For the attention of Mr. Dan Montgomery
Interim Technical Director
International Auditing and Assurance Standards Board
529 Fifth Avenue, 6th Floor
New York, New York, 10017
USA

[Submitted via IAASB website]

4 November 2018

Dear Mr. Montgomery,

IAASB Exposure Draft: Proposed International Standard on Auditing 315 (Revised), *Identifying and assessing the risks of material misstatement*

We[1] appreciate the opportunity to comment on the IAASB's Exposure Draft (ED).

ISA 315 forms the foundation of the risk-based approach to all audits and, in our view, extant ISA 315 has provided a robust framework to guide auditors to obtain a comprehensive understanding of the entity and its environment, providing an appropriate basis on which to make an informed risk assessment and to perform an effective risk-based audit.

Given its importance, it is critical that the revised standard drives an informed, consistent and effective approach to risk assessment through clear and robust requirements. Those requirements should be capable of application to audits of all sizes and complexities, and reflect that a range of appropriate methodologies can be applied to achieve the intended outcomes.

Support for the IAASB's objectives but concerned that the proposals do not achieve them

We support the IAASB's original objectives in revising ISA 315 but we do not believe that the proposed revisions, as currently drafted, fully achieve those aims.

We agree that there are aspects of the current standard that warrant clarification. Responses to the IAASB's Post-Implementation Review of the Clarity ISAs and regulatory inspections of audits indicate that certain extant concepts, including the spectrum of risk, controls relevant to the audit, and the definition of significant risk, are not being understood or implemented in a consistent manner. We also support the need to update the ISA to better reflect the evolving use of technology, both with respect to how entities' use of increasingly sophisticated IT systems, including cloud based technology, impacts the audit, as well as the evolving use of technology by the auditor in conducting the audit. We further support, within that context, the increased focus on general information technology controls (GITCs). Aspects of the proposed ED are useful in addressing these topics; however we believe there is a need to focus further on whether the standard will remain fit for purpose, given the pace of technological change.

[1] This response is being filed on behalf of the network of member firms of PricewaterhouseCoopers International Limited and references to "PwC", "we" and "our" refer to the PwC network of member firms.

PricewaterhouseCoopers International Limited
1 Embankment Place
London WC2N 6RH
T: + 44 (0)20 7583 5000, F: + 44 (0)20 7822 4652

We note the acknowledgement by the Board that there was no intent to change the extant risk assessment model. However, in our view, the ED represents, in certain aspects, quite a fundamental revision of the model. We have concerns that the extent and clarity of the proposed changes to the risk assessment requirements, and the totality of the proposed revisions, risk confusion that may lead to increasing, rather than reducing, the current inconsistency in practice.

The complexity of the proposed requirements in the ED, and lack of clarity of some of the concepts, together with the overall length of the standard, also, in our view, raise questions as to whether the proposed revision can be applied effectively and efficiently to smaller and less complex audits. Given the critical nature of this standard in underpinning the entire range of audits, if clarity and scalability are not successfully addressed this poses a risk to adoption by jurisdictions and of national standard setters seeking alternative solutions to the ISAs. We comment further on this issue below.

For these reasons, we do not support the ED in its current form.

We believe the issues identified in relation to the extant ISA can best be addressed through structural changes to the extant requirements, together with targeted refinements to requirements and the provision of additional guidance in those areas identified as requiring clarification. This would bring the needed clarity to strengthen the extant ISA and support consistent and robust risk assessments in performing high quality audits.

Our recommendations for appropriate changes that address the project scope

Given our concerns about the proposed revisions, we felt it was important to invest the time to articulate alternative suggestions that would address our concerns while achieving the objectives behind the revision of ISA 315.

Appendix 2 sets out an initial outline of what we believe to be a more helpful approach and structure for the requirements of the standard. In developing this approach, our thinking has been framed with the following objectives in mind:

- Building a logical and intuitive structure that appropriately incorporates new concepts that clarify, and thereby drive consistency in, the auditor's work effort;
- Directly addressing concerns about scalability by making clear the extent of the understanding of the entity's system of internal control relevant to financial reporting that is appropriate to support the auditor's assessment of inherent risks, and the further understanding that is needed when planning to obtain audit evidence from testing controls; and
- Clarifying existing concepts identified as being misunderstood in practice or applied inconsistently, based on the ISA post-implementation review.

Our suggestions more directly link what the auditor needs to understand regarding the entity's system of internal control to support separately the assessments of inherent risk and control risk. We believe more explicitly setting out the required understanding of internal control to support each of these assessments presents an opportunity to deliver the much called for clarity for audits of smaller and less complex entities regarding the nature and extent of understanding that, as a minimum, is needed when the auditor does not intend to obtain audit evidence from evaluating the design and testing the operating effectiveness of controls. We would be happy to work with the Board's Task Force to explain our thinking and further develop this approach if this is considered appropriate.

Our suggestions also seek to minimise the introduction of unnecessary new definitions and concepts. The ED's proposed approach appears to be drawing on concepts included within the PCAOB risk assessment model, yet trying to fit these into the existing framework of an ISA audit. This may cause confusion. We believe our suggestions achieve the objective of the revision without needing to introduce new concepts.

In other areas, we believe the proposed changes do not go far enough in eliminating confusion that exists in the extant standard around certain critical key concepts. In particular, we believe there is an opportunity to clarify how the concept of "control risk" is used in a financial statement audit by reframing the application of the audit risk equation to better reflect how auditors apply it in gathering audit evidence.

Using the concept of planned controls reliance as an opportunity to provide clarity about how the concept of control risk is used in a financial statement audit

We are concerned that the potential implications of a separate assessment of control risk have not been fully considered, nor the nature of what is expected sufficiently explained.

In a financial statement audit, once inherent risk has been assessed, the auditor's concern is obtaining audit evidence to reduce that risk to an appropriately low level. It is not necessary for the auditor to make a discrete identification and assessment of control "risk" similar to what is needed when the auditor plans an audit designed to give an opinion on internal control. Instead, the auditor's focus is whether to obtain evidence in response to an identified inherent risk from evaluating the design, and testing operating effectiveness, of controls, or from performing substantive procedures, or from a combination thereof. While the risk of material misstatement comprises both inherent risk and control risk, the latter concept is more readily understandable, and better supports scalability in the risk assessment and planning stage of the audit, by focussing on assessing the "planned control reliance". We believe that is how the concept is most commonly considered today.

In our view, reframing the proposed separate assessment of control risk to focus more explicitly on the fact that this can be accomplished through the auditor's assessment of the extent to which the auditor plans to obtain evidence from testing the operating effectiveness of controls would also bring clarity within the standard to how much understanding of direct controls is needed. This is an area that requires clarification, particularly for those circumstances when the audit approach is expected to be based primarily on substantive procedures. In our view, the ISA would be clearer if it set out separately the nature and extent of understanding of the system of internal control needed to assess inherent risk, and then the additional level of understanding needed of direct controls if the auditor's intention is to rely on the operating effectiveness of them as part of the audit evidence obtained in response to assessed inherent risks.

We acknowledge that the application material that discusses control risk is an attempt to reconcile control risk and planned controls reliance (e.g., if the auditor is not intending to test the operating effectiveness of controls, control risk is assessed at maximum), but application material alone is not the solution to fixing a broader problem of misunderstanding. We believe the requirements could better support this concept.

Reframing the control risk part of the traditional audit risk equation to focus on planned controls reliance was not possible in the extant ISA because a combined risk assessment was allowed (i.e., the auditor's risk assessment could be a combined assessment of inherent risk taking into account the expected effectiveness of related controls). Because inherent risk is now proposed to be a separate assessment, there is now an opportunity to simplify and bring much needed clarity to the area of the extant ISA that has caused the most confusion.

In addition, we believe reframing control risk in this way would help more clearly illustrate that firms may think about this assessment within their methodologies in a variety of ways, including by considering how planned controls reliance can appropriately reduce the overall risk of material misstatement.

We support the IAASB's efforts in ISA 540 (Revised) to describe the relationship between control risk and planned controls reliance, and we think it would be valuable to build on this guidance in ISA 315 (Revised) to take advantage of the opportunity to address current misconceptions.

Other areas of focus in our response

In addition to the broad matters outlined above, there are a number of other aspects of the proposed ED that we believe would benefit from further consideration, including:

- New and revised definitions that we do not feel clarify the risk assessment process, but in fact introduce a level of complexity that increases the risk of inconsistent understanding and application of the requirements – which is counter to the intended objectives in revising the standard. In particular:
    - The definition of a new concept of "inherent risk factors" and how those factors are proposed to be used, which is complex and different to how external and company-specific factors are applied in the PCAOB risk assessment standard and also different to how they are used in the very recently approved revision of ISA 540. We also believe fraud risk factors are best addressed in ISA 240 and that inclusion of susceptibility to misstatement due to bias or fraud as a discrete risk factor in ISA 315 may lead to confusion;
    - The interaction of the proposed definitions of "relevant assertion" and "significant classes of transactions, account balances and disclosures" and their relationship with the risk assessment requirements, which we believe adds unnecessary complexity; and
    - The revised definition of "significant risk", which we believe results in items potentially falling within its scope that typically may not be considered significant risks.
- How the requirements have been restructured, including how they refer to "identified risks of material misstatement" for which the auditor then assesses inherent and control risk. In our view, this leads to a perception that the proposed ISA requires a preliminary assessment, or separate identification, of potential risks of material misstatement, which is confusing in light of the IAASB's objective of promoting a stronger focus on the separate assessment of inherent and control risk. The approach seems forced and unduly restrictive;
- The proposed ISA 315 stand-back for "material classes of transactions, account balances and disclosures", which we do not consider necessary given the stand-back in ISA 330;
- The use of the broad concept of "sufficient appropriate audit evidence" as the measure of the nature and extent of risk assessment procedures to be performed as the basis for the auditor's risk assessment, without providing the necessary context for that judgment; and
- The clarity of expected documentation requirements arising from the ED taken as a whole when viewed in the context of ISA 230.

In the responses to the specific questions posed in the explanatory memorandum, we explain why we believe the changes we have suggested should be considered. We also include in the appendices our suggestions for an alternative structure and an initial outline draft of requirements to illustrate our thinking; other detailed substantive and editorial comments; and a summary of the field-testing exercise that we conducted.

Scalability

Scalability is a significant challenge that the IAASB is aiming to address in the revisions, particularly in articulating the nature and extent of understanding of the entity's system of internal control, including design and implementation of controls, needed in order to perform a largely substantive audit for smaller, less complex entities. Due to the matters identified above, we do not believe that the ED successfully resolves this challenge.

Furthermore, paragraph 13 of the ED seeks to explain scalability by reference to relevant considerations for smaller entities when such entities are less complex. That paragraph is explanatory only; it does not have the authority of a requirement. Whether or not the ISA is scalable depends on the clarity of the requirements and how they are applied to audits of varying size and complexity. The length and complexity of the proposed standard, as well as a lack of clarity in how certain new concepts are to apply, in our view, raises questions as to whether it can be applied effectively and efficiently to smaller and less complex audits.

We are particularly concerned that failing to illustrate appropriately how the standard can be applied could lead to inconsistent application.

In conclusion, we support the IAASB's original objectives in revising ISA 315. To achieve these objectives we believe it is essential that the revised standard: is understandable and capable of practical application; supports consistent and appropriate risk assessments; and is scalable to audits of entities of varying size and complexity.

The proposed structure of the risk assessment requirements and interrelationships of the proposed new concepts and definitions are not always easy to understand and, in our view, may give rise to an ineffective and inconsistent approach to risk assessment across engagements. The changes could also have a significant cost impact, including with respect to many firms' methodologies and supporting technologies, with little clear benefit.

As explained above, and as illustrated in the appendices, we believe it is possible to achieve the IAASB's objectives through restructuring the extant standard and strengthening the requirements and application guidance to clarify key concepts and address the issues raised in practice and by regulators, while also addressing questions about the scalability of the standard. This can be achieved without fundamentally re-imagining the risk assessment process. We also support robust implementation guidance, which may better be able to convey, in a more effective manner, examples of how the requirements may be applied to audits of smaller and less complex entities.

Retaining, but strengthening, the existing risk assessment model and clarifying how it is expected to be applied will, in our view, result in a robust, high quality, yet practical, standard that supports an effective and consistent approach to risk assessments and reinforces audit quality, in the public interest.

We would be happy to discuss our views further with you. If you have any questions regarding this letter, please contact Diana Hillier, at diana.hillier@pwc.com, Ralph Weinberger, at ralph.a.weinberger@pwc.com, or me, at james.chalmers@pwc.com.

Yours sincerely,

James Chalmers

James Chalmers

Global Assurance Leader

Appendix 1 – Responses to specific questions

1. **Has ED-315 been appropriately restructured, clarified and modernized in order to promote a more consistent and robust process for the identification and assessment of the risks of material misstatement. In particular:**
    a. **Do the proposed changes help with the understandability of the risk identification and assessment process? Are the flowcharts helpful in understanding the flow of the standard (i.e., how the requirements interact and how they are iterative in nature)?**
    b. **Will the revisions promote a more robust process for the identification and assessment of the risks of material misstatement and do they appropriately address the public interest issues outlined in paragraphs 6-28?**
    c. **Are the new introductory paragraphs helpful?**

Overall Comments

No, for the reasons that we describe below, we are concerned that the restructured ED-315 will not result in a more consistent or more robust process for the identification and assessment of the risks of material misstatement.

ISA 315 forms the foundation of the risk-based approach to all audits. As a result, it is critical that the standard drives an informed, consistent and effective approach to risk assessment through clear and robust requirements. Those requirements should be capable of application to audits of all sizes and complexities and reflect that a range of appropriate methodologies can be applied to achieve the intended outcomes. In our view, the proposals do not fully achieve these objectives.

We support the IAASB's original objectives in revising ISA 315, but we do not believe that the proposed revisions, as currently drafted, fully achieve those aims. We agree that there are aspects of the current standard that warrant clarification. Regulatory inspections and responses to the IAASB's Post-Implementation Review of the Clarity ISAs have indicated that certain extant concepts, including the spectrum of risk, controls relevant to the audit, and the definition of significant risk, are not being understood or implemented in a consistent manner. We also support the need to update the ISA to better reflect the evolving use of technology, both with respect to how entities' use of increasingly sophisticated IT systems, including cloud based technology, impacts the audit, as well as the evolving use of technology by the auditor in conducting the audit. We also support, within that context, the increased focus on general information technology controls (GITCs). Aspects of the proposed ED are useful in addressing these topics; however we believe there is a need to focus further on whether the standard will remain fit for purpose, given the pace of technological change.

We note the acknowledgement by the Board that there was no intent to change the extant risk assessment model. However, in our view, the ED represents, in certain aspects, quite a fundamental revision of the risk assessment model. We believe the clarification of key concepts that would strengthen the extant ISA and support consistent application in performing robust high quality audits can be achieved without such extensive revision of the model.

We are concerned about the extent and clarity of the proposed changes to the risk assessment requirements. We believe the specific thought process that has been built into the risk assessment requirements is convoluted and therefore confusing, with a concern that this may lead to increasing, rather than reducing, the current inconsistency in practice. Further, we believe it is important to allow flexibility in how the auditor achieves the intended outcome, as different firms' methodologies that exist today and that will continue to evolve over time may lead to the same outcomes, albeit in a different way.

The proposed model appears to be drawing on concepts included within the PCAOB risk assessment model. However, the role of some of the concepts in the PCAOB risk assessment model is to clarify the scope of work needed to have an appropriate basis for the auditor's opinion on the design and operating effectiveness of the entity's internal control over financial reporting. This is not directly comparable with, nor is this relevant to, an ISA audit to form an opinion on the entity's financial statements. Consequently, we do not believe these changes are helpful.

The complexity of the proposed requirements in the ED, and lack of clarity of some of the concepts, together with the overall length of the standard, also, in our view, raises questions as to whether it can be applied effectively and efficiently to smaller and less complex audits. Given the foundational nature of this standard, if scalability is not successfully addressed this poses a further risk to adoption by jurisdictions and of national standard setters seeking alternative solutions to the ISAs. We comment further on scalability in our response to question 2.

Changing the fundamentals of the risk assessment model could also have a significant cost impact, including with respect to the effect on many firms' methodologies and supporting technologies, with little clear benefit.

We aim to support the IAASB in addressing the above concerns through highlighting areas where we see challenges in implementation and then proposing solutions. Our assessment of the ED, which includes the findings from our field-testing, has led us to conclude that the following key aspects would benefit from further consideration:

- New and revised definitions and concepts that we do not feel clarify the risk assessment process, but in fact introduce a level of complexity that increases the risk of inconsistent understanding and application of the requirements – which is counter to the intended objectives in revising the standard. In particular:
    - The extent of the understanding of the system of internal control that is appropriate to support the auditor's inherent risk assessment and, when the auditor plans to obtain evidence from controls, what further understanding of internal control is needed;
    - The definition of a new concept of "inherent risk factors" and how those factors are proposed to be used, which is complex and different to how external and company-specific factors are applied in the PCAOB risk assessment standard and also different to how they are used in the very recently approved revision of ISA 540. We also believe fraud risk factors are best addressed in ISA 240 and that inclusion of susceptibility to misstatement due to bias or fraud as a discrete risk factor in ISA 315 may lead to confusion;
    - The interaction of the proposed definitions of "relevant assertion" and "significant classes of transactions, account balances and disclosures" and their relationship with the risk assessment requirements, which we believe adds unnecessary complexity;
    - The articulation of the concept of "control risk", in support of the proposed requirement to separately assess control risk, which continues to often be misunderstood; and
    - The revised definition of "significant risk", which we believe results in items potentially falling within its scope that typically may not be considered significant risks.
- How the requirements have been restructured, including how they refer to "identified risks of material misstatement" for which the auditor then assesses inherent and control risk. In our view, this leads to a perception that the proposed ISA requires a preliminary assessment, or

separate identification of, potential risks of material misstatement, which is confusing in light of the IAASB's objective of promoting a stronger focus on the separate assessment of inherent and control risk. The approach seems forced and unduly restrictive;

- The proposed ISA 315 stand-back for "material classes of transactions, account balances and disclosures", which we do not consider necessary given the stand-back in ISA 330;
- The use of the broad concept of "sufficient appropriate audit evidence" as the measure of the nature and extent of risk assessment procedures to be performed as the basis for the auditor's risk assessment, without providing the necessary context for that judgement; and
- The clarity of expected documentation requirements arising from the ED taken as a whole when viewed in the context of ISA 230.

Our concerns on the various matters described above, together with our recommendations for addressing them, are further explained in our responses to the remaining questions below.

Our recommendations for appropriate changes that address the project scope

Given our concerns about the proposed revisions, we felt it was important to invest the time to articulate alternative suggestions that would address our concerns while achieving the objectives behind the revision of ISA 315.

Appendix 2 sets out our vision of what we believe to be a more helpful approach and structure for the requirements of the standard. In developing this approach, our thinking has been framed with the following objectives in mind:

- Building a logical and intuitive structure that appropriately incorporates new concepts that bring clarity around, and thereby drive consistency in, the auditor's work effort;
- Directly addressing concerns over scalability by making clear the extent of the understanding of the entity's system of internal control relevant to financial reporting that is appropriate to support the auditor's assessment of inherent risks, and the further understanding that is needed when planning to obtain audit evidence from testing controls; and
- Clarifying existing concepts identified as being misunderstood in practice or applied inconsistently, based on the ISA post-implementation review.

Our suggestions more directly link what the auditor needs to understand regarding the entity's system of internal control to support separately the assessments of inherent risk and control risk. We believe more explicitly setting out the required understanding of internal control to support each of these assessments presents an opportunity to deliver the much called for clarity for audits of smaller and less complex entities regarding the nature and extent of understanding that, as a minimum, is needed when the auditor does not intend to obtain audit evidence from evaluating the design, and testing the operating effectiveness, of controls. We would be happy to work with the Board's Task Force to explain our thinking and further develop this approach if this is considered appropriate.

Flowcharts

We conducted field-testing as part of the formulation of our response, the approach to which is set out in Appendix 5 of this letter. As part of this, we had two different groups - with some teams receiving the flowcharts and others not. The comments we received from our field-testing suggested that the flowcharts were helpful to aid understanding of the standard, with teams noting the flowchart relating to General IT Controls as particularly helpful.

We are, however, concerned that the flowcharts are proving necessary to facilitate understanding of the standard, in particular the risk assessment requirements. It is important that any standard issued by the Board is able to stand alone, and that the requirements be understandable without any additional guidance documents such as these flowcharts proving necessary. We welcome the inclusion of the flowcharts in the materials issued for exposure. They may also serve as useful supplementary implementation support materials – as long as the standard itself is clear and understandable in its own right. Acknowledging that many stakeholders like visual representations, we have illustrated an alternative flowchart based on our suggestions for how the risk assessment requirements could be restructured. We do not believe, however, that the flowchart is necessary to understand the suggestions we propose in Appendix 2.

Introductory paragraphs

Feedback from our field-testing exercise was that engagement teams found this section to be useful. Consequently, we support retaining an introductory section that explains the thought process and key concepts used in the risk assessment process, having addressed the concerns we describe related to the current complexity of proposed concepts, which would enable the explanation of the key concepts to be simplified and made more succinct. Clearer mapping or cross-referencing from this section to the relevant requirements of the standard would also be useful.

While the overall length of this introductory section needs to be carefully managed, we would also recommend that this section could do more to draw out two specific points that would reinforce the scalability of the standard. First, consistent with one of our key themes, we think the standard could better explain the required extent of understanding of the system of internal control necessary to support each of the assessments of inherent risk and control risk. Our suggested structure for the requirements would allow this point to be made clearly in the introductory section. Secondly, we believe the introductory section could highlight the role of IT and why this is of increasing importance in today's audit environment. This could specifically draw out a key scalability message by highlighting that in smaller entities the sophistication of an entity's use of IT (and overall control environment) and related documentation may be less. This would help avoid implications, from reading and applying the requirements and application material, that a certain level of IT structure and auditor work effort thereon is required, or indeed possible, in all audits.

Documentation

We are concerned at the overall documentation expectations resulting from the changes to the various requirements. For example, it remains unclear how the auditor would be expected to document consideration of both inherent risk factors and relevant assertions. We believe this may give rise to a complicated "matrix" risk assessment. While the statement made in paragraph A245 that the auditor does not need to document how every inherent risk factor was taken into account is helpful, we do not believe a single sentence of application material is sufficient to avoid inconsistent interpretation. We recommend the Board provide greater clarity around the expectations for documentation arising from the revised requirements. While limited changes have been made to the actual documentation requirement, it has been stated through the recent webinars that the significant judgements to be documented should be viewed in light of ISA 230. Relying on ISA 230 alone is, in our view, not helpful given the significant changes to requirements that have been made. For example, it is unclear whether the "position on the spectrum" is expected to be a significant judgement – especially where the risk is ultimately not deemed to be a significant risk. The scope of significant judgements is also being debated across a number of the IAASB's ongoing projects. In light of those ongoing discussions, we believe the Board needs to give further consideration to appropriate application material explaining this term, in the context of judgements made in identifying and assessing risks of material misstatement, in finalising the ISA.

2. Are the requirements and application material of ED-315 sufficiently scalable, including the ability to apply ED-315 to the audits of entities with a wide range of sizes, complexities and circumstances?

Paragraph 13 seeks to explain scalability by reference to relevant considerations for smaller entities when such entities are less complex. That paragraph is explanatory only; it does not have the authority of a requirement. Whether or not the ISA is scalable depends on the clarity of the requirements and how they apply to audits of varying size and complexity. While some of the changes proposed help in that regard, we do not believe scalability has been achieved. Notwithstanding the clarification that states that this "smaller and less complex" guidance may also be relevant to larger entities that are also less complex, we believe there is a risk of the "and" construct of the phrase may be misinterpreted to mean that both of these criteria must apply for the guidance to be applicable. We believe there may also be confusion as to the applicability of the guidance in an audit of a larger entity that has a high degree of complexity in some respects but also has classes of transactions or account balances for which the degree of complexity is low and therefore a scaled approach to risk assessment procedures may be appropriate.

We acknowledge the intent of merging the guidance on smaller entities into the body of the application material, rather than separately calling this out. However, the volume of text makes it harder to locate the material explaining how the requirements throughout the ISA may be applied in an audit of a smaller and less complex entity. We are concerned that the standard's overall length and complexity are themselves barriers to its scalable application.

With respect to understanding the system of internal control relevant to financial reporting, we find the requirements impose a framework in which it is not clear where the auditor could do less, and in which circumstances doing less would be appropriate. We believe that an alternative solution can be developed that would more clearly describe the nature and extent of understanding needed, as a minimum, to support the auditor's inherent risk assessment, together with a more precise direction on what is needed in relation to understanding direct controls. Such an approach would, in our view, better address the questions raised with respect to the extant standard about how much understanding is needed, for example with respect to control activities and general IT controls, and when the design and implementation of controls needs to be evaluated. In many cases, smaller entities simply do not have the sophistication of controls or documentation that the auditor can evaluate to support planned reliance on controls. We describe this proposal in our response to question 5.

Further to our comments in response to question 1, a number of the teams that participated in our field-testing either raised questions about what was expected to be documented or stated that they believed the documentation that would be needed, in particular for the revised risk assessment requirements, would be extensive, onerous and not scalable to smaller entities. Providing greater clarity around the nature of the significant judgements that the Board believes may be documented together with what is envisaged by "key aspects" of the auditor's understanding would more directly assist understanding the scalability of documentation.

Lastly, related to the above, implementation materials that provide better "signposts" and examples of the nature and extent of the understanding of the system of internal control that is required, for example for smaller entities with less sophisticated IT systems and informal documentation around the system of internal control (e.g., the entity's risk assessment process), would also be useful.

3. Do respondents agree with the approach taken to enhancing ED-315 in relation to automated tools and techniques, including data analytics, through the use of examples to illustrate how these are used in an audit (see Appendix 1 for references to the relevant paragraphs in ED-315)? Are there other areas within ED-315 where further guidance is needed in relation to automated tools and techniques, and what is the nature of the necessary guidance?

We are supportive of the approach taken within the ED, referring broadly to technology and the use of the generic term "automated tools and techniques", rather than "data analytics", as an umbrella term that seeks to avoid prematurely prescribing certain techniques or inadvertently implying unduly narrow boundaries on how such techniques may be used and what evidence they can provide. We do, however, note that not all tools are necessarily automated. Therefore, the Board may wish to consider whether a term such as "technology enabled (or assisted) tools and techniques" may be more appropriate.

Recognising and embracing the opportunities that technology can bring to an audit of financial statements is, in our view, critical to maintaining the relevance of the profession and driving audit quality in the future.

We feel that the guidance included in the ED strikes broadly the right balance for the topic at this time, but highlight two points for the Board's further consideration. Firstly, we believe it is important, as the use of such technology tools increase, to recognise that in many cases these can replace the more traditional risk assessment procedures the auditor might perform. We don't believe the intent was to suggest that such tools are incremental to other procedures and we would encourage that point to be made clear, avoiding any use of terms that might imply otherwise (for example see paragraph A155 that refers to identifying "additional" risks).

Secondly, we believe it would be helpful to give further consideration to the future technology enabled environment and, specifically, in the context of GITCs, the impact of cloud-based solutions on how the auditor would consider such controls. Likewise, seeking to understand GITCs around Artificial Intelligence systems may be quite fundamentally different. Cryptocurrency and blockchain also raise similar questions. ISA 315 cannot reasonably answer all these questions at this time. However, we believe it would be useful for the Board to consider if, and to what extent, the standard can acknowledge the impact of such technology on the auditor's risk assessment considerations.

Consideration of the need for any broader changes should be addressed through the IAASB's proposed Audit Evidence project, when matters can be considered on a more holistic basis across the audit, taking into account the implications for the execution standards. For example, what evidence (credit) can be taken from analysing 100% of a population, or what if such analysis concludes there are no apparent anomalies and hence no risk – is some form of further testing still needed?

4. Do the proposals sufficiently support the appropriate exercise of professional scepticism throughout the risk identification and assessment process? Do you support the proposed change for the auditor to obtain "sufficient, appropriate audit evidence" through the performance of risk assessment procedures to provide the basis for the identification and assessment of the risks of material misstatement, and do you believe this clarification will further encourage professional scepticism?

We support reinforcing the importance of maintaining professional scepticism in performing risk assessment procedures and in identifying and assessing risks of material misstatement. We do not, however, support the change in paragraph 17 to obtain "sufficient appropriate audit evidence" as the basis for the identification and assessment of risks of material misstatement as it creates an open-ended judgement. Seeking to have the auditor question whether their basis is sufficient is well intentioned and a principle we support. However, linking this to the concept of sufficient appropriate audit evidence is, in our view, problematic as drafted.

The concept of "sufficient appropriate audit evidence" in the ISAs defines the threshold of evidence needed on which to form a conclusion or opinion. It is a concept that requires context. For example, ISA 500 explains that "reasonable assurance" is achieved when the auditor has obtained sufficient appropriate audit evidence to reduce audit risk to an acceptably low level (audit risk being a well-defined and understood term in the auditing profession). We also acknowledge that ISA 500 states that audit evidence is obtained from performing risk assessment procedures. However, ISA 500 does not set a threshold for a level of audit evidence from such procedures, in the way in which the concept is applied to forming an opinion. Therefore, we believe this is an inappropriate extension of the concept to the risk assessment procedures. As such, with respect to ISA 315 either the standard needs to define the threshold, or it needs to articulate how much evidence is enough by being explicit in the requirements about the procedures the auditor must perform in order to have obtained sufficient appropriate audit evidence. As drafted, the threshold is undefined, judgmental and, therefore, open to differing interpretation. We believe the previous wording in extant ISA 315 remains appropriate, with the requirements in the ISA clearly defining the nature and scope of understanding that provides that basis. The sufficiency and appropriateness of evidence to support the risk assessment is also relevant to IAASB's upcoming audit evidence project. The IAASB may wish to consider deferring this proposed change pending a more holistic consideration of the concept of the sufficiency and appropriateness of evidence as part of the ISA 500 project, including how it relates to risk assessment. A conforming amendment can then be made to ISA 315 as part of that project if necessary.

The specificity of the revised requirements on understanding the entity, its environment and the financial reporting framework are useful in focusing the auditor on what is important to understand in informing their risk assessment and will, we believe, aid professional scepticism. However, the overall complexity of the standard could inadvertently undermine the intended reinforcement of the importance of professional scepticism due to auditors focusing on seeking to understand and comply with the requirements, rather than standing back and applying a questioning mind based on their enhanced understanding.

See also our response to question 6, which includes our views on how the concept of inherent risk factors could be amended, to enhance further professional scepticism.

5. **Do the proposals made relating to the auditor's understanding of the entity's system of internal control assist with understanding the nature and extent of the work effort required and the relationship of the work effort to the identification and assessment of the risks of material misstatement? Specifically:**
    a. **Have the requirements related to the auditor's understanding of each component of the entity's system of internal control been appropriately enhanced and clarified? Is it clear why the understanding is obtained and how this informs the risk identification and assessment process?**

While we believe that the requirements in relation to the understanding of the system of internal control are reasonable when applied in the context of a large, more complex audit, as noted in our cover letter and response to question 2, we do not believe the standard has effectively addressed questions over the scalability of obtaining this understanding when applied to smaller or less complex audits. We believe that the requirements need further clarification for circumstances where the auditor does not plan to seek to obtain audit evidence from evaluating the design and operating effectiveness of controls. We have suggested a two-step model that we believe better reflects the move to performing separate assessments of inherent and control risk (see also our recommendations with respect to control risk).

We do not believe a detailed understanding of all control activities is necessary, although we acknowledge that some awareness of controls may be of use in understanding where management has determined there to be inherent risk that needs to be managed. Drawing on the concept in paragraph 36 of the ED, when obtaining an understanding of the information system, the auditor will obtain a basic understanding of where the entity has put in place controls relevant to financial reporting that relate to classes of transactions, account balance or disclosures that are significant to the financial statements, or that address journal entries. When the auditor expects to place reliance on controls through testing their operating effectiveness, a detailed understanding of those control activities on which the auditor plans to rely would be required, including evaluating their design and implementation.

Our suggested redrafted requirements in Appendix 2 identify the matters we believe are relevant to understand for an inherent risk assessment (and therefore required for all audits), and the additional understanding that is relevant when the auditor plans to place reliance on controls. We believe such an approach would be more directly responsive to calls for scalability and bring additional clarity to the nature and extent of understanding that is always necessary when the auditor does not plan to seek to obtain audit evidence from evaluating the design and operating effectiveness of controls. This is an area that lacked clarity in the extant ISA and we believe it is possible to much more clearly articulate the understanding needed.

Appendix 4 presents our suggestions in Appendix 2 for restructured requirements visually in the form of a flowchart. As we noted in our response to question 1, we would be happy to work with the Board's Task Force to explain our thinking and help further develop this approach.

We are supportive of the intent of the Board's flowchart developed in relation to understanding the system of internal control, together with the new material trying to better describe direct and indirect controls. We believe the Board's flowchart could be revised to incorporate our alternative structure described above.

We also support the changes to terminology to address inconsistent and confusing use of specific terms such as "controls", "internal control" and "internal controls".

b. **Have the requirements related to the auditor's identification of controls relevant to the audit been appropriately enhanced and clarified? Is it clear how controls relevant to the audit are identified, particularly for audits of smaller and less complex entities?**

We welcome the intent of paragraph 39. Explicitly describing those controls that the auditor must always consider will eliminate confusion that exists in applying extant ISA 315. However, we believe the standard can give direction on those controls the auditor must always understand without specifically needing to define a term for such controls. This is reflected in our suggested alternative requirements described above.

With respect to the requirements as proposed in the ED, the understanding and interpretation of the flow and interaction of paragraphs 26, 36, 38, 39 and 40-42 is critical to success. In that regard we have a number of observations and concerns.

We are unclear as to the purpose of paragraph 26 and suggest further consideration be given as to whether it is necessary or can be deleted.

We do not support proposed paragraph 36. Paragraph 39 identifies the controls for which the auditor must obtain an understanding. However, the intent of paragraph 36 appears to be that all controls within the information system that fall within the scope of the requirement (see related comment below) must be identified and an evaluation of their design and whether they have been implemented performed. It will aid understanding if all controls the auditor needs to understand and evaluate are addressed in one clear requirement.

However, we disagree that all information system controls need to be understood and evaluated. Evaluating the design and implementation primarily serves to support a controls based approach and, in our view, this requirement imposes a level of work effort on audits that may not plan to place reliance on controls, in particular for smaller and less complex entities, that we do not believe is necessary.

The wording of paragraph 38 also could cause confusion. Extant ISA 315 equated obtaining an understanding of the control activities "component" to understanding and identifying controls relevant to the audit. Referring to identifying the controls relevant to the audit "in" the control activities component is a confusing concept. As the application material describes, such controls are typically controls over the entity's information system, but also may be controls in other components.

While we believe the defined term is unnecessary, we welcome the clarity brought by describing those direct controls which the auditor is always required to treat as "relevant" (paragraph 39(a)-(d)). However, paragraph 39(e) is, in our view, problematic. Leaving an open-ended judgement as to any other control for which it is "appropriate" to evaluate its design, and determine whether it has been implemented, undermines the clarity provided by other elements of the requirement. This retains the ambiguity of this concept that exists today. If none of items (a)-(d) are triggered, and specifically, under (d), when the auditor does not intend to rely on controls, then we see no circumstances when (e) becomes applicable. We believe paragraph A179 is further application material that is relevant to judgements the auditor needs to make relevant to (d). Alternatively, the requirement needs to go further to define the criteria or circumstances when it would be "appropriate" – if this cannot be done, then we question whether this belongs as a requirement.

Furthermore, coupling the judgemental requirement of (e) with the overarching requirement to obtain "sufficient appropriate audit evidence" from the auditor's risk assessment procedures, as a whole, results in a highly subjective and unclear threshold as to how much work is expected of the auditor.

We seek to address each of the points described above in our initial outline of suggested redrafted requirements in Appendix 2. In our suggestions and in our comments in Appendix 3, we note that we do not believe it is necessary that all controls over journal entries be mandated as relevant, as this should be based on the assessed risks.

We interpret paragraphs 39 through 42 as a funnel. In other words, paragraph 39 requires the identification of controls relevant to the audit, which determines the scope of the auditor's identification of IT applications and other aspects of the IT environment that may be relevant to the audit – i.e., in which applications or other IT aspects do those controls sit. Paragraph 41 then requires GITCs relevant to the audit to be identified based on the scope of applications determined in paragraph 40. Making this thought process clear is essential to consistent application. However, aspects of the application material seem to contradict this "funnel" approach. See our comments in Appendix 3 on paragraphs A180-A181.

With respect to paragraph 41(b), we believe the application guidance could provide further direction on how "relevant to the audit" is to be considered with respect to GITCs. Appendix 4 to the ED could perhaps be expanded to address such considerations and we would be happy to provide further input. Alternatively, if the intent is actually to say that for IT applications and other aspects of the IT environment relevant to the audit the auditor should identify the GITCs, i.e., without a further scoping judgement as to relevance, then we suggest deleting the condition "relevant to the audit" here as it may otherwise confuse.

c. Do you support the introduction of the new IT-related concepts and definitions? Are the enhanced requirements and application material related to the auditor's understanding of the IT environment, the identification of the risks arising from IT and the identification of general IT controls sufficient to support the auditor's consideration of the effects of the entity's use of IT on the identification and assessment of the risks of material misstatement?

The introduction of the IT related concepts and definitions and additional guidance on considerations relevant to the IT environment, IT applications and General IT Controls are useful additions that reflect the fundamental importance to financial reporting that IT now has. The IT flowchart is also useful and could be added as a helpful appendix to the standard. As noted in our response to question 1, given this importance we believe there is merit in drawing out the role of IT and linking this with scalability considerations i.e., that the extent of the auditor's understanding may be less in smaller and less complex entities due to the sophistication of IT systems and related documentation.

See also our comments on part (b) of this question with respect to paragraphs 40 and 41. In addition, we suggest that the application material could better explain the importance of general IT controls in providing a basis for the operation of direct controls.

Lastly, we suggest that a definition of "information system" be added to the standard to help distinguish this concept from the definition of IT environment and its constituent elements (as shown on the flowchart). This would help to set the understanding for the requirements that follow.

We also provide some specific comments on areas of clarification in our detailed comments in Appendix 3.

6. Will the proposed enhanced framework for the identification and assessment of the risks of material misstatement result in a more robust risk assessment?

In a number of respects, we find the proposed requirements in the ED less clear than extant ISA 315, for reasons that we explain in our cover letter and response to question 1. We further explain our concerns on those matters in response to each part of this question below.

Risks of material misstatement

In several places in the proposed standard the term "risk of material misstatement" is used. Specifically, we draw attention to paragraph 45 where the term is used, as we understand it, to mean forming an initial view of where "risks" exist. Paragraphs 48 and 50 go on to require the auditor to assess inherent and control risk "for the identified risks of material misstatement". As the definition of RoMM is a function of inherent and control risk, as defined in ISA 200, we find this confusing and circular.

We understand that the intent was, as noted, to require a preliminary identification of potential risks – a so-called "educated guess" – from which the auditor would go on to then formally assess inherent and control risk. This is not clear from the proposed requirements. Paragraph 45 looks very similar to the requirement in paragraph 25 of extant ISA 315. However, in the extant standard, this was not positioned as an initial view, but instead acts as the overarching requirement, or outcome to be achieved, with subsequent paragraphs making clear how that is to be achieved. For example, paragraph 26 of the extant standard specifically states "for this purpose, the auditor shall…", and paragraph 27 states "As part of the risk assessment as described in paragraph 25…". The interrelationship of the requirements is therefore clear. The language used in the ED - "for the identified risks of material misstatement" - lacks this clarity. Coupled with the interaction of the proposed definitions of significant classes of transactions, account balances and disclosures ("SCOTABD") and relevant assertion (see below), it is unclear whether the auditor first identifies SCOTABD and then makes the "educated guess", or vice versa. This becomes challenging to understand and implement. Significant interpretation is therefore required to understand what is being asked of the auditor and how these various requirements interact, which we are concerned may lead to inconsistent practice. We believe this can be simplified and the initial outline of our suggested redrafted requirements shown in Appendix 2 seek to better delineate consideration of inherent risk and control risk in arriving at the risks of material misstatement.

Specifically:

a. Do you support separate assessments of inherent and control risk at the assertion level, and are the revised requirements and guidance appropriate to support the separate assessments?

We support the explicit introduction of requiring a separate assessment of inherent risk. However, while we support the concept we believe the manner in which the requirements have been drafted can be clarified. We comment in our overarching points above on the circularity and confusion created by the separation of the identification and assessment requirements, the "educated guess" and the use of the term risk of material misstatement. As described in our cover letter we also believe there is an opportunity to reframe the control risk element of the audit risk equation to focus more explicitly on the fact that this can be accomplished through the auditor's assessment of the extent to which the auditor plans to obtain evidence from testing the operating effectiveness of controls to reduce audit risk to an acceptably low level.

Control risk

Audit risk is a well understood concept, being the product of both inherent and control risk. However, we believe that control risk is often misunderstood as a concept. In discussions, we often hear that some confuse the concept of "control risk" as implying a possible increase in inherent risk.

We agree with the introductory and application material that explains that this concept is more commonly thought of today, in the context of planning an audit, in terms of the auditor's "planned controls reliance" i.e., where the auditor expects to be able to obtain evidence to reduce the overall risk of material misstatement by testing the operating effectiveness of controls. We believe more can be done within the requirements themselves to make this linkage clearer.

In a financial statement audit, once inherent risk has been assessed, the auditor's concern is obtaining audit evidence to reduce that risk to an appropriately low level. It is not necessary for the auditor to make a discrete identification and assessment of control "risk" similar to what is needed when the auditor plans an audit designed to give an opinion on internal control. Instead, the auditor's focus is whether to obtain evidence in response to an identified inherent risk from evaluating the design, and testing operating effectiveness, of controls, or from performing substantive procedures, or from a combination thereof. While the risk of material misstatement comprises both inherent risk and control risk, the latter concept is more readily understandable, and better supports scalability in the risk assessment and planning stage of the audit, by focussing on assessing the "planned control reliance".

Reframing the control risk part of the traditional audit risk equation to focus on planned controls reliance was not possible in the extant ISA because a combined risk assessment was allowed (i.e., the auditor's risk assessment could be a combined assessment of inherent risk taking into account the expected effectiveness of related controls). Because inherent risk is now proposed to be a separate assessment, there is now an opportunity to simplify and bring clarity to the area of the extant ISA that has caused the most confusion.

In our view, reframing the proposed separate assessment of control risk to more explicitly focus on the fact that this can be accomplished through the auditor's assessment of the extent to which the auditor plans to obtain evidence from testing the operating effectiveness of controls would also bring clarity within the standard to how much understanding of direct controls is needed – see our response to question 5 for further detail. This is an area that requires clarification, particularly for those circumstances when the audit approach is expected to be based primarily on substantive procedures.

We acknowledge that the application material that discusses control risk is an attempt to reconcile control risk and planned controls reliance (e.g., if the auditor is not intending to test the operating effectiveness of controls, control risk is assessed at maximum), but application material is not the solution to fixing a broader problem of misunderstanding. We believe the requirements could better support this concept.

In addition, we believe reframing control risk in this way would help more clearly illustrate that firms may think about this assessment within their methodologies in a variety of ways, including by considering how planned controls reliance can appropriately reduce the overall risk of material misstatement.

We believe that the required separate identification and assessment of control risk may exacerbate the confusion about the objective of a financial statement audit if the necessary clarity described above is not provided. Without this clarification, referring more explicitly to control risk identification and assessment, together with the new requirements on control deficiencies, promotes expectations that auditors are forming a view on the overall effectiveness of an entity's controls. That is not part of an ISA audit.

See also our comments in response to questions 2 and 5 on the nature and extent of understanding of controls to support the decision around planned reliance.

b. Do you support the introduction of the concepts and definitions of 'inherent risk factors' to help identify risks of material misstatement and assess inherent risk? Is there sufficient guidance to explain how these risk factors are used in the auditor's risk assessment process?

Inherent risk factors were introduced as a concept in the recently approved ISA 540 (Revised), and we believe that how this concept was incorporated into that standard will lead to risk assessments that better identify the reasons underlying inherent risk and enable auditors to tailor their responses more appropriately. However, how they have been introduced into the proposed ED is slightly different and we find that it does not work as well as in ISA 540 (Revised).

For example, we find the definition to be confusing by referring to "characteristics of events or conditions". What matters is the characteristics inherent to a particular class of transactions, account balance or disclosure; not the characteristics of the events or conditions.

In making a proper risk assessment, we believe it would be more helpful to distinguish between external factors that influence an entity's risks from internal company-specific risk factors, rather than combining these under a single construct. External factors, events or conditions are not inherent to an item, but are still relevant factors to take into account. In that regard, we recommend adopting an approach similar to the PCAOB's articulation of internal and external factors. We believe this would bring greater clarity and be more understandable.

We are concerned about the inclusion of susceptibility to misstatement due to management bias or fraud as a discrete inherent risk factor in ISA 315 (Revised) given the interaction between ISA 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of the Financial Statements* (ISA 240) and ISA 315 (Revised) that exists today. Paragraph 25 of ISA 240 already requires the auditor to identify and assess the risks of material misstatement due to fraud at the financial statement level and at the assertion level for classes or transactions, account balances and disclosures. ISA 240 also sets out robust fraud risk factors for the auditor to evaluate. Inclusion as a separate inherent risk factor in ISA 315 (Revised) may lead to confusion between the two standards, or in how the two standards interact. We also note that susceptibility to fraud may also arise as a result of a weak control environment or deficiencies in internal control. Therefore, we do not believe this can be thought of in the context of inherent risk only, in isolation from understanding the entity's system of internal control.

In removing the risk factor, to maintain a focus on the importance of considering risks arising from fraud, we suggest the standard could clarify the relationship between ISA 240 and ISA 315 (Revised), by referring to the requirements and guidance in ISA 240 as additional application material in paragraph A6 of the Exposure Draft. Alternatively, if considered necessary, essential application material could be incorporated into paragraph 45 of ISA 315 (Revised) (or our equivalent requirement, paragraph 39) to remind auditors that the auditor's risk assessment includes the auditor's assessment of the risk of material misstatement due to fraud in accordance with paragraph 25 of ISA 240.

We comment further in our response to question 9 on the proposed conforming amendments to ISA 240.

c. In your view, will the introduction of the 'spectrum of inherent risk' (and the related concepts of assessing the likelihood of occurrence, and magnitude, of a possible misstatement) assist in achieving greater consistency in the identification and assessment of the risks of material misstatement, including significant risks?

We support making explicit the concept of the spectrum of inherent risk, which is implicit in the extant standard. This is an important concept linked with the principle in ISA 330 that the higher the assessed risk the more persuasive the audit evidence needed. As a principle-based concept, firm methodologies will therefore continue to play an important role in how this is implemented in practice. We anticipate the existing approaches of firms will likely continue using terms, for example, such as low/medium/high. That is compatible with the concept, and the additional application material provided in the ED should prove useful in reinforcing understanding.

See also our comments in relation to significant risks in response to part e) below.

d. **Do you support the introduction of the new concepts and related definitions of significant classes of transactions, account balances and disclosures, and their relevant assertions? Is there sufficient guidance to explain how they are determined (i.e., an assertion is relevant when there is a reasonable possibility of occurrence of a misstatement that is material with respect to that assertion), and how they assist the auditor in identifying where risks of material misstatement exist?**

We agree that the auditor needs to consider the classes of transactions, account balances and disclosures that are significant to the financial statements. This is a relevant scoping decision. The auditor also thinks about risks and to which assertions those risks relate. In that regard, we support the broad intent of the concept of SCOTABD. However, we do not agree that the relevant assertions are thought of first and then used to drive the scope of what is significant. Rather, having identified a risk, the assertions to which that risk relates are identified, thus becoming “relevant”.

Consequently, while there may be a useful purpose for a definition of significant classes of transactions, account balances and disclosures, its circular definition (using the definition of relevant assertions) needs revision. We believe explaining how to consider what is significant to the financial statements can be described with reference to materiality and relevant qualitative considerations, addressed through application material. Such guidance could explain that COTABD that individually exceed overall materiality would generally be considered significant. COTABD that fall between performance and overall materiality may be deemed significant based on professional judgement. By doing this, a definition of relevant assertions is not needed. Having identified the risk, the auditor can then determine the related assertions.

The use and interrelationship of these definitions adds unnecessary complexity to the requirements and creates challenges in their interpretation and application. The way that they have been applied in the related requirements feels like the proposed revision is driving a specific approach and methodology, rather than being outcome-driven requirements that can be applied as appropriate to audits of entities with differing characteristics. We believe this is contrary to the IAASB’s intent to allow flexibility, recognising various firm methodologies.

We recognise that the definition of relevant assertion incorporates the threshold developed by the IAASB for determining what is significant. We believe the notion of reasonable possibility can be built into the application material, alongside consideration of materiality and qualitative factors, to determine significance.

Linked to our comment on question 1, we are also concerned at the implications for documentation resulting from the relationship between these definitions and the requirement to assess inherent risk, taking into account the inherent risk factors, for all SCOTABD, which we believe will result in a complex documentation exercise by risk factor and assertion.

We believe the intent can be achieved without the need for these definitions, as set out in our suggestions in Appendix 2.

e. **Do you support the revised definition, and related material, on the**

determination of 'significant risks'? What are your views on the matters presented in paragraph 57 of the Explanatory Memorandum relating to how significant risks are determined on the spectrum of inherent risk?

We do not agree that significant risks should be defined by reference to likelihood "or" magnitude, which will result in items that do not represent a significant risk being unnecessarily defined as such, for example, certain classes of transactions, account balance or disclosure that may be highly material but for which the likelihood of misstatement is very low.

We do not believe that balances that simply have a high magnitude, of themselves, sit at the upper end of the spectrum of inherent risk - for example, a significant fixed asset, for which the risk of misstatement is low, should not be captured by the definition of a significant risk. In fact, the proposed definition of significant risk that includes stating "<u>or</u> the magnitude of potential misstatement" could be interpreted as implying that any material balance in the financial statements is at the upper end of the spectrum of inherent risk simply because if misstated, the financial statements could be materially misstated.

The category of "significant risk" is used in the ISAs to set requirements for those areas in the audit that warrant greater focus and more persuasive evidence. Other ISAs (in particular ISA 330) set out the additional work effort that is required in relation to such risks, including, when the auditor plans to rely on controls that address a significant risk, requiring that those controls be tested in the current period. Such requirements are warranted to reduce the risk of material misstatement for those areas in the audit subject to higher inherent risk to an acceptably low level. It is one of the ways that the ISAs demonstrate how to design an appropriately risk-based audit with more audit attention on areas of heightened risk. In our view, however, these procedures are unnecessary to reduce risk to an acceptably low level for classes of transactions, account balances or disclosures that may be material, even highly material, but that have a low likelihood of misstatement. In fact, doing so may risk distracting auditor attention away from areas with a higher likelihood, and reducing scepticism by suggesting that all material items are, in a sense, worthy of "equal" audit work.

If the IAASB believes that there are specific matters that should be considered in relation to material balances that would not be addressed by complying with the requirements other than those addressing significant risks, those matters should be articulated separately in requirements specifically targeted at that category.

If the intention of the change is to seek to address populations that may seem to be low risk at a transaction level, but when aggregated into a single population have a heightened risk profile, then we would instead propose that additional application material make this specific point rather than amending the definition to be likelihood "or" magnitude.

We also believe the Board needs to make clear if the intent of the requirements is that at least one significant risk would always be identified. We do not believe that is the intent, nor that this is the case, but the recent webinars have not helped our understanding in this respect.

7. **Do you support the additional guidance in relation to the auditor's assessment of risks of material misstatement at the financial statement level, including the determination about how, and the degree to which, such risks may affect the assessment of risks at the assertion level?**

We fully support the need to consider how pervasive risks might increase the risk at the assertion level for a particular financial statement item. However, we find the articulation of the requirements addressing the relationship between risks at the financial statement level and risks at the assertion level to be unclear. We agree that the auditor *takes into account* the potential effect of financial statement level risks when thinking about risks at the assertion level. However, it is unclear how the auditor is supposed to determine "the degree to which" financial statement level risks affect the assessment of risks of material misstatement at the assertion level - how is this to be measured and what are the consequences of varying degrees? The application material does not address this aspect of the requirement. This same concern also applies to paragraph 48(b). Furthermore, the requirement to "determine" an effect also implies a quantifiable judgement, which we believe is unrealistic and creates an onerous and impractical documentation expectation. We also question the intent of the requirement in paragraph 47(a), given the almost identical requirement in paragraph 48(b).

8. What are your views about the proposed stand-back requirement in paragraph 52 of ED-315 and the revisions made to paragraph 18 of ISA 330 and its supporting application material? Should either or both requirements be retained? Why or why not?

We support the retention of paragraph 18 of ISA 330. For the reasons described in our previous responses with respect to the definition of SCOTABD, we do not support the proposed ISA 315 stand-back.

We believe ISA 330 provides a more robust stand-back requirement to guard against a flawed risk assessment as it addresses procedures that would be required for all material classes of transactions, account balances and disclosures. If the core requirements in ISA 315 are clearly drafted, fit for purpose and appropriately followed by auditors, there should be no need for an intermediate stand-back in ISA 315 and the safeguard provided by paragraph 18 of ISA 330 should be sufficient.

Under the proposed 315 model, we find this stand-back to be redundant. Given the concept of "relevant assertion" uses the threshold "more than remote", the auditor should have identified all classes of transactions, account balances and disclosures for which there could be a potential risk of material misstatement. However, assuming all risks were not adequately identified, asking the auditor to simply revisit their judgement that there were no relevant assertions is unlikely to result in a change in view and thus does not guard against a flawed risk assessment. This is consistent with the findings from our field-testing. The majority of engagement teams concluded no further risks were identified. However, there continues to be confusion between the concept of "relevant assertion" when applied to disclosures, specifically in relation to the presentation (and disclosure) assertion. This is, however, not a stand-back related issue but a broader challenge to be addressed in relation to the description of assertions. We believe this is evidence that the increased complexity of the proposed requirements creates the potential for increased inconsistent judgements, placing even greater emphasis on the need to retain the current safeguard provided by ISA 330 paragraph 18.

9. With respect to the proposed conforming and consequential amendments to:

   a. ISA 200 and ISA 240, are these appropriate to reflect the corresponding changes made in ISA 315 (Revised)?

   b. ISA 330, are the changes appropriate in light of the enhancements that have been made in ISA 315 (Revised), in particular as a consequence of the introduction of the concept of general IT controls relevant to the audit?

   c. The other ISAs as presented in Appendix 2, are these appropriate and complete?

   d. ISA 540 (revised) and related conforming amendments (as presented in the Supplement to this exposure draft), are these appropriate and complete?

Our detailed comments on the conforming amendments are included in Appendix 3 to this letter. We note that, where we have raised comments on the concepts, terms or language of the requirements in

ISA 315, we have not repeated those comments in relation to the conforming amendments in response to this question. We have, however, indicated in Appendix 3 those paragraphs that we believe would need to be amended based on our comments. We also make the following additional observations:

ISA 240

We continue to believe that the inclusion of both "susceptibility to misstatement due to management bias or fraud" and the fraud risk factors, and the notion that incentives, pressures or opportunities arise from conditions that create susceptibility, is potentially circular and confusing. We support retention of the fraud risk factors as defined in ISA 240 and do not support the proposed inherent risk factor in ISA 315. Consequently, we do not believe the proposed conforming changes are appropriate.

ISA 330

Consistent with our comment on paragraph 21 of proposed ISA 315 (Revised) in Appendix 3, we are not convinced of the need to add "reliability" in paragraph 14 and related application paragraphs. It is unclear why the passage of time affects the reliability of evidence that was previously assessed as reliable. We note that the example in the application material only explains why evidence may no longer be relevant.

We support the amendments made in relation to GITCs, and believe these to be useful additions.

With respect to the changes made to paragraph A1, we are unclear as to the reason for including reference to changing performance materiality and why such a change arises as a conforming amendment from proposed ISA 315.

ISA 540

We note that the proposed amendment to paragraphs A39 and A86 could be construed as suggesting that evaluating the design and implementation of model controls provides audit evidence that, on its own, can be used to reduce the overall level of substantive evidence required to address the risk. We do not believe that is the intent and recommend this be clarified to be consistent with the position set out in the ED that *"[…] the risk assessment procedures to obtain audit evidence about the design and implementation of controls relevant to the audit are not sufficient to test the operating effectiveness of controls (and thus assess control risk below the maximum) […]".*

10. Do you support the proposed revisions to paragraph 18 of ISA 330 to apply to classes of transactions, account balances or disclosures that are 'quantitatively or qualitatively material' to align with the scope of the proposed stand back in ED-315?

While we do not support the proposed stand back in ISA 315, as explained in our response to question 8, we are supportive of the change proposed to ISA 330, as this does not, in our view, change the intended application of the requirement. While materiality by definition includes consideration of both quantitative and qualitative factors, we believe this will act as a useful reminder that there may be financial statement items, in particular disclosures, that although not quantitatively material may be material for qualitative reasons.

11. In addition to the requests for specific comments above, the IAASB is also seeking comments on the matters set out below:

   a. Translations - recognizing that many respondents may intend to translate the final ISA for adoption in their own environments, the IAASB welcomes comment on potential translation issues respondents note in reviewing the ED-315.

We make two observations with respect to translation. First, the significant length of the standard will inevitably require additional time and effort in translation. The Board should look for further opportunities to streamline the content.

Secondly, we have commented on the complexity of the ED, specifically the interrelationships between several new concepts and definitions, which we believe may be confusing and risks inconsistent interpretation and application. We suggest that if native English speakers find understanding the text challenging, the problem is likely to be exacerbated through translation.

b. **Effective date - recognizing that ED-315 is a substantive revision, and given the need for national due process and translation, as applicable, the IAASB believes that an appropriate effective date for the standard would be for financial reporting periods beginning at least 18 months after the approval of a final ISA. Earlier application would be permitted and encouraged. The IAASB welcomes comments on whether this would provide a sufficient period to support effective implementation of the ISA.**

We support an effective date expressed in terms of "periods *beginning* on or after", consistent with that recently adopted for ISA 540 (Revised), given this standard affects the planning phase of an audit.

Any such period should begin at least 18 months after the Board's approval of the final ISA.

In fact, this is the minimum period that we believe is necessary to implement the significant revisions and investment into firms' own internal methodologies, training, and related technologies and tools that will result from the proposed revisions – assuming the concerns described in our response are addressed. However, if the definitions and concepts as proposed are retained without revision, a greater implementation period would be necessary to address the implementation challenges we foresee in practice.

In addition, timing of approval also needs to be factored into the decision. Many firms conduct annual training in the April to October period in advance of December year-ends. If the expected approval does not take place on or before September 2019 and moves to December 2019 or later, appropriate consideration should be given to an effective date of periods beginning in the 3rd or 4th calendar quarter of 2021.

Appendix 2 – Suggested restructured and redrafted requirements

The suggestions below represent an initial outline of how we believe the requirements could be restructured and redrafted in a way that meets the Board's objectives in revising ISA 315 and addresses the concerns described in our responses to questions. While these suggestions would benefit from further drafting considerations and input, we felt it useful to illustrate our thinking to assist the Board's further considerations in developing final proposals.

Requirements

Risk Assessment Procedures and Related Activities

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

    - The entity and its environment, in accordance with paragraph 23(a);
    - The applicable financial reporting framework, in accordance with paragraph 23(b); and
    - The entity's system of internal control, in accordance with paragraphs 26-38 and 43-47

    that is sufficient to provide a reasonable basis for the identification and assessment of risks of material misstatement at the financial statement and assertion levels. Risk assessment procedures by themselves do not provide sufficient appropriate audit evidence on which to base the audit opinion.

18. The risk assessment procedures shall include the following:

    (a) Inquiries of management, of appropriate individuals within the internal audit function (if the function exists), and of others within the entity who in the auditor's judgment may have information that is likely to assist in identifying risks of material misstatement due to fraud or error.
    (b) Analytical procedures.
    (c) Observation and inspection.

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

20. If the engagement partner and other key engagement team members have performed other engagements for the entity, the auditor shall consider whether information obtained is relevant to identifying and assessing risks of material misstatement.

21. When the auditor intends to use information obtained from the auditor's previous experience with the entity and from audit procedures performed in previous audits, the auditor shall evaluate whether such information remains relevant as audit evidence for the current audit.

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

Obtaining an Understanding of the Entity and Its Environment and the Applicable Financial Reporting Framework

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

    (a) The entity and its environment, and any changes thereto, including:

        (i) The entity's organizational structure, ownership and governance, and its business model, including the extent to which the business model integrates the use of IT;
        (ii) Relevant industry, regulatory and other external factors; and
        (iii) The relevant measures used, internally and externally, to assess the entity's financial performance.

    (b) The applicable financial reporting framework, including:

        (i) How it applies in the context of the nature and circumstances of the entity and its environment; and
        (ii) The entity's application of the framework through its accounting policies and any changes thereto, including the reasons for any such changes.

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

Determining the Classes of Transactions, Account Balances and Disclosures that are Significant to the Financial Statements

25. The auditor shall determine the classes of transactions, account balances and disclosures that are significant to the financial statements.

Obtaining an Understanding of the Entity's System of Internal Control to Identify and Assess Inherent Risk

26. In performing risk assessment procedures to obtain an understanding of the entity's system of internal control, including the entity's use of IT, sufficient to provide a reasonable basis to identify and assess inherent risk, the auditor shall obtain an understanding of the components of internal control addressed by the requirements set out in paragraphs 27 to 37.

Control Environment

27. The auditor shall obtain an understanding of the control environment relevant to financial reporting, including understanding how the entity:

    (a) Demonstrates a commitment to integrity and ethical values;
    (b) When those charged with governance are separate from management, demonstrates how those charged with governance exercise oversight of the entity's system of internal control, including as appropriate, their independence from management;
    (c) Establishes, with the oversight of those charged with governance, structures, reporting lines, and appropriate authorities and responsibilities, in pursuit of its objectives;

(d) Demonstrates a commitment to attract, develop, and retain competent individuals in alignment with its objectives; and
(e) Holds individuals accountable for their responsibilities in the pursuit of the objectives of the system of internal control.

28. Based on the auditor's understanding of the control environment, in accordance with paragraph 27, the auditor shall evaluate whether:

(a) Management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior; and
(b) The strengths in those areas of the entity's control environment addressed in paragraphs 27(a) to (e) collectively provide an appropriate foundation for the other components of the system of internal control, or whether those other components are undermined by control deficiencies in the control environment component.

The Entity's Risk Assessment Process

29. The auditor shall obtain an understanding of the entity's risk assessment process, including the extent to which it is formalized, by understanding:

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

(i) Identifies business risks relevant to financial reporting objectives;
(ii) Assesses the significance of those risks, including the likelihood of their occurrence; and
(iii) Addresses those risks.

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

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

31. Based on the auditor's understanding of the entity's risk assessment process in accordance with paragraph 29 and, if applicable, paragraph 30, the auditor shall:

(a) Evaluate whether the nature of the entity's risk assessment process, including the extent to which it is formalized, is appropriate to the entity's circumstances considering the nature and size of the entity; and
(b) If not, consider the implications of the lack of an appropriate risk assessment process for the audit and for the auditor's consideration of control deficiencies in paragraphs 48 and 49.

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

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

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

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

34. If the entity has an internal audit function, the auditor shall obtain an understanding of the nature of the internal audit function's responsibilities, its organizational status, and the activities performed, or to be performed.

The Information System and Communication

35. The auditor shall obtain an understanding of the information system relevant to financial reporting, including the related business processes, through understanding:

    (a) How information relating to classes of transactions, account balances and disclosures that are significant to the financial statements flows into, through and out the entity's information system, whether manually or using IT, and whether obtained from within or outside of the general ledger and subsidiary ledgers. This understanding shall include how:

        (i) Transactions are initiated, and how information about them is recorded, processed, corrected as necessary, and incorporated in the general ledger and reported in the financial statements; and
        (ii) Information about events and conditions, other than transactions, is captured, processed and disclosed in the financial statements.

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

    (c) The financial reporting process used to prepare the entity's financial statements from the records described in paragraph 35(b), including as it relates to:

        (i) Controls over journal entries, including non-standard journal entries used to record non-recurring unusual transactions or adjustments; and
        (ii) Disclosures, and to accounting estimates relating to classes of transactions, account balances and disclosures that are significant to the financial statements;

    (d) The entity's IT environment relevant to (a) through (c) above.

36. Based on the understanding obtained in accordance with paragraph 35(d), the auditor shall identify the IT applications and the other aspects of the entity's IT environment that are relevant to financial reporting. In doing so, the auditor shall take into account whether the IT applications include or address:

    (a) Automated controls that management is relying on and on which the auditor may intend to rely in obtaining audit evidence;
    (b) Maintenance of the integrity of information stored and processed in the information system that relates to classes of transactions, account balances or disclosures that are significant to the financial statements;
    (c) System-generated reports on which the auditor intends to rely; or
    (d) Controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.

37. For the IT applications and other aspects of the IT environment identified in paragraph 36, the auditor shall identify the risks arising from the use of IT.

38. The auditor shall obtain an understanding of how the entity communicates financial reporting roles and responsibilities and significant matters relevant to financial reporting, including:

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

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

Identifying and Assessing Inherent Risk

39. Based on the auditor's understanding obtained in accordance with paragraphs 23-38, the auditor shall identify and assess inherent risk by applying the requirements in paragraphs 40 and 41 to each class of transactions, account balance, and disclosure that is significant to the financial statements, determined in accordance with paragraph 25.

40. The auditor shall identify and assess inherent risk by assessing the likelihood and magnitude of material misstatement. In doing so, the auditor shall:

   (a) Identify and assess risks that exist at the financial statement level, by evaluating whether the risks relate more pervasively to the financial statements as a whole, including potentially affecting many assertions, to provide the basis for designing and implementing overall responses to the assessed risk of material misstatement at the financial statement level in accordance with ISA 330.

   (b) Identify and assess risks at the assertion level for the classes of transactions, account balances and disclosures determined in accordance with paragraph 25. In doing so, the auditor shall take into account:
      (i) How, and the degree to which, such classes of transactions, account balances and disclosures are subject to, or affected by, the inherent risk factors; and
      (ii) How the risks at the financial statement level affect the assessment of inherent risk at the assertion level.

Significant Risks

41. The auditor shall determine, based on the auditor's assessment of inherent risk, whether any of the assessed risks are significant risks.

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

42. The auditor shall determine, for any of the assessed inherent risks at the assertion level, whether substantive procedures alone cannot provide sufficient appropriate audit evidence.

Obtaining a Further Understanding of the Entity's System of Internal Control to Determine Planned Reliance on Controls

43. The auditor shall perform additional risk assessment procedures to provide a reasonable basis to determine the auditor's planned audit approach in response to the assessed inherent risks at the financial statement and assertion levels by obtaining a further understanding of the components of the entity's system of internal control addressed by the requirements set out in paragraphs 44-47.

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

44. The auditor shall obtain an understanding of any control deficiencies identified by management that are relevant to identified and assessed inherent risks at the assertion level to inform the

auditor's judgments as to whether to seek audit evidence by testing the operating effectiveness of controls.

Control Activities

45. The auditor shall identify controls that address assessed inherent risks:

    (a) For which substantive procedures alone do not provide sufficient appropriate audit evidence;
    (b) That have been identified as significant risks; and
    (c) For which the auditor intends to obtain evidence through testing their operating effectiveness, taking into account the understanding obtained in accordance with paragraph 44.

    It is a matter of the auditor's professional judgment as to whether to seek audit evidence from testing the operating effectiveness of a control, individually or in combination with other controls.

General IT Controls

46. The auditor shall identify the general IT controls that are relevant to the auditor's planned audit approach in response to the assessed inherent risks at the financial statement and assertion levels, taking into account the results of applying paragraphs 36, 37 and 45.

Evaluating Control Design and Implementation

47. For each control identified in accordance with paragraphs 45-46, the auditor shall:

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

Control Deficiencies Within the System of Internal Control

48. If, based on the work performed in accordance with this ISA, the auditor identifies one or more deficiencies in the system of internal control, the auditor shall determine whether, individually or in combination, they constitute significant deficiencies and respond accordingly, in accordance with ISA 265.

49. The auditor shall consider the implications for the audit of one or more control deficiencies in the system of internal control relevant to financial reporting, including for:

    (a) The determination of risks of material misstatement at the assertion level in accordance with paragraph 51; and
    (b) Designing and implementing overall responses to address the assessed risks of material misstatement as required by ISA 330.

Assessing Control Risk Taking Into Account Planned Control Reliance

50. Based on the auditor's understanding obtained in accordance with paragraphs 44-49, the auditor shall determine those controls for which the auditor is either required, or plans, to test their operating effectiveness in designing and implementing overall responses to address the assessed risks of material misstatement as required by ISA 330 ("planned control reliance") and

assess the related control risk. If the auditor does not plan to perform tests of controls, the auditor's determination of the risks of material misstatement at the assertion level, in accordance with paragraph 51, shall not take into account the effective operation of controls with respect to that assertion[2].

Determining the Risks of Material Misstatement

51. Based on the assessments of inherent risk and control risk in accordance with paragraphs 40 and 50, the auditor shall determine the risks of material misstatement, for the purposes of designing and implementing overall responses to address the assessed risks of material misstatement as required by ISA 330.

Revision of Risk Assessment

52. The auditor's assessment of the inherent risks at the financial statement level and assertion level and planned controls reliance may change during the course of the audit as additional audit evidence is obtained. In circumstances where the auditor obtains audit evidence from performing further audit procedures, or if new information is obtained, either of which is inconsistent with the audit evidence on which the auditor originally based their determination of the risks of material misstatement, the auditor shall revise the assessment of inherent risk or planned controls reliance and modify the planned responses or further audit procedures accordingly.

Documentation

53. The auditor shall include in the audit documentation:

(a) The discussion among the engagement team, when required in accordance with paragraph 22, and the significant decisions reached;
(b) Key aspects of the auditor's understanding obtained regarding the entity and its environment and of each of the components of the system of internal control specified in this ISA; the sources of information from which the auditor's understanding was obtained; and the risk assessment procedures performed;
(c) The controls identified and evaluated in accordance with paragraphs 45-47.
(d) The risks of material misstatement at the financial statement level and at the assertion level determined in accordance with paragraph 51, including significant risks, and the significant judgments made in identifying and assessing the related inherent risks and planned controls reliance.

[2] Application material would also need to address that no "credit" can be taken for having evaluated the design and implementation of identified controls in accordance with paragraph 47.

Appendix 3 - Detailed comments

The below tables set out our detailed recommendations and editorials for content of the standard other than the requirements, which are addressed in our suggestions in Appendix 2.

Table 1 presents our more substantive comments, while Table 2 includes comments of a lesser editorial nature. For the purposes of reviewing the application material, we have focused on the content alone and not sought to remap the application material to our redrafted suggested requirements in Appendix 2. With respect to the conforming amendments in Table 3, where we have made an editorial suggestion in relation to ISA 315, we have not replicated the comment in the other affected ISAs but instead included a cross-reference back to the related ISA 315 paragraph for reference.

Table 1 – Substantive comments

Paragraph	***Comment***
3	We suggest the definition of inherent risk could be simplified: *"Inherent risk is described as the susceptibility, at the ~~of an~~ assertion level, ~~about~~ of a class of transaction, account balance or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls."*
4	We recommend removing the formally defined terms 'significant classes of transactions, account balances and disclosures" and "relevant assertion" (see also paragraph 16(h) and (j) below): *"The required understanding of the entity and the environment, the applicable financial reporting framework, and the system of internal control forms the basis for the auditor's identification of risks of material misstatement. The identification of inherent risks ~~of material misstatement at the assertion level~~ is performed before consideration of any controls. The auditor does so based on an ~~preliminary~~ assessment of inherent risk for classes of transactions, account balances and disclosures that are significant to the financial statements, ~~that involves identifying those risks for which there is a reasonable possibility of material misstatement. In this ISA~~ including consideration of the assertions to which such risks ~~of material misstatement~~ relate ~~are referred to as 'relevant assertions,' and the classes of transactions, account balances and disclosures to which the relevant assertions relate are referred to as 'significant classes of transactions, account balances and disclosures~~.'"* Our further editorial comments below do not address all other use of these defined terms in the standard, which we would similarly recommend be amended accordingly.
6	See comments on articulation of control risk: *"In assessing control risk, the auditor takes into account whether the auditor's further audit procedures contemplate planned reliance on the operating effectiveness of controls (that is, control risk is assessed as less than maximum).*

	The auditor's understanding of the system of internal control forms the basis for the auditor's intentions about whether to place reliance on the operating effectiveness of controls. That is, the auditor may identify specific controls that address the ~~identified~~ inherent risks ~~of material misstatement~~ and for which the auditor intends to test operating effectiveness. If the auditor does not intend to test the operating effectiveness of controls related to certain inherent risks ~~of material misstatement,~~, the auditor~~'s assessment of control risk~~ cannot take into account ~~be reduced for~~ an expectation of the effective operation of controls with respect to the particular assertion in determining the risks of material misstatement (that is, control risk is assessed at maximum)."
9-11	We recommend revising these paragraphs in light of our suggestions in Appendix 2.
16(d)	We understand the intent of referring to controls being "implied through actions". However, we are concerned about how this can then be practically addressed through evaluating design and implementation and testing operating effectiveness, if there is no documentation of such controls. We suggest using the word "evidenced" as shown below, to indicate that there would be a means through which the auditor could further address such controls. We also suggest an additional reference to application controls would be useful. *"Controls – Policies.......* • *Policies are statements of what should, or should not, be done within the entity to effect control. Such statements may be documented, built in to the information system (e.g. Application Controls), explicitly stated in communications, or evidenced through recurring ~~implied through~~ actions and decisions.* *...."*
16(f)	We recommend simplifying the language used to define inherent risk factors and incorporating the notion of internal and external factors. We suggest using application material paragraphs to describe examples of both internal and external factors, rather than building directly into the definition. *"Inherent risk factors - Qualitative or quantitative factors ~~Characteristics of events or conditions~~ that affect the likelihood or magnitude of a potential ~~susceptibility to~~ misstatement of an assertion about a class of transactions, account balance or disclosure, before consideration of controls. Such factors may be internal or external to the entity. ~~qualitative or quantitative, and include complexity, subjectivity, change,~~ and ~~uncertainty or susceptibility to misstatement due to management bias or fraud~~."*
16(h) & (j) & A9	We recommend these definitions be deleted, as we believe they are unnecessary and add undue complexity, for the reasons set out in our question responses.
17	We believe it is important to reflect in application material that the auditor's understanding of the system of internal control is in the context of those aspects of that system that are relevant to financial reporting. The auditor is not required to understand aspects related to operational controls that do not directly, or indirectly, relate to financial reporting.

21 & A40	We question whether it is necessary to add reference to reliability. We do not believe passage of time affects the reliability of information. We believe the extant standard only addressed relevance for that reason.
A5	As noted within our responses, we believe that inherent risk should be separated between internal and external factors and "susceptibility to misstatement due to management bias or fraud" deleted as this is better addressed in ISA 240. In addition we suggest references to "the best available" in the description of "Uncertainty" (in the context of information and data) be replaced with "relevant and reliable" or, alternatively, "appropriate".
A6	We do not believe that materiality and volume are relevant examples to include here. Being subject to differing risks also does not seem to relate to a factor inherent to a class of transaction, account balance or disclosure. Similar to our comments on fraud, we believe consideration of risks arising from related party transactions are best addressed holistically in ISA 550 and therefore would not include a reference to such transactions as a further inherent risk factor.
A10	The third sentence of this paragraph, by referring to the implications for the performance of the audit, appears to retain the extant notion of significant risk being those risks that require special audit consideration. The intent of the revised definition was to remove that circularity issue. It is where the risk sits on the inherent risk spectrum that drives the required audit evidence to reduce that risk to an acceptable level. It is therefore inappropriate, in our view, to suggest that the significance of a risk is driven by the further audit procedures the auditor may need to perform and the amount of evidence that the auditor is required to obtain – those are consequences, rather than drivers, of making such a determination. We therefore propose that this sentence be deleted.
A12	We recommend aligning language referring to control risk with our suggestions on paragraph 6.
A79	It is unclear to us whether share-based payments are being characterised as controversial or an emerging area. We believe these characterisations may not apply to such transactions today, and instead suggest cryptocurrency may be a more current example.
A83-88	See response to question 6(b).
A90	See response to question 4 with respect to the use of the term "sufficient and appropriate audit evidence".
A103	See response to question 5(b). Stating that the control activities component includes general IT controls but then providing an example of a control in the information system component may be confusing. The "For example" also implies that what follows is an example of an indirect control, when instead it describes a direct control, which may also cause confusion. We suggest simplifying the second sentence to state:

	"In particular, general IT controls within the entity's information system may include both direct and indirect controls. For example, ….."
A104	See response to question 5(b) and appendix 2 and re-characterisation of the concept of controls "relevant to the audit" as controls for which the auditor either is required to understand or understands because they plan to place reliance through testing their operating effectiveness. In Appendix 2, we suggest a structure that does not require a separate notion of controls "relevant to the audit". We have not repeated the above comment for all subsequent paragraphs referring to controls relevant to the audit.
A118	We do not believe that the nature, timing and extent of the auditor's risk assessment procedures are determined with the evaluation in paragraph 31 as an objective. We believe this implies more of a focus on an audit of internal control, as opposed to a sufficient understanding to identify and assess risks. Paragraph 31 is an evaluation based on the auditor's understanding.
A136	See recommendation to include a formal definition of information system to underpin this section in our response to question 5(c). In addition to the lead-in language, we suggest this paragraph should also capture that the information system also comprises the IT environment relevant to financial reporting.
A154 & A157	See response to question 5(b). We do not believe that all controls relevant to financial reporting need to have their design and implementation evaluated.
A157, A160 & A166	See response to question 5(b) on describing controls in one component of the system of internal control as controls "in" the control activities component. It may be less confusing to simply state that control activities can exist within different components of the system of internal control.
A166	We believe the last sentence could be clarified. We suggest this should refer to "controls" (i.e., plural). We also believe that the intent is that each of those controls does not need to be determined as "relevant to the audit" (or, in our suggestions in Appendix 2, the auditor would not plan to rely and test each of them). The reference to "identified" may therefore cause confusion, as the controls would need to have already been identified to determine that they address the same objective.
A167	We do not believe that in <u>all</u> circumstances the auditor must evaluate the design and implementation of controls over journal entries. Having identified such controls, the auditor will determine, based on professional judgement, the need to test them as part of their audit strategy in response to identified and assessed risks of material misstatement, including whether such controls are directly related to a significant risk or are controls for which the auditor plans to place reliance through testing their operating effectiveness.
A179	As described in our main letter, we suggest incorporating this thinking into the guidance on those controls for which the auditor decides to test the operating effectiveness.
A180	The third sentence states that understanding implementation of general IT controls

	may assist in identifying IT applications relevant to the audit. This appears somewhat inconsistent with paragraph 41 that requires, for the IT applications relevant to the audit, that the auditor identify general IT controls relevant to the audit.
A181	We believe the following statement is in conflict with paragraph 40, as there is no "reputable" or "reliable" carve out in applying paragraph 40 based on the outcome of paragraph 39: *"When an entity uses an IT application that is reputable, widely-used and considered reliable, is unable to change its programming, and maintains hard-copy accounting records, the auditor may determine that there are no IT applications relevant to the audit."*
A184	We suggest separating the first sentence in the paragraph into its own paragraph. While we agree that consideration of the source code is helpful, management may still be able to configure reports or queries and this should be considered. With regard to the third sentence, we believe it could be read as implying that the auditor could simply test general IT controls and be able to rely on a report, rather than testing completeness and accuracy.
A185	It is unclear to us why the guidance is distinguishing between databases and data warehouses. In our view, there are more significant IT risks that could affect the business that could be further explored (e.g., cybersecurity, cloud computing and the impact of using third-party vendors).
A189-A192	We suggest the guidance could reinforce more clearly the importance of general IT controls in supporting other controls e.g., automated controls over which the auditor intends to rely.
A195	We believe in many cases there may be a single control that addresses multiple assertions and suggest this could be included to contrast the guidance that has been included.
A197	We believe the concept of precision of controls could be brought in to better explain indirect controls.
A201	Notwithstanding the reference to supporting risk assessment, we believe there is a risk that the following (bold text) could be misinterpreted as implying that you can take "credit" for evaluating design and implementation to reduce the level of substantive work that is required in circumstances when the auditor does not test operating effectiveness: *"Information gathered by performing risk assessment procedures,* ***including the audit evidence obtained in evaluating the design of controls relevant to the audit and determining whether they have been implemented****, is used as audit evidence to support the risk assessment."*
A208, A211-A214 & A232-A235	See response to question 6.

A213	This paragraph's premise is that a zero-balance account within the general ledger may contain risks of material misstatement if it contains entries netting off at the period end. Whilst we understand this, we do not feel the paragraph sufficiently explains the point. For example, it would be useful if the example given could be based more on a general business situation rather than a specific financial services example that is not readily understandable to those involved in non-financial services audits, and could describe the assertions that may be relevant in such an example.
A221	See response to question 6. We believe events and conditions are not susceptible to misstatement. Rather it is the financial reporting of those events and conditions i.e., the related classes of transactions, account balances and disclosures that may be misstated.
A224	We believe a reason should be provided for this statement. For example, by linking to other application guidance that describes the characteristics of smaller and less complex entities.
A240-A242	See response to question 7.
A244-247	See response to question 1.
Appendix 2	We note the following comments: *Subjectivity* We suggest a new example be considered, for example related to percentage of completion, rather than depreciation, as this may not be that subjective. *Susceptibility to misstatement due to management bias or fraud* In addition to our overall comments that we are concerned about retaining this inherent risk factor, we also believe the final bullet of the "transactions" list is unclear as to the implied risk by referring to transactions recorded based on "management's intent". *Other inherent risk factors* It is not clear to us how these three bullets describe inherent factors as opposed to other events or conditions that may indicate risks of material misstatement.

Table 2 – Other editorial comments

Paragraph	***Comment***
5	*"~~For the identified risks of material misstatement at the assertion level, a~~ A separate assessment of inherent risk and control risk is required by this ISA. The auditor assesses ~~the~~ inherent risk by assessing the likelihood and magnitude of material misstatement, and by taking into account inherent risk factors….. "*
16(a)	We suggest moving the definition of application controls into part (g) of the definitions to follow the definition of IT applications as part of the definition of the IT environment. We think this would better link these concepts.
16(e)	*"General information technology (IT) controls – Controls related to the IT environment that support the effective functioning of ~~application~~ controls (e.g. application controls, access controls, change management) or the integrity of information by helping to maintain the continued operation, as designed, of the entity's information system. General IT controls include controls over the entity's IT processes. Also see the definition of IT environment."*
16(k)	See response to question 6(e). *"Significant risk – An identified risk of material misstatement:* • *For which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk due to the degree to which one or a combination of the inherent risk factors affect the likelihood of a misstatement occurring ~~or~~ and the magnitude of potential misstatement should that misstatement occur* • *……"*
A15	*".......For example, through the use of technology the auditor may perform procedures on large volumes of data, and audit evidence may be obtained that provides information that is useful for the identification and assessment of risks of material misstatement, as well as providing sufficient appropriate audit evidence to support ~~the~~ a conclusion that the risk ~~possibility~~ of a material misstatement is at an acceptably low level ~~remote~~."*
A18	Within the final sentence, we believe the opening clause is not required and may unintentionally suggest that automated tools and techniques may only be used for risk assessment procedures. It is also duplicative with the remainder of the sentence: *"…… ~~In performing risk assessment procedures, t~~The auditor may use automated tools and techniques in performing the risk assessment procedures, including for analysis, recalculations, reperformance or reconciliations."*
A42 bullet 3	*".......In particular, the discussion assists engagement team members in identifying and further considering contradictory information based on each member's own understanding of the nature and circumstances of the entity."*
A45	*"……The engagement partner may discuss matters with key members of the*

	engagement team including, if considered appropriate, those with specific skills or knowledge, and those responsible for the audits of components, while delegating discussion with others, ~~while~~ taking into account ~~of~~ the extent of communication considered necessary throughout the engagement team. A communications plan, agreed by the engagement partner, may be useful."
A74 bullet 2	We are uncertain if "Revenue" is being used here in the context of a taxation authority. If so, for purpose of translation and avoiding possible confusion we suggest simply stating "taxation authorities".
A77	We recommend this paragraph should be located at the beginning of the section to follow paragraph A70. It sets relevant context for the rest of the section.
A81	The linkage of this paragraph to the underlying requirement relating to understanding the financial reporting framework is not obvious. We recommend leading with the reference to financial reporting frameworks, as follows: *"~~Disclosures in the financial statements of smaller and less complex entities may be simpler and less detailed (e.g., s~~Some financial reporting frameworks allow smaller entities to provide simpler and less detailed disclosures in the financial statements). However, this does not relieve the auditor of the responsibility to obtain an understanding of the entity and its environment, the applicable financial reporting framework as it applies to the entity, and its related system of internal control."*
A131	*"… If the auditor determines that the function's responsibilities are related to the entity's financial reporting, the auditor may ~~obtain further~~ expand the understanding obtained of the activities performed…"*
A141	*"Risk identification and assessment is an iterative process. The auditor's expectations formed in paragraph 23 about the classes of transactions, account balances and disclosures may assist the auditor in determining the ~~significant~~ classes of transactions, account balances and disclosures that are significant to the financial statements ~~in accordance with paragraph 46~~, which are those that need to be understood when obtaining an understanding of the information system in accordance with paragraph 35. For example, the auditor may have an expectation that certain significant classes of transactions related to revenue exist, but in obtaining the understanding about the flows of information in the information system, the auditor may identify additional classes of transactions related to revenue that may be significant."*
A146	*"The auditor may take an approach to obtaining the understanding of the IT environment that involves identifying the IT applications and supporting IT infrastructure concurrently with the auditor's understanding of how information relating to ~~significant~~ classes of transactions, account balances and disclosures flows into, through and out the entity's information system"*
A153	● *"……;* ● *Inquiries of relevant personnel about the procedures used to initiate, record, process and report transactions or about the entity's financial reporting process; ~~or~~*

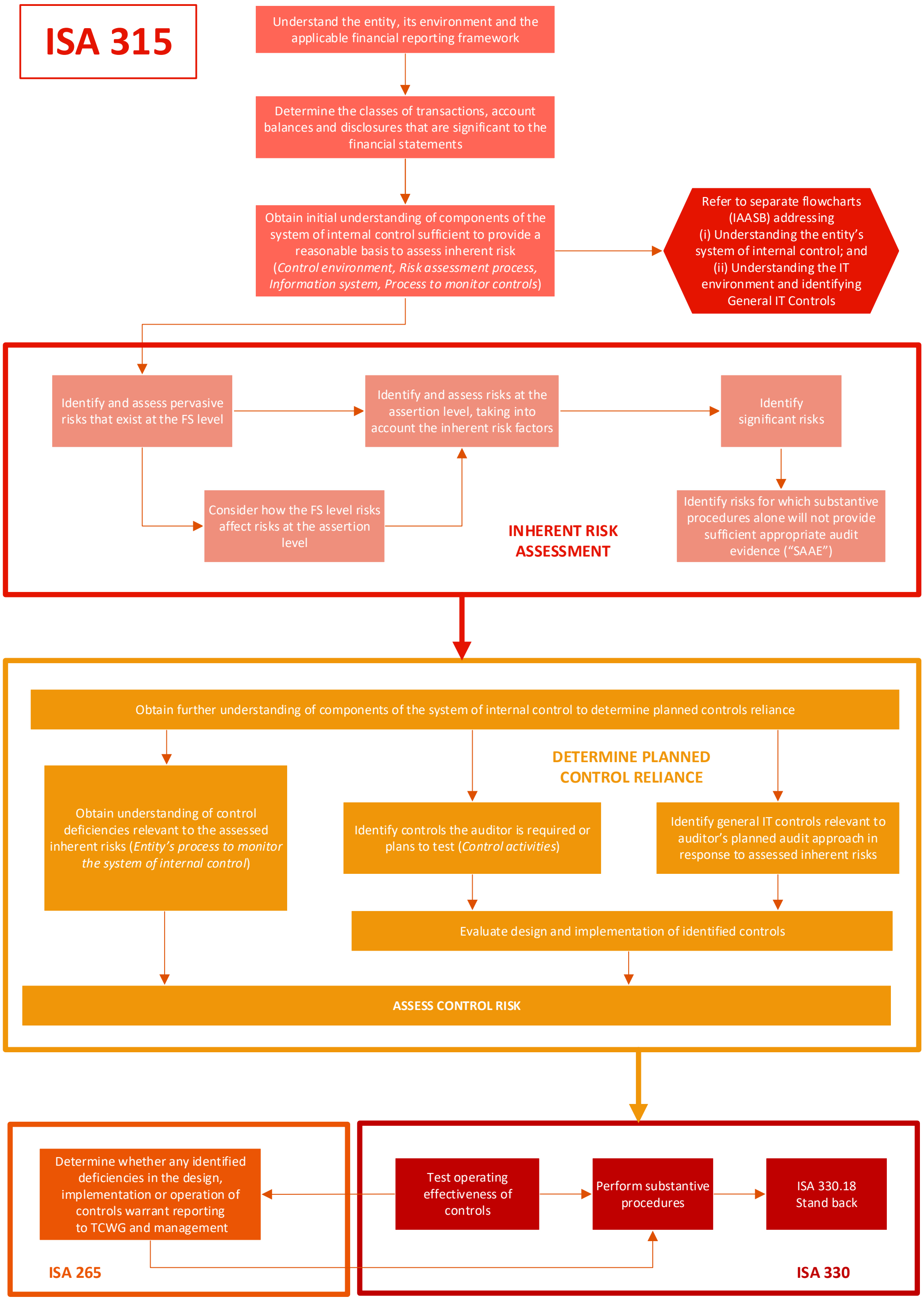
	• *Observation of the performance of the policies or procedures by entity's personnel~~.~~; or* • *Selecting transactions and tracing them through the applicable process in the information system......"*
A155	See response to question 3. *".....Analysis of complete or large sets of transactions may also result in the identification of variations from the normal, or expected, processing procedures for these transactions, which may result in the identification of ~~additional~~ risks of material misstatement related to non-standard procedures."*
A156	*"~~Regardless of the techniques used to evaluate the design of the information system and determine whether it has been implemented, t~~The auditor's understanding of the sources of data, and the IT applications involved in processing that data, may also assist the auditor in understanding the IT environment."*
A183	The controls are identified in accordance with paragraph 39, rather than 40. It is that knowledge that then helps identify the relevant IT applications relevant to the audit.
A193	We believe use of "likely" is too strong in the first sentence and suggest: *"Identifying the risks arising from the use of IT and the general IT controls relevant to the audit ~~is likely to~~ may require the involvement of team members with specialized skills in IT...."*
A196	*"....For example, ~~the~~ controls that an entity establishes~~d~~ to ensure that its personnel are properly counting and recording the annual physical inventory relate directly to the risks of material misstatement relevant to the existence and completeness assertions for the inventory account balance."*
A229	"....... • *Accounting estimates that have high estimation uncertainty or involve the use of complex models"*
A243	*"In performing tests of those controls, the auditor may obtain audit evidence that they were not operating effectively at relevant times ~~during the~~ throughout the period subject to audit."*

Table 3 - Conforming amendments

Standard & Paragraph	***Comment***
ISA 200.13 (n)(i) & A40	See ISA 315 paragraph 3 above.
ISA 240.27 & A7	See comments on "controls relevant to the audit".
ISA 240.44 (c) & A32	See comments on "controls relevant to the audit". In this instance we suggest: *"Controls ~~identified to be relevant to the audit because they~~ that address assessed risks of material misstatement due to fraud."*
ISA 240.A25 & Appendix 1 paragraph 2	See response to question 9.
ISA 330.7(a), A9, A42 & A60	See ISA 315 paragraph 4 comment.
ISA 330.10 (a)(iii)	A reference to paragraph A29b is missing.
ISA 330.10 (b)	Given the importance attached to obtaining an understanding of GITCs in ISA 315, we believe it is equally important to make more explicit that such controls may need to be tested. Otherwise, we believe there is a risk that the enhancements made in ISA 315 are not followed through appropriately in ISA 330. We suggest appending to this requirement the following: *"The auditor's determination shall take into account the general IT controls evaluated in accordance with ISA 315 (Revised) paragraph 42."*
ISA 330.14, d A35 & A36	See ISA 315 paragraph 21 comment.
ISA 330.A1	See response to question 9.
ISA 330.A29b	See comments on "controls relevant to the audit".
ISA 330.A42a	The term "would be most material" is not one used in other standards. Generally, we find the drafting of this paragraph to be unclear. We suggest the following: *"The auditor's consideration of the assertion(s) in which a possible misstatement could occur, and if it were to occur, whether that misstatement would be material, assists the auditor in designing the substantive procedures to be performed, and the nature, timing and extent of those procedures to be performed."*

ISA 540.1	See response to question 4 with respect to the use of "sufficient appropriate audit evidence".
ISA 540.13 (h)(i), 18 & A34	See ISA 315 paragraph 4 comment.
ISA 540.A10	Delete the word "that" in the second line preceding "whether".
ISA 540.A39	See ISA 315 paragraph A201 comment. We believe that there is a risk of misinterpretation of the reference to design and implementation providing audit evidence without a corresponding reference to testing operating effectiveness.
ISA 540.A50 & A51	See comments on "controls relevant to the audit".
ISA 540.A86 second bullet	We believe inherent risk is the more appropriate term here, rather than risk of material misstatement. A control is designed to address inherent risk and logically cannot be designed factoring in control risk (which seems to be the implication by referring to risk of material misstatement).

Appendix 4 – Flowchart[3]



[3] The flowchart represents a visual illustration of our initial outline of a suggested restructured set of core requirements, together with the linkages to ISAs 265 and 330. It does not seek to show every requirement in the ISA. As noted in Appendix 2, while these suggestions will benefit from further consideration and input, we felt it useful to illustrate our thinking to assist the Board's further considerations in developing final proposals.

Appendix 5 – Summary of approach to field-testing

We asked seven engagement teams to field-test the new requirements, some of whom were provided the ED flowcharts to the ED (the purpose of this being to obtain insight into whether the requirements were understandable without the supplementary flowcharts). Each team was asked to:

- read the ED requirements, and to the extent necessary the associated application material
- conduct a realistic but mock team planning meeting to discuss the requirements and questions below, using the prior year audit working papers of the selected engagement to provide a realistic basis for the planning/risk assessment discussion.

The importance of the engagement leader having the same level of input into the field-testing process as would be expected during the planning and risk assessment phase of a live audit was stressed.

The sample of teams included a broad geographical cross-section of the network's client base, including small and large sized audits, private and listed (including FPI) audits, some of which were either group or component auditors, and covered a range of industries including financial services, manufacturing and the service sector.

Questions

Understanding the entity, the applicable financial reporting framework and the system of internal control

1. With respect to the requirements around understanding the entity, its environment, its control environment and the applicable financial reporting framework (paragraphs 17-44):
    a. do you think your level of understanding obtained when planning the prior year audit would be enough (i.e., remain the same), or do you think you would need to understand more? If more, in what specific areas?
    b. was it clear how much you had to do in terms of understanding controls, taking into consideration what you expected your planned audit strategy to be? Please explain.
    c. did you find the revised requirements overall to be clear and understandable? If there were any areas you found to be unclear, please describe.

Risk assessment

2. Perform and **document** the risk assessment procedures described in paragraphs 45-47.
    a. Was it clear what you had to do? If there were any areas you found to be unclear, please describe.
3. For one significant financial statement line item identified as part of step 2, perform and document the separate assessment of inherent and control risk required by paragraphs 48-50.
    a. Was it clear what you had to do? If there were any areas you found to be unclear, please describe.
4. Thinking about your documented risk assessment for the financial statement line item chosen in item 3 above, and comparing it to what you documented in your prior year audit file under the old standard:
    a. Did you identify more or fewer risks? Please explain why.
    b. Based on the revised definition, did you identify more or fewer significant risks? Please explain why.

c. Were your risks more or less specific than previously identified i.e., did you identify more specific reasons (drivers) and/or assertions for your identified risks? Please explain why.

5. What was the outcome of applying paragraph 52? Please **document** the considerations you worked through and, if you identified any additional risks, please explain why.

General

6. General questions:

    a. The introductory section of the standard includes some introductory paragraphs describing new concepts (paragraphs 2-13). Having read this section, do you find it useful?

    b. Do you have any other observations not addressed through the previous questions?

    c. [Additionally, for those engagement teams that received the supplementary flowcharts] Did you find the flowcharts helpful in trying to apply the new requirements? Please explain your answer.