Ernst & Young Global Limited
6 More London Place
London
SE1 2DA

Tel: + 44 20 7980 0000
Fax: + 44 20 7980 0275
ey.com

Mr. Dan Montgomery
Interim IAASB Technical Director
International Auditing and Assurance Standards Board
529 Fifth Avenue, 6th Floor
New York NY 10017

2 November 2018

Exposure Draft: *Proposed ISA 315 (Revised), Identifying and Assessing the Risks of Material Misstatement*

Dear Mr. Montgomery

Ernst & Young Global Limited, the central coordinating entity of the Ernst & Young organization, welcomes the opportunity to offer its views on the Exposure Draft, *Proposed ISA 315 (Revised), Identifying and Assessing the Risks of Material Misstatement* (ED-ISA 315), issued by the International Auditing and Assurance Standards Board (IAASB).

We support the revision to this important International Standard on Auditing, because we believe the revised standard will enable improvement to audit quality by clarifying the auditor's process for identifying and assessing the risks of material misstatement, and by enhancing consistency in the application of the requirements of the standard. We believe that the proposals support the appropriate exercise of professional skepticism, and that, in particular, the references to consideration of management bias are helpful.

We particularly support the introduction of guidance on the use of automated tools and techniques in the audit, including data analytics, as this represents a recognition by the IAASB of the importance of using digital techniques within the audit. We are supportive of the proposal to require additional focus on the entity's business model and the applicable financial reporting framework.

We do have some overall comments in respect of ED-ISA 315, which are set out below, as are our detailed responses to the questions on which the IAASB is seeking feedback, which include further clarifying detail in respect of our overall comments, when applicable. We have included a number of drafting and editorial suggestions in the Appendix.

Overall comments

Understandability

The proposed standard, although long, is easy to read and is well-structured with a logical flow, and we note that many additional helpful examples have been added to ED-ISA 315.

The introduction of flowcharts to illustrate the concepts within ED-ISA 315 is very helpful in demonstrating the iterative nature of the requirements. We would support including these within the final standard as an enabler to understanding.

Scalability

We believe that the ISA addresses scalability for a wide range of sizes, complexities and circumstances, given the specific guidance for smaller and less complex entities.

However, as noted above, the ISA is long – 37 requirement paragraphs, 247 application material paragraphs and 4 appendices. Therefore, even with the application material to assist the auditors of smaller and less complex entities, we believe that it will be time-consuming to apply ED-ISA 315 for audits of smaller and less complex entities. One way to help the auditors of smaller and less complex entities manage this issue may be to create a separate section or appendix specifically to address the guidance for smaller and less complex entities, rather than discussing it throughout ED-ISA 315.

Risk assessment and identification

We believe that the revised standard will enable sound risk identification and assessment through the introduction of a structured framework for identifying and assessing inherent risk and control risk to guide auditors through the thought process. The discussion on the spectrum of inherent risk is particularly useful to assist in the assessment of inherent risk.

Controls

We support the clarifications to 'controls relevant to the audit' as well as the introduction of the concept of direct and indirect controls, which we find very useful in clarifying the nature of controls expected to be relevant to the audit. We also support the changes to the guidance related to the components of the entity's system of internal control, especially the change in terminology for 'the entity's process to monitor the system of internal control', as we believe this is a better description of what this component entails.

We believe that pointing out that controls in smaller and less complex entities may be less formal and may be not documented by the entity is useful guidance for the auditors of these entities because this reflects the nature of internal control in many small entities. The auditor's understanding of the system of internal control for these small entities often involves understanding procedures, formal or informal, that management uses in their day-to-day involvement in the financial aspects of the business and how management influences or participates in activities and transactions.

Significant risk

ED-ISA 315 changes the definition of a significant risk. We support the change in definition, except for the inclusion of 'or' in the phrase 'inherent risk factors affect the likelihood of a misstatement occurring ***or*** the magnitude of potential misstatement should that misstatement occur'.

We believe that it is helpful to link the definition of significant risk to the spectrum of inherent risk and to an assessment of magnitude of potential misstatement and likelihood of occurrence. However, ED-ISA 315 suggests that a risk is significant 'due to the degree to which one or a combination of the inherent risk factors affect the likelihood of a misstatement occurring ***or*** the magnitude of potential misstatement should that misstatement occur'. We do not agree with this part of the definition, and suggest that 'or' (as italicized) be replaced with 'and'.

We believe that the use of 'or' in the definition will expand the population of significant risks on every audit. In turn, this could have the undesired effect of reducing the auditor's focus on those risks that have both a higher likelihood of occurring ***and*** a higher magnitude of potential misstatement.

We appreciate that certain risks may have a low likelihood of occurring but, should they occur, the magnitude of potential misstatement would result in a significant risk of material misstatement. However, for several risks that may be viewed as falling within this category, it is only after they have occurred that they have an effect on the entity's financial statements and become significant risks in the context of the audit. Examples of such risks may include natural disasters (e.g., the 'volcanic ash cloud' that grounded European flights for several days), political uncertainty (e.g., the potential effect of Brexit on European (including the UK) businesses) or environmental matters (e.g., the effects of asbestos in structures worldwide).

In this regard, we find the wording of paragraph A10 helpful: 'The significance of a risk of material misstatement at the assertion level is considered in the context of the implications of the assessment of its inherent risk for the performance of the audit, including the nature, timing and extent of the auditor's further audit procedures and the persuasiveness of the audit evidence that will be required to reduce audit risk to an acceptable level. Significance can be considered in the context of how, and the degree to which, the susceptibility to misstatement is subject to, or affected by, the inherent risk factors, which affect the likelihood that a misstatement will occur, ***as well as*** the potential magnitude of the misstatement were that misstatement to occur.'

Therefore, while we agree that a significant risk is one for which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk, we believe that categorization of a significant risk should be reserved for those risks that are at the upper end of the spectrum due to the degree to which one or a combination of the inherent risk factors affect the likelihood of occurrence ***and*** the magnitude of potential misstatement should that misstatement occur.

The information system and communication (paragraph 36)

The requirement in paragraph 36 requires the auditor to evaluate the design of the information system controls relevant to financial reporting. We are unclear what this requirement intends, particularly as we are unsure what the term 'information system controls' means in the context of this requirement.

Paragraph 35 requires the auditor to obtain an understanding of the information system relevant to the audit, and paragraph 36 appears to require an evaluation of that design and whether the design has been implemented (i.e., for the auditor to confirm their understanding of the information system as it has been implemented).

However, paragraph 36 introduces the concept of 'information system controls', which we do not understand, given the requirement set out in paragraph 38 for the auditor to obtain an understanding of the controls activities component by identifying controls relevant to the audit.

If the intent of paragraph 36 is that the auditor is expected to confirm their understanding of the flows of information through the entity's information system and the reporting process used to prepare the financial statements, then we suggest that paragraph 36 be reworded accordingly and that references to 'information system controls' be removed.

IT

We strongly support the addition of further guidance on IT, which recognizes that most entities use IT to some extent in the preparation of the financial statements, and that it is therefore becoming less likely for an auditor to be able to audit 'around the computer' or 'ignore the black box'. However, we do have a concern about the drafting of paragraphs 40 and 41 (see our response to Question 2

below), which may have the unintended effect of requiring the auditor to identify general IT controls (GITCs) on every audit, regardless of relevance to the audit.

We also have a small number of comments on the detailed guidance, which are set out in our response to question 5(c) below.

Attracting, developing and retaining competent individuals

Paragraph 27(d) requires the auditor to obtain an understanding of how the entity demonstrates a commitment to 'attract, develop and retain competent individuals in alignment with its objectives'. We are concerned that this requirement is very broadly drafted and could require the auditor to consider the design and implementation of Human Resources (HR) policies related to the entity's personnel in all parts of the business and at all levels of seniority (e.g., health and safety, marketing, HR, production). We suggest that this requirement be redrafted to restrict the requirement to competent individuals responsible for financial reporting (including senior IT personnel) and for the governance and oversight related to financial reporting.

Internal audit

The application material in paragraph A26 states 'If, based on responses to the auditor's inquiries, it appears that there are findings that may be relevant to the entity's financial reporting and the audit, the auditor may consider it appropriate to read related reports of the internal audit function.'

We believe that, if it appears there are findings relevant to the audit, the auditor is 'on notice' and cannot ignore those findings, and should read the related reports to obtain further details. Therefore, we recommend that the IAASB elevate this application material to a requirement.

'Components'

ED-ISA 315, as does extant ISA 315, uses the term 'components of the system of internal control'. Extant ISA 315 uses the term sparingly, whereas ED-ISA 315 uses the term much more often. When used as a complete term, there is no scope for confusion with the term 'components' in the context of a group audit. However, when abbreviated to just 'component' in a second or third mention within a paragraph in ED-ISA 315, the scope for confusion increases. This may result in translation issues, particularly of longer, more complex sentences. The last usage of 'component' in the last sentence of paragraph A97 provides an example of where such confusion might arise: in this case, both meanings of 'component' (i.e., internal control component or group component) could be relevant interpretations. We therefore suggest that the IAASB clarify which meaning of 'component' is intended in paragraphs containing multiple references to 'component'.

Effective date

We believe that an effective date for periods beginning at least 18 months after approval of the final revised standard would provide a sufficient period to support effective implementation.

Responses to the specific questions on which the IAASB is seeking feedback

Q1. ***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)?

Yes, we believe that the proposed changes help to make the risk identification and assessment process more understandable.

Although ISAs have generally not contained flowcharts in the past, we support the inclusion of such enablers within the standard. The inclusion of the flowcharts may also help to simplify or eliminate wording from the application material, for example, the paragraphs that mention the iterative nature of the audit and contain multiple cross references to requirements (i.e., paragraphs A12, A141, A202 and A216).

However, if the IAASB decides against this, we support publishing the flowcharts separately as non-authoritative guidance.

In terms of the flowcharts, we have a small number of specific observations:

- A color key would enhance the usefulness of the flowcharts, presuming the colors are intended to have a meaning.
- The Auditor's Understanding of the IT Environment and the Identification of General IT Controls Relevant to the Audit flowchart – we did not understand the difference in activities between the leftmost column, with only the one shape in it, and the second column, that seems to show the steps to do the activity in the leftmost column.

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?

Yes.

c) Are the new introductory paragraphs helpful?

Yes.

Q2. ***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?***

Yes, the requirements and application material are generally sufficiently scalable. In addition, we support the premise that only when an auditor can execute a 'fully' substantive audit (with extensive testing and recomputation of information) should the auditor be permitted to ignore the GITCs that maintain the integrity of the entity's financial data within its IT applications.

However, we are concerned that the requirements of paragraphs 40 and 41, taken together, will cause a large population of 'fully' substantive smaller and less complex audits to be required to identify GITCs, when, in reality, the IT is sufficiently simple, and the risks from IT are sufficiently low that the auditor would be justified in determining that the IT applications and other aspects of the IT environment are not relevant to the audit. In these circumstances, when the auditor concludes that the IT is not relevant to the audit, it would be appropriate for the auditor to take a 'fully' substantive approach and test the outputs of the IT system substantively.

Although the audit is iterative in nature, the necessary linear drafting of the standard requires the auditor to identify the IT applications and other aspects of the entity's IT environment that are relevant to the audit (paragraph 40) before considering the risks arising from the use of IT (paragraph 41) in relation to the information system relevant to financial reporting. We therefore recommend that the IAASB consider moving paragraph 41 to before paragraph 40, and linked more closely to paragraph 35(d), in which the auditor is required to obtain an understanding of the entity's IT environment.

The example in paragraph A181, which does allow for smaller and less complex entities to have no IT applications relevant to the audit, is restrictive – implying the need for 'hard-copy accounting records' and an inability to change the programming of the IT application in use. We believe that this example is unnecessarily restrictive, although we do recognize that 'off-the-shelf' applications allow for setting certain user-driven parameters, which may, if changed, affect the recording and reporting of transactions. We therefore suggest that it would be helpful to include further discussion on user-driven parameters, and the effect that inappropriate or changes to parameters (such as a change to a VAT rate) could have.

See also our suggestion in our Overall comments regarding the creation of a separate section or appendix specifically to address the guidance for smaller and less complex entities, rather than discussing it throughout ED-ISA 315.

Q3. ***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?***

Yes, we agree with the approach taken, as noted in the introductory paragraphs of our letter. We believe that automated tools and techniques, including data analytics, can play a key part in the audit, and that their role in the audit will increase over time.

Q4. ***Do the proposals sufficiently support the appropriate exercise of professional skepticism throughout the risk identification and assessment process?***

Yes, we believe that the proposals generally support the appropriate exercise of professional skepticism, and that, in particular, the references to consideration of management bias are helpful.

However, we draw attention to the wording of paragraph A44 (i.e., 'the engagement team may also have an opportunity to exercise professional skepticism while performing risk assessment procedures'). The implication is that the auditor is 'looking for opportunities' to exercise professional skepticism, and we suggest re-wording this to read '…the engagement team exercises professional skepticism …', given that the engagement team is expected to exercise professional skepticism throughout the audit, rather than looking for discrete opportunities to do so.

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 skepticism?

No, we do not support the proposed change for the auditor to obtain 'sufficient appropriate audit evidence' through the performance of risk assessment procedures. We believe that this implies that the auditor needs to evaluate whether 'sufficient appropriate audit evidence' has been obtained in respect of the risk assessment procedures, whereas sufficient appropriate audit evidence needs to be evaluated on all audit evidence obtained, to determine the auditor's opinion on the financial statements.

Q5. ***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 or 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?

Yes, with two exceptions.

Control environment

We are concerned that the requirement in paragraph 27(d) is very broadly drafted and could require the auditor to consider the design and implementation of Human Resources (HR) policies related to the entity's personnel in all parts of the business and at all levels of seniority. We suggest that this requirement be redrafted to restrict the requirement to competent individuals responsible for financial reporting (including senior IT personnel) and for the governance and oversight related to financial reporting.

Information system controls

Paragraph 36 introduces the concept of 'information system controls', which we do not understand, given the requirement set out in paragraph 38 for the auditor to obtain an understanding of the controls activities component by identifying controls relevant to the audit.

If the intent of paragraph 36 is that the auditor is expected to confirm their understanding of the flows of information through the entity's information system and the reporting process used to prepare the financial statements, then we suggest that paragraph 36 be reworded accordingly and that references to 'information system controls' be removed.

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?

Yes, except that we find paragraph A233 confusing. ED-ISA 315 (paragraph 50) requires that control risk be assessed at 'maximum' or 'less than maximum', which implies a binary choice, and this is supported by the example in paragraph A233, as well as other parts of ED-ISA 315 (e.g., Paragraph 6). However, the application material in the remainder of paragraph A233 implies an assessment using qualitative categories that include 'moderate' and 'minimum'. It is not clear how these categories would be applied, nor what effect that would have on the audit procedures. Does 'moderate' imply an expectation of 'partial' operating effectiveness, requiring a suite of 'moderate' controls to address a risk of material misstatement? Therefore, we recommend deleting the first two sentences of paragraph A233, and combining the example in paragraph A233 into paragraph A232.

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?

Yes. However, we do have a number of comments on the detailed guidance, as follows:

Underlying controls (paragraphs A124, A127 and A128)

The use of the term 'underlying controls' appears to be used differently within different paragraphs in the application material.

In paragraph A124, there is reference to 'underlying controls', but, as used in ED-ISA 315, application controls are direct controls. In paragraph A127, we are uncertain about what the phrase 'underlying controls that involve the use of IT' means. We suggest that the term 'direct controls involving IT' is clearer than 'underlying controls'.

Paragraph A128 uses the same language of 'monitor underlying automated controls' as used in paragraph A127. In this context, does this mean monitoring the IT environment in aspects that relate to financial reporting, such as monitoring security settings or monitoring for

unusual activities of IT persons with privileged access at the operating system or database levels?

Other comments

- Further guidance about what is expected of the auditor when the entity relies on outsourcing for maintenance of the IT systems would be helpful.

- A definition of automated controls would be helpful to reduce potential confusion with application controls (paragraph 16).

- We disagree that operating systems are 'typically relevant' to the audit (paragraph A188 – sentence beginning 'similarly, because an IT application's ability to operate is dependent on the operating system'). Access to operating systems is typically relevant because the ability to move program changes to production is often done at the operating system level. We therefore suggest that the wording be changed to read '…certain aspects of the operating system, such as controls over access, are typically relevant …'

- We also disagree that the basis for the network being relevant to an audit (paragraph A188) is because an IT application interacts with vendors or external parties through the internet. The network is typically relevant because it is one of the 'doors' to gaining access to the IT applications and related data (i.e., it is in the access path, even within an entity that does not use the internet).

Q6. ***Will the proposed enhanced framework for the identification and assessment of the risks of material misstatement result in a more robust risk assessment? 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'?

Yes.

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?

Yes, we support the concepts and definitions of inherent risk factors, as set out in paragraph A5. We believe the use of inherent risk factors creates a framework for identifying inherent and significant risks. However, we do have concerns about how the auditor's thought-process is expected to be documented, particularly for inherent risks assessed at the lower end of the spectrum of inherent risk. We are also concerned about how formally this framework is expected to be applied and documented, i.e., is the expectation that each factor needs to be documented for each identified inherent risk? We believe that it would be helpful to clarify that formal documentation is not required of how each inherent risk factor has been considered.

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?*

Yes, we believe that the 'spectrum of inherent risk' is a helpful concept in recognizing that 'inherent risk is higher for some assertions and related classes of transactions, account balances and disclosures than for others', and that the spectrum will assist auditors in making their assessments of inherent risk.

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?*

Yes, we believe these concepts reflect the approach to risk assessment that is taken in practice. In particular, we agree with the threshold for the identification of risks of material misstatement to be those risks that are 'reasonably possible'. This threshold provides a practical approach to identifying and focusing on those risks that matter to the audit.

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?*

No, not entirely. Although we support the concepts in the revised definition, we do have concerns about a particular part of the definition because we believe it will capture many more risks than those at the highest end of the spectrum of inherent risk. As noted in our overall comments, we believe that categorization of a significant risk should be reserved for those risks that are at the upper end of the spectrum due to the degree to which one or a combination of the inherent risk factors affect the likelihood of occurrence ***and*** the magnitude of potential misstatement should that misstatement occur.

We also have a concern about the wording of the penultimate sentence in paragraph A167, which states 'further, the auditor may not have identified any significant risks …for which it is necessary to evaluate the design of controls'. Requirements in certain other ISAs (for example, paragraphs 26 and 27 of ISA 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*) presume the existence of significant risks in specific situations. Although we accept that such presumed significant risks may not be present on some audits, we are concerned that the example implies that this may be a common occurrence. We suggest that this sentence be qualified as follows: 'Further, the auditor may not have identified any significant risks, including those presumed by the ISAs as existing on every audit…'

Q7. ***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?***

Yes, we believe that this guidance provides useful clarification about the nature of risks at the financial statement level and how such risks are assessed.

Q8. ***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 deletion of paragraph 18 of ISA 330. We believe that the performance of a comprehensive and appropriate risk assessment, including the newly introduced 'stand-back' requirement set out in paragraph 52 of ED-ISA 315 is sufficient to drive an appropriate audit response, and that the requirement in ISA 330 paragraph 18 is redundant.

Q9. ***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?

Yes, although we have some minor editorial comments, as follows:

- ISA 330, paragraph A42a: Delete 'most' as follows: '…, the effect of that misstatement would be ~~most~~ material …'
- ISA 540, paragraph 17: Delete 'and' as follows: '… ~~and~~ evaluate whether such controls …'
- ISA 540, paragraph A10: Delete 'that' as follows: '~~that~~ whether the auditor intends …'
- ISA 540, paragraph A22: Should 'smaller entities' be amended to read 'smaller and less complex entities'?
- ISA 540, paragraph A39: The use of the term 'higher assessed risks' is not used in ED-ISA 315 nor in the other conforming amendments. We suggest that the IAASB revisit the use of this term in paragraph A39.
- ISA 540, paragraph A86, fourth bullet: This bullet is not clear: Should 'identified deficiencies' read 'identify deficiencies' or 'monitor identified deficiencies'?

Q10. *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?*

No, given that we support the deletion of paragraph 18 of ISA 330 – please see our response to question 8.

Q11. *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 ED-315.

No comment.

a) 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 believe that an effective date for periods beginning at least 18 months after approval of the final revised standard would provide a sufficient period to support effective implementation.

****

We would be pleased to discuss our comments with members of the IAASB or its staff. If you wish to do so, please contact Kurt Hohl, Global Deputy Vice Chair, Professional Practice (kurt.hohl@ey.com).

Yours sincerely,

Ernst & Young Global Limited

Appendix: Editorial and typographical suggestions

Paragraph Reference	Suggested change
31(b)	The requirement in paragraph 31(b) starts with 'If not', because it is related to the requirement in paragraph 31(a) rather than to the lead-in to the bullet. As such, paragraph 31(b) effectively reads: 'the auditor shall, if not, determine …', which does not make sense. We suggest that, in this case, bullets are unhelpful, and that the requirement be amended to read: '…the auditor shall evaluate whether ….considering the nature and size of the entity. If not, the auditor shall determine whether the lack …'
39(c) and A167	Journal entries are at the end of a process of information accumulation and processing. Are controls over the entire process of developing the information that is recorded in the journal entry part of this requirement? If so, we suggest this be clarified. If not, the starting point to identify controls over journal entries should be specified. In addition, it would be helpful to add guidance that recognizes that the risk of management override does not occur only at the journal entry level (i.e., at the general ledger level), but can occur in the sub-ledgers as well. For example, when customer and supplier supply chains are integrated, the supplier's system may accept sales invoices from the customer based on amounts of product used by the customer, cancelling their own sales invoices based on deliveries to the customer. Such adjustments may provide opportunities for management override of controls at the sub-ledger level.
39(e) (ii)	Add 'of material misstatement' as shown: 'Design further audit procedures responsive to assessed risks of material misstatement.'
40(a)	We suggest the phrase 'automated controls' in paragraph 40(a) should read 'automated or partially automated controls'.
40(c), A183	It may be helpful to mention information in an end user computing (EUC) tool that started as system-generated output or that used information from a system-generated report that is manually keyed into the EUC tool, rather than just system-generated reports or system-generated output. In addition, we suggest modifying the references to 'system-generated reports' in paragraph A183 to reference 'System-generated output, or information based on system-generated output', and including an example such as a reserve computation that starts as output from an IT application or a tax computation, i.e., which is done completely in an end-user computing tool but that uses system-generated information.
A7	We suggest the addition of a third sentence: 'A data warehouse becomes an IT application when programs to alter the data received by, or included in, the data warehouse, or programs to produce reports from the data warehouse, are included in, and run from, the data warehouse (e.g., stored procedures).'

Paragraph Reference	Suggested change
A8	We suggest paragraph A8 be separated into three paragraphs, one for network, one for operating systems, and one for databases.
A48	Paragraph A48 is referenced to paragraph 23, but seems more appropriately referenced to paragraph 35 particularly because of the example in the second sentence. If the second sentence was deleted, or moved to relate to paragraph 35, then what is left of paragraph A48 would be appropriate to be associated with paragraph 23.
A50	Amend '… the entity mandate and strategic direction…' to read '… the entity's mandate and strategic direction…'
A51	We are confused by the first sentence, particularly the part after the comma – responsibilities are not 'prerequisites'. We therefore suggest deleting the wording ', but are generally prerequisites for an effective system of internal control.'
A52	Missing word: '… which may affect the reasonableness of significant assumptions and the expectations of management or those charged with governance …'
A56, second sentence	This sentence is difficult to understand – perhaps it could be reworded as 'Not all aspects of the business model are relevant for the auditor's understanding.~~,~~ ~~but~~ However, those aspects that give rise to business risks~~, which are relevant to the identification and assessment of risks of material misstatement,~~ are likely to be more relevant for the auditor's understanding, because they are relevant to the identification and assessment of risks of material misstatement.'
A82	Should 'further impacts the ability to assess the accountability' read 'further impacts the auditor's ability to assess the accountability'?
A86, first sentence	'When complexity is an inherent risk factor…' would be clearer if reworded to specify the complexity of what.
A93	The word 'respectively' is not needed at the end of the first sentence of paragraph A93.
A94	We suggest amending 'controls over compliance with laws and regulations may be relevant' to one of 'controls to ensure compliance …' or 'controls that monitor compliance …'
A98, bullet 1	We do not understand what is meant by the phrase 'control parameters' in this bullet.
A103	Second sentence: We disagree with the statement that GITCs 'may' include indirect controls. The definition of a direct control is one that prevents, or detects and corrects, risks of material misstatement, and therefore GITCs are not direct controls, a view that is reinforced by the text of paragraph A197.

Paragraph Reference	Suggested change
	We suggest deleting the example in A103.
A116	Word missing, as shown: 'Irrespective of whether the risk assessment …'
A127	It would be helpful to clarify the first and third bullets with an example in each bullet, as we were unclear about the meaning of these bullets. In the second bullet, we were unclear about the meaning of 'permissions applied'. Does this mean 'permissions granted that affect segregation of duties'? Automated actions of the computer do not involve people.
A136	The language in the first bullet of paragraph 35(a)(i) ('transactions are initiated, and how information about them is recorded, processed, corrected as necessary, and incorporated into the general ledger and reported in the financial statements') is helpful and clear. We recommend that this language should be carried through to bullet 1 of paragraph A136. In addition, we suggest changes to the following terms: ▶ In the second bullet of paragraph A136, 'automated suspense files' should read 'suspense files from automated processing', as the two phrases do not have the same meaning ▶ In the third bullet or paragraph A136, we suggest 'system overrides' be changed to 'clear online system halts'
A139	Word missing, as shown: Understanding the entity's information system relevant to financial reporting may therefore require less effort in an audit of a smaller and less complex entity …
A142	The last bullet is redundant, and can be deleted.
A145	In paragraph A145, the first risk encompasses all the rest. Therefore, the first risk could be deleted and the other risks left in place, or the first risk can be left and all the other bullets could be deleted. Alternatively, the 2nd through 8th bullets can be presented as examples of the meaning of the first bullet. This change would reinforce the need to understand IT processes as a step to determining the necessary GITCs.
A148	Bullet 5 of paragraph A148, we suggest 'the system' be replaced with 'the information system' for clarity. Bullet 6, sub-bullet 3 refers to cyber security risks. The phrase should be 'cyber risks'. Cyber security is used to address cyber risks. Paragraph A148 ignores the processes used by those who manage and change IT systems, including programs, configurations, security settings and access rights. We therefore suggest that an additional bullet be added to include changes to access rights. The current last bullet and the new bullet we have proposed are better described in the context of the processes to perform the IT department actions.

Paragraph Reference	Suggested change
A149	Bullet 2 should include the addition of add-ons to the base software. Many vendors provide 'hooks' for entities to use. Bullet 3, despite the initial broader language, focuses only on configurations. Direct data changes should also be included as a risk.
A151	There is a stray closing parenthesis at the end of the paragraph.
A158	Amend the sentence to reflect that the entity would be providing 'information about' individual roles and responsibilities rather than 'an understanding of' such roles and responsibilities.
A166	Last sentence, last line – 'control related to such objective' should be 'controls related to such objective'
A169 / A222 / A229	We do not believe it is necessary to repeat that significant risks are those that are close to the upper end of the spectrum of inherent risk, as this is addressed in the definition of significant risk in paragraph 16. This duplication could therefore be deleted.
A181 / A149	The second and third sentences on paragraph A181 do not make sense as drafted. We do not believe that an entity would pay for and install an IT application if it was not planning to rely on the information that comes out of it. Also, it is not possible to reconcile all pieces of important information (e.g. dates). In addition, we suggest deleting the word 'reputable' from the phrase 'reputable, widely-used and considered reliable' in paragraph A181, which aligns more closely with paragraph A149, which suggests the auditor may consider the extent to which software is 'well established and has a reputation for reliability'.
A182	We suggest deleting the first 'and', and adding commas to make it easier to follow, as shown: 'In larger entities, the entity may be relying on IT to a greater extent , ~~and~~ the IT environment may involve multiple IT applications, and the IT processes to manage the IT environment may be complex'.
A185	Second sentence: The key point is not the separate report-writing software; it is the program that defines the report itself. For example, in the same way that the auditor is concerned with controls over changing the code rather than the language SAP is written in or the tools used to write the program code, the auditor should not focus on the tools used to write reports, but rather the report program itself. The last two sentences of paragraph A185 do not seem to have anything to do with the first two sentences of paragraph A185. Although the information is accurate, we are unsure of the purpose it serves here, and therefore could be deleted.

Paragraph Reference	Suggested change
A190, first sentence	General IT controls do not solely address the risks arising from the use of IT. User actions are also important. We therefore suggest the first sentence be qualified by adding the word 'help' in front of the word 'address'.
A192, Appendix 4, paragraph 1(a)	In paragraph A192, quantity of controls is an irrelevant metric because the wording and level of a control is not prescribed. In addition, we disagree that the quantity of controls necessarily correlates with the nature and extent of application functionality.
A198, second bullet	We suggest rewording this bullet to read A198 – second bullet 'Observing the ~~application~~ performance of controls'. The use of 'application' in this bullet could be confusing, given the use of IT 'applications' within ED-ISA 315.
A239	We believe that this paragraph could be deleted.
A244 / A246	We suggest that the order of the sentences in paragraph A244 be changed, as shown. In addition, we suggest moving the first sentence of paragraph A246 to A 244. A244. (1) The manner in which the requirements of paragraph 54 are documented is for the auditor to determine using professional judgment. (2) The form and extent of the auditor's documentation is influenced by the nature, size and complexity of the entity and its system of internal control, availability of information from the entity and the audit methodology and technology used in the course of the audit. (Moved from A246) For the audits of smaller and less complex entities, the form and extent of documentation may be simple in form and relatively brief. (3) For example, in audits of smaller and less complex entities the documentation may be incorporated in the auditor's documentation of the overall strategy and audit plan. (4) Similarly, for example, the results of the risk assessment may be documented separately, or may be documented as part of the auditor's documentation of further procedures. … A246 (First sentence moved to A244) It is not necessary to document the entirety of the auditor's understanding of the entity and matters related to it. Key elements of understanding documented by the auditor may include those on which the auditor based the assessment of the risks of material misstatement.
Appendix 3, paragraph 5	We suggest deleting the last example of the paragraph, as it demonstrates an unnecessarily cynical view of the personnel.
Appendix 3, paragraph 12	Comma is missing from after the word 'pertaining to the entity's system of internal control'
Appendix 4, paragraph 1(b)	We suggest '… risks arising from the use of IT related to …' be replaced with '… the risk of …'

Paragraph Reference	Suggested change
Appendix 4, paragraph 1(c)	We suggest 'IT related to' be deleted. In addition, the tone is of an intent to commit fraud rather than the risk of human error in performing actions (enabled by the administrator IDs) that can have a pervasive effect on the IT environment.
Appendix 4, paragraph 1(d)	Data transmissions point to the need for interface controls – we suggest adding this as a consideration.
Appendix 4, paragraph 2(a)	Authentication – This sentence is inaccurate because GITCs are not able to verify who uses an ID. What is typically tested is that safeguards exist (such as passwords) that help ensure the user to which an ID is assigned is the person who uses it. Provisioning – This sentence relates to authorization, already addressed as a bullet in the list. The act of provisioning is an IT process, not a control, unless the accuracy of the provisioning is verified, which rarely happens, or is automated. De-provisioning – The request and action to de-provision a user is not a control unless the action is automated. Validation of manual actions would be controls, but rarely exist other than through a periodic access review. Physical access – Consideration of physical access is of less importance because of current technology and remote connectivity.
Appendix 4, par 2(b)	Change management process – reference to design should be deleted. In addition, 'programming' is only relevant as part of a control if the focus is on programming to minimize vulnerabilities to attack, which is not typically part of a financial statement audit. Systems development or acquisition or implementation – There is limited, if any, relevance of systems development or acquisition to an IT environment supporting financial reporting. Implementation, however, is very relevant.