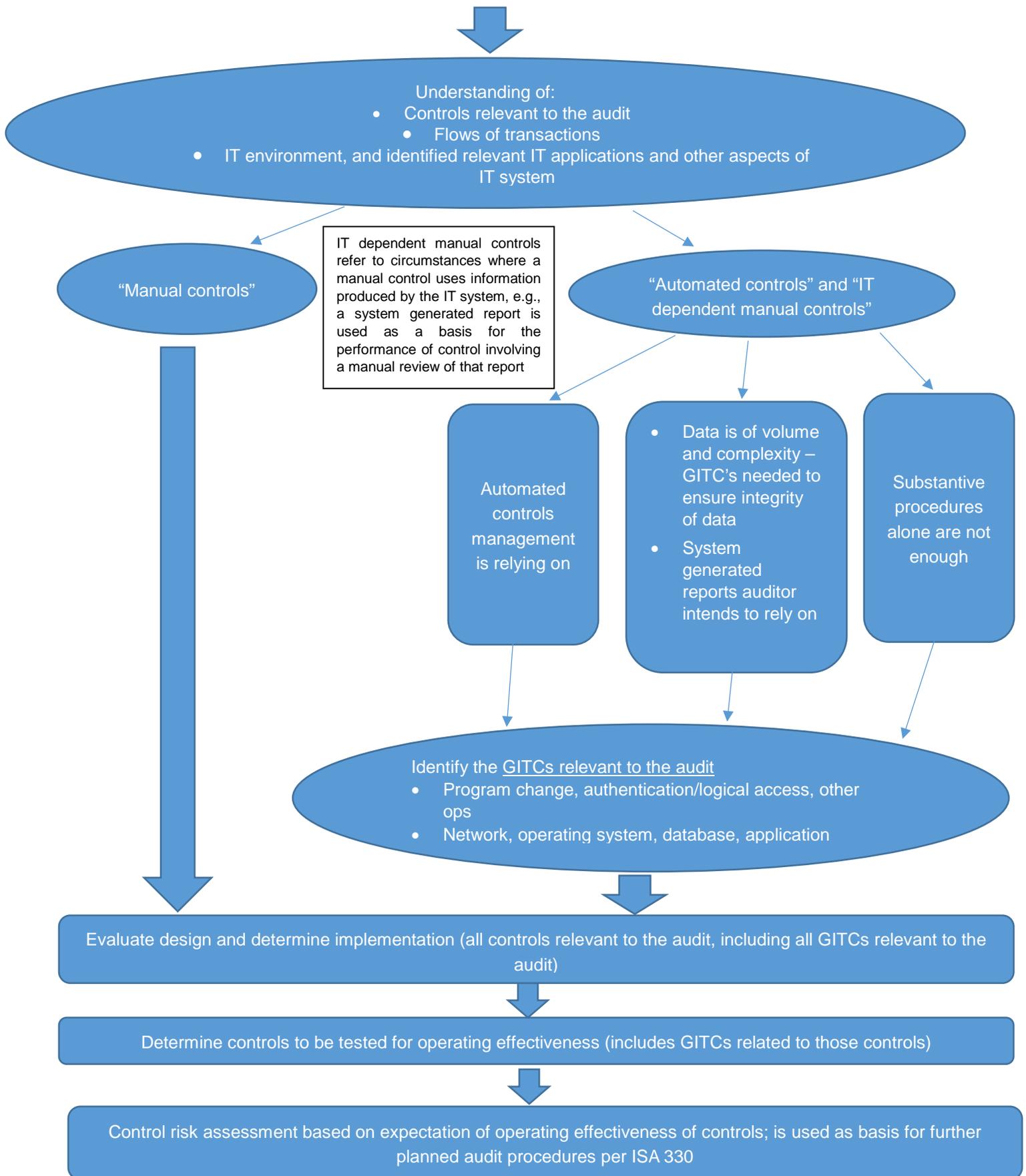
Identifying and Assessing the Risks of Material Misstatement

26. Proposed new paragraph 25D requires that the auditor assesses control risk by:
- (a) Relating the controls relevant to the audit that the auditor intends to test to what can go wrong at the assertion level; and
 - (b) Considering whether controls identified address inherent risks assessed.
27. In its deliberations, the Task Force has agreed that a separate risk assessment for risks arising from IT is not required, but agreed that the link between general IT controls and the control risk assessment needs to be made (and relevant application material developed), including to address circumstances when GITCs are not present or are found to be ineffective. In addition, the Task Force is still considering whether changes are needed in respect of risks where substantive procedures alone are not sufficient (with any proposed revisions presented in December 2017 for discussion).

Appendix 1 to IAASB October 2017 issues paper:

The following presents a high-level overview of how the information gathered in 'understanding the 5 components of internal control' (including related to IT) is used in assessing control risk, and subsequently as a basis for further audit procedures under ISA 330. It also illustrates the considerations involved in determining whether general IT controls are relevant to the audit. It is noted that many of these steps are iterative.

This is not intended to be presented as a decision summary and various aspects of this diagram are still being discussed (such as 'controls relevant to the audit').



Extracts from relevant Standards**ISA 200 Overall Objectives of the Independent Auditor and the Conduct of an Audit in accordance with International Standards on Auditing***Audit Risk*

- A34. Audit risk is a function of the risks of material misstatement and detection risk. The assessment of risks is based on audit procedures to obtain information necessary for that purpose and evidence obtained throughout the audit. The assessment of risks is a matter of professional judgment, rather than a matter capable of precise measurement.
- A35. For purposes of the ISAs, audit risk does not include the risk that the auditor might express an opinion that the financial statements are materially misstated when they are not. This risk is ordinarily insignificant. Further, audit risk is a technical term related to the process of auditing; it does not refer to the auditor's business risks such as loss from litigation, adverse publicity, or other events arising in connection with the audit of financial statements.

Risks of Material Misstatement

- A36. The risks of material misstatement may exist at two levels:
- The overall financial statement level; and
 - The assertion level for classes of transactions, account balances, and disclosures.
- A37. Risks of material misstatement at the overall financial statement level refer to risks of material misstatement that relate pervasively to the financial statements as a whole and potentially affect many assertions.
- A38. Risks of material misstatement at the assertion level are assessed in order to determine the nature, timing and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence. This evidence enables the auditor to express an opinion on the financial statements at an acceptably low level of audit risk. Auditors use various approaches to accomplish the objective of assessing the risks of material misstatement. For example, the auditor may make use of a model that expresses the general relationship of the components of audit risk in mathematical terms to arrive at an acceptable level of detection risk. Some auditors find such a model to be useful when planning audit procedures.
- A39. The risks of material misstatement at the assertion level consist of two components: inherent risk and control risk. Inherent risk and control risk are the entity's risks; they exist independently of the audit of the financial statements.
- A40. Inherent risk is higher for some assertions and related classes of transactions, account balances, and disclosures than for others. For example, it may be higher for complex calculations or for accounts consisting of amounts derived from accounting estimates that are subject to significant estimation uncertainty. External circumstances giving

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

- A41. Control risk is a function of the effectiveness of the design, implementation and maintenance of internal control by management to address identified risks that threaten the achievement of the entity's objectives relevant to preparation of the entity's financial statements. However, internal control, no matter how well designed and operated, can only reduce, but not eliminate, risks of material misstatement in the financial statements, because of the inherent limitations of internal control. These include, for example, the possibility of human errors or mistakes, or of controls being circumvented by collusion or inappropriate management override. Accordingly, some control risk will always exist. The ISAs provide the conditions under which the auditor is required to, or may choose to, test the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures to be performed.²⁰
- A42. The ISAs do not ordinarily refer to inherent risk and control risk separately, but rather to a combined assessment of the "risks of material misstatement." However, the auditor may make separate or combined assessments of inherent and control risk depending on preferred audit techniques or methodologies and practical considerations. The assessment of the risks of material misstatement may be expressed in quantitative terms, such as in percentages, or in non-quantitative terms. In any case, the need for the auditor to make appropriate risk assessments is more important than the different approaches by which they may be made.
- A43. ISA 315 (Revised) establishes requirements and provides guidance on identifying and assessing the risks of material misstatement at the financial statement and assertion levels.

ISA 330 The Auditor's Responses to Assessed Risks

Paragraph 6:

The auditor shall design and perform further audit procedures whose nature, timing and extent are based on and are responsive to the assessed risks of material misstatement at the assertion level. (Ref: Para. A4–A8)

Paragraph 7:

In designing the further audit procedures to be performed, the auditor shall:

- (a) Consider the reasons for the assessment given to the risk of material misstatement at the assertion level for each class of transactions, account balance, and disclosure, including:
 - (i) The likelihood of material misstatement due to the particular characteristics of the relevant class of transactions, account balance, or disclosure (that is, the inherent risk); and

²⁰ ISA 330, *The Auditor's Responses to Assessed Risks*, paragraphs 7–17

- | |
|---|
| <ul style="list-style-type: none">(ii) Whether the risk assessment takes account of relevant controls (that is, the control risk), thereby requiring the auditor to obtain audit evidence to determine whether the controls are operating effectively (that is, the auditor intends to rely on the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures); and (Ref: Para. A9–A18)(b) Obtain more persuasive audit evidence the higher the auditor's assessment of risk. (Ref: Para. A19) |
|---|