Responses to ED–3151
Comments on ‘IT’
NVivo Report 5A
(FOR REFERENCE)

01. Basel

We welcome the increased recognition of IT as an issue that auditors need to consider.

Nevertheless, we recommend that the standard address the nature and extent of IT outsourcing (and possibly outsourcing more generally) by the entity as an activity that the auditor should understand. As drafted, ED-315 contains only one brief reference to IT outsourcing in the application material (ie in paragraph A148 of ED-315).

IT outsourcing is an activity that has been growing in recent years and it introduces new risks and issues around data storage and management that the auditor will need to understand and assess. For example, it is important that the auditor understands the location of data relevant to the audit of the financial statements and whether those data are held by a third party, whether the auditor has access to that data, what security exists around the data, and what management’s controls are around the outsourcing arrangement.

Some possible amendments that the IAASB should consider are:

- Paragraph 23(a)(i) could reference the need to understand the usage by, or reliance of, the entity on third-party providers of IT services; and
- Paragraph 35 could introduce the need to understand the location of data and the involvement of third parties in its storage and management, with further elaboration in the application material (ie in paragraphs A55, A61, and A136–A141).

02. Committee of European Auditing

Information Technology (IT)

Given the increased use of IT in audit, we believe it is important that the standards provide appropriate requirements and guidance in this area, without mandating the use of IT where it is not appropriate for a given audit. We noted some instances however where the terminology in the standard was not used in a consistent way. This applies for instance to the terms automated controls, application controls and automated application controls.

04. IAASA

Information Technology (IT)

- Given the increased use of IT in audit, we believe it is vital that the standards provide appropriate requirements and guidance in this area, without mandating the use of IT where it is not appropriate for a given audit. We have a number of specific comments on the ED relating to IT.

---

1 Exposure Draft International Standard on Auditing 315, *Identifying and Assessing Risks of Material Misstatement*
• The system of internal control as well as the financial reporting process may include relevant tools or files under the responsibility of end users. A definition of ‘End User Computing’ may therefore be beneficial.

• The terms automated controls, application controls and automated application controls are used. The terminology used should be consistent and defined.

• Paragraph A160 states that ‘Such controls consist of application controls and general IT controls, both of which could be manual or automated’. We believe that this is unclear, as application controls cannot be automated.

• Appendix 4 2 (c) ‘Intrusion detection’ could be extended to ‘Intrusion prevention and detection’ to also include preventative protection of the IT environment. The auditor should ensure that mechanisms such as firewalls are in place to protect the entity’s Local Area Network.

• Paragraph A148 and A189 may benefit from the inclusion of cloud computing, considering growing use of this technology. The auditor should identify which type of cloud computing services the client is using, to identify potential risks.

05. IAIS

The IAIS is supportive of the IAASB’s initiatives on improving the auditor’s risk assessment procedures. These improvements are particularly important in the following areas:

− Introduction of new concepts of inherent risk factors and spectrum of risks.

− Clarification that the auditor should perform a separate assessment of inherent risk and control risk.

− Additional emphasis in the standard and application guidance focused on obtaining a sufficient understanding of information technology.

06. IFIAR

As a starting point, we are encouraged by some of the improvements seen in the proposed standard that have the potential to improve the auditor’s risk assessment procedures including:

− Additional emphasis in the standard and application guidance focused on obtaining a sufficient understanding of information technology.

08. IRBA

We support the introduction of the new IT-related concepts and definitions.

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 are 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.

We suggest that the IAASB consider issuing non-authoritative guidance on the new IT-related concepts and definitions, for example staff audit practice alerts.
09. UK Financial Reporting Council

Recognizing that inspection findings by audit regulatory bodies and audit oversight bodies have consistently highlighted issues with respect to auditors’ understanding of internal control and consideration of IT risk, we strongly support the introduction of the new IT-related concepts and definitions, along with the enhanced requirements and much of the application material. The material better reflects the current IT environment and is sufficiently principles-based to allow for changing circumstances.

However, we suggest that relocating some of the application material to a dedicated appendix would be beneficial in reducing the length of the application material overall. For example, the lists of material in ED-315 paragraphs A145, A148, A149 and other paragraphs such as A180 and A183-A187 as appropriate.

11. Australian A&A Standards Board

The AUASB supports the introduction of the new IT-related concepts and definitions. We agree that the enhancements contained in ED 315 assist greatly in understanding the impact of the IT environment and how to identify IT controls, including general IT controls, which are relevant to the audit.

We consider that ED 315 could be enhanced by including the risk factors relating to current and evolving technology which connect to organizational networks, such as infrastructure / software as a service solutions, wireless networks, blockchain, and other technology devices that connect to organisational networks. We also consider the guidance in A7 and A8 to be very technical and may not be sufficiently understood by many practitioners.

12. Canadian AASB

In part. We support many of the enhancements made including to elevate definitions from the glossary and update them in respect of application controls, general IT controls and the IT environment.

However, we believe further improvement is needed in the proposed approach to the information system and communication component.

Lack of clarity in the understanding and evaluation of the information system and communication component

Results of the field testing indicated the requirements in paragraphs 35 and 36, and their relationship with other requirements in the proposals, are not clear. In particular, practitioners were concerned with:

- The depth of understanding required to comply with paragraphs 35(a)-(d) may drive onerous documentation of the business processes related to the information system relevant to financial reporting. For example, the extent of the understanding of the entity’s IT environment considering the broad definition in paragraph 16(g) that includes applications, infrastructure, processes and personnel.

- The types of controls the auditor is expected to identify and evaluate to comply with paragraph 35(a) and paragraph 36. Of particular concern was the reference in paragraph A157 indicating that “controls over the information system are treated as controls in the control activities component”. Some practitioners understood this reference as implicitly requiring an understanding of control activities for significant classes of transactions, account balances and disclosures. Therefore, it wasn’t clear how the requirement in paragraph 36 is different or how it relates to the requirement in paragraph 42 to evaluate design and determine implementation of controls relevant to the audit.
We include the following three recommendations which we believe would bring clarity to the issues discussed above:

i. We believe this component of internal control should be a higher-level understanding of the business processes and how information and data flows through the entity. We suggest that general IT controls, and all controls related to initiation, recording, processing and reporting transactions should be considered in the control activities component. By doing so, the requirement in paragraph 35 could be set at a higher level and focus on how the entity obtains or generates relevant quality information, such as data accuracy in reporting and business policies to address data accuracy and the flow of information. The IAASB may consider the terms used in the COSO framework to describe “information and communication” as this is a widely accepted framework.

ii. We believe this component should also include a consideration of whether it provides an appropriate foundation for the audit or whether there is a pervasive impact on the audit in situations where the methods and controls used in generating this information are weak. An example may be when the entity has no documentation about how transactions flow through the system. In this case, the auditor may need to directly test all information used as audit evidence that is generated by the entity’s system instead of testing operating effectiveness of controls around the generation of that information.

iii. Clarification is also needed regarding how understanding the IT processes, the IT support structure and the IT applications (in paragraph 35(d)) helps the auditor identify or assess risks of material misstatement. Paragraph A180 seems to indicate the purpose is to obtain a high-level understanding of the IT environment to help the auditor identify whether there are IT applications relevant to the audit. If that is the case, the requirement in 35(d) should be moved and incorporated into the requirement in paragraph 40.

13. CNCC-CSOEC

The introduction of the new IT-related concepts and definitions is helpful for the understanding of the IT environment for larger and more complex entities. However, such concepts may appear to be too complex for smaller and less complex entities. We consider that the standard should further clarify the work to be performed in case of simple and low-risk environment, i.e. small or less complex entities, using especially off-the-shelf software packages.

In addition, we are concerned with the introduction of paragraph 36 in the ED that requires the auditor to “evaluate the design of the information system controls relevant to financial reporting”; we believe the exact scope of this requirement and its expected documentation are to be clarified, including in the context of entities where the auditor does not plan to rely on the operating effectiveness of controls.

14. Hong Kong Institute of CPAs

We consider further guidance should be provided on types or examples of audit procedures in assessing commercial software where entities do not have access to the underlying source code.

We note in paragraph 36 that the auditor is required evaluate the design of the information system controls relevant to financial reporting, by understanding how the matters in paragraph 35(a)-(d) are addressed by the entity, and implemented. In the application material in paragraph A154, the auditor is to consider whether such controls would meet their financial reporting objectives, if implemented as designed and
operating effectively. It would be helpful for the IAASB to clarify whether the auditor is expected to test operating effectiveness.

15. IDW - NSS

We support the introduction of the definitions of general information technology controls and IT environment (however, in the definition of IT infrastructure therein, "is comprised of" needs to be corrected to "is composed of" or "comprises", and the second sentence of the definition of application controls needs to be moved to the application material). We also agree that the auditor shall obtain an understanding of the IT environment relevant to the information system as required by paragraph 35 (d), even though, as noted in our response to (a) above, we disagree with the scope of that understanding as required in paragraph 35 (a) that results from the definition of significant classes of transactions, account balances and disclosures. One matter requiring further clarification throughout the standard (both requirements and application material) is the use of the term “risks arising from the use of IT”: risks of what? Risks of material misstatement at the financial statement level? Inherent risks? Control risks? All of these? We presume that since the IT environment, general IT controls and IT applications are dealt with in the draft in the sections on internal control and therefore represent a part of the internal control system, these relate either to risks of material misstatement at the financial statement level (e.g., control environment) or control risks. If not, then further clarification is needed (our response to main question 6 indicates why, in our view, simply using “risks of material misstatement” to remedy this will not suffice).

We also support the introduction of concepts relating to data warehouses, report-writers, and networks in paragraphs A7 and A8 of the draft. However, they are currently written like definitions. Either these need to be moved to the definitions section, or the wording needs to be changed in the application material to assert that this is how these terms may be commonly understood.

While we support the requirements in paragraphs 40 and 41 addressing such matters as automated controls, [controls over] the integrity of information, [controls over] system-generated reports, and general controls, we do not believe that these requirements have been appropriately integrated into the concept of relevant controls so that it is clear when these controls over IT are relevant ("take into account... address or include” as used in paragraph 40 is rather vague), nor has the issue of controls over IT been appropriately structured so that auditors have clear conditions when the controls over IT are relevant.

We also note that paragraph 41 (a) deals with the identification of “risks arising from IT”. We presume this risk identification relates primarily to control risk (see above). If so, this matter ought to be dealt with in the section that deals with the assessment of control risk around paragraph 50 of the draft.

16. Japanese Institute of Certified Public Accountants

Identification of risks arising from the use of IT and general IT controls relevant to the audit (paragraphs 40 and 41).

We believe that the proposals do not sufficiently clarify the identification of risks arising from the use of IT and the general IT controls relevant to the audit. Paragraph 40 states that the auditor shall identify the IT applications and other aspects of the entity’s IT environment that are relevant to the audit based on the understanding obtained in accordance with paragraph 35(d), and the identification of the controls relevant to the audit in accordance with paragraph 39. Also, paragraph 41 states that the auditor shall identify the risks arising from the use of IT and the general IT controls relevant to the audit for the IT applications and other aspects of the IT environment that are relevant to the audit.
However, the scope of the IT applications and other aspects of the entity’s IT environment that are relevant to the audit is not clear from the ED-315. The proposals seem to suggest that, if a risk arising from the use of IT exists but is not related to risks of material misstatement, the auditor is still required to evaluate the design and determine the implementation of general IT controls relevant to such a risk. Also, paragraph 4 (the entity’s risk assessment process) of Appendix 3 “Understanding the Entity’s System of Internal Control” describes cybersecurity risks as risks relevant to reliable financial reporting arising from the use of IT. We are concerned that cybersecurity risks may be misunderstood as typical examples of risks arising from the use of IT. We believe it is necessary to clarify that the auditor identifies risks arising from the use of IT taking into account the likelihood and magnitude of misstatements, and that general IT controls relevant to audits are those only for relevant assertions.

In addition, paragraph 40(b) does not refer to the aspect of management reliance and auditor’s determination on the control which is not consistent with paragraph 40(a). In order to be consistent with paragraph 40(a) and the last sentence of paragraph A186, the following modifications should be made.

(b) Maintenance of the integrity of information stored and processed in the information system that relates to significant class of transactions, account balances or disclosures that management is relying on and that the auditor has determined to be relevant to the audit

- Definition of general IT controls (paragraph 16(e))

The current definition of IT general controls has been changed from “... by helping to ensure the continued proper operation of information system...” to “... by helping to maintain the continued operation, as designed, of the entity’s information system).” It is unclear why “proper” was deleted and “as designed” was added.

- Relationship between the definition of the IT environment and the entity’s process to monitor the system of internal control

According to the definition of general IT controls (paragraph 16(e)), general IT controls include controls over the entity’s IT processes. Also, according to the definition of the IT environment (paragraph 16(g)), the IT processes in the IT environment include “monitoring of the IT environment.” We believe that it is necessary to clarify the relationship between the controls in general IT controls, the monitoring of the IT environment included in the IT environment, and the entity’s process to monitor the system of internal control, which is a component of the system of internal control.

- Definition of “integrity of information"

The term “information integrity” is used in several paragraphs in ED-315. We propose that ED-315 should explain the meaning of “information integrity,” or define it, to clarify the relation with “accuracy” and “completeness” in assertions (paragraph A204).

17. Malaysian Institute of Accountants>

We support the introduction of the new IT-related concepts and definitions. The enhanced requirements and application material 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 are appropriate.

Paragraph 40(b) requires the auditor to consider whether the IT applications include or address maintenance of the integrity of information stored and processed in the information system that relates to significant classes of transactions, account balances or disclosures. ‘Integrity of information’ is not defined
in ED-315. We recommend for ED-315 to include a definition or description of ‘integrity of information’ to clarify the auditor’s consideration when identifying the IT applications that are relevant to the audit.

As more entities are moving towards outsourcing its IT infrastructure or cloud-based IT infrastructure, auditors may face practical difficulties in accessing information on the general IT controls, IT infrastructure or IT applications of a cloud-based service provider. Guidance in relation to the auditor's consideration for such circumstances would be useful.

In addition, it would also be useful if ED-315 can be enhanced to provide examples of IT control deficiencies that may exist and the auditor’s consideration in evaluating and responding to the risk arising from those deficiencies.

8. Nederlandse Beroepsorganisatie van Accountants

There is sufficient attention to IT. However, in the ED IT is dealt with as a separate subject matter. It would be better to integrate this within the audit and not treat it separately.

Furthermore, we wonder whether it is it clear when GITC should be considered, what the impact is on other audit procedures and what the relationship is with application controls. The subject matter is described in a complex and detailed way especially for audits of smaller and/or less complex entities. We recommend providing clear guidance which audit procedures should be performed when only standard commercial software is used in the entity.

Finally, in the ED mainly the design and implementation of IT controls is mentioned (e.g. paragraph 42). More attention should be paid to (the testing of) the operating effectiveness of the IT controls.

19. National Board of Accountants (Tanzania)

We support the introduction of the new IT-related concepts and definitions and also 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 effect of the entity’s use of IT on the identification and assessment of the risks of material misstatements.

20. NZ Auditing and Assurance Standards Board

The NZAuASB strongly supports the new IT-related concepts and definitions. The NZAuASB welcomes the proposed clarifications and enhancements as well as the additional guidance included in ED-315 about risks arising from an entity’s use of IT in its information system.

Notwithstanding the above, the NZAuASB is concerned that the application material corresponding to the requirements included in paragraphs 35(d) and 40 of ED-315 may be difficult to understand and interpret for the auditors of smaller and less complex entities.

Paragraph A144 explains that the objective of performing the required procedures in paragraph 35(d) is to identify and assess risks arising from the use of IT. Paragraph A145 provides examples of such risks. Finally, paragraph A149 explains that obtaining the required understanding in the audits of smaller and less complex entities can be easily accomplished. This paragraph describes matters an auditor may need to consider in such circumstances.
However, the application material does not explain how the recommended work described in Paragraph A149 will relate to the identification of risks arising from the use of IT as discussed in paragraphs A144 and A145 (e.g. whether well-established, reputable and reliable software is immune to unauthorized access or improper changes to data). It also remains unclear whether the auditor of a small and less complex entity that meets the circumstances described in para 149 is required to consider matters included in paragraphs A147 and A148 of ED-315.

Finally, the NZAuASB is concerned that the described circumstances in paragraph A149 for a small and less complex entity is not typical for small and less complex entities in the developed countries. Even micro entities are likely to use electronic banking solutions, software for managing human resources (including payroll processing and employment record keeping), computerised sale and ordering systems and/or inventory management systems in addition to a commercial accounting software. Consequently, the included example in ED-315 for a small and less complex entity may be over simplified and may cause some auditors to underestimate the importance of IT in their circumstances.

The NZAuASB recommends that instead of contrasting a very simple IT environment (where IT is effectively not applicable) to a sophisticated IT environment, the application material considers a spectrum for how the use of IT can influence the information systems (and controls) underlying the financial statements.

21. Altaf Noor Ali Chartered Accountants

We fully support the introduction of IT related concepts and definitions. However, much of the discussion is not relevant for the smaller and less complex entities. Consideration specific to use of third-party software on cloud is not addressed.

22. BDO International

The new requirements in paragraph 40 for the auditor to identify IT applications and other aspects of the IT environment that are relevant to the audit are helpful, particularly since paragraph 40(a) to (d) are fairly clear on what makes these IT elements relevant to the audit.

The application guidance in A181 on a smaller less complex entity’s use of commercial software is helpful, although we feel it is quite an extreme example. The key to the conclusion that there are no IT applications relevant to the audit is that the entity maintains hard-copy accounting records, which is quite rare these days. Our fear is that auditors will misinterpret this example and use it to support the decision to not assess relevant general IT controls. If this example in A181 is retained, we think it should be emphasized that it is rare that all of those conditions will be met, and that the key requirement is that the entity maintains hard-copy accounting records.

The guidance in A183 – A188 on determining whether IT applications or the IT environment are relevant to the audit was also very helpful.

The requirement in paragraph 41 to identify risks arising from the use of IT is significantly clearer than in the current standard. This explicit requirement should improve the auditor’s identification of IT risks. The examples of IT risks in paragraph A145 are useful and easy to understand.

24. Crowe International

We support these improvements and they should improve the application of the standard.
25. Deloitte

DTTL agrees with the inclusion of the new IT-related concepts and definitions. Specifically, DTTL believes that the four criteria to determine IT application relevancy, combined with clarifications on identifying risks arising from IT and the general IT controls to address them, and the need to evaluate design and implementation of said controls only if IT applications are determined to be relevant, represent significant enhancements to the proposed standard that will result in substantial improvements in the risk assessment process.

DTTL would encourage the Board to consider additional expansion of IT content regarding assessing the risks arising from IT and varying the nature, timing and extent of general IT control testing based on those risk assessments. In addition, the Board should consider providing non-authoritative guidance on typical general IT controls to address relevant risks arising from IT described by the IT layer (e.g., application, database, operating system and network).

26. EY Global Limited

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).
27. Grant Thornton International

Reference 1:

We support the introduction of the new IT related concepts and of the definitions. However, we are of the view that the incorporation of IT requirements throughout the components of internal control results in excessive focus on the IT environment and the controls therein. It impairs the auditor’s overall understanding of the IT environment and IT controls and creates the implication that issues with the IT environment or with IT controls, in and of themselves, could cause issues for the component in which it is placed. Further, there is no requirement to document the auditor’s understanding of the IT environment or IT controls in such a manner.

As such, we would recommend further clarification related to the extent of the understanding and evaluation of the IT environment required by the proposed standard and of the overlap of the IT environment and IT controls, and the implications thereof, with the business processes to which they relate. Scalability could also be emphasized by providing explicit guidance on how the proposals in this area can be applied to less complex engagements and, at a minimum, what is required of auditors for such engagements.

Reference 2:

Paragraph 35(d) of the proposed standard, and related application, includes a requirement for the auditor to understand the entity’s IT environment. We are of the view that further guidance in the application material would be helpful in situations where the entity uses an “off the shelf” IT package.

28. KPMG IFRG Limited

We support the introduction of the new IT-related concepts and definitions and agree that these are necessary to ensure that ISA 315 remains fit for purpose in a modern environment.

In connection with the above concerns regarding the understanding to be obtained in respect of the information system and communication component and the evaluation of the design and implementation of controls relevant to financial reporting within this component, the requirement at 35(d) relating to the auditor’s understanding of the IT environment, in particular, gives rise to scope for confusion. In conjunction with the definition of “IT environment” at 16(g), it may appear to indicate that the auditor is required to obtain an understanding of:

− All IT applications and IT infrastructure relevant to financial reporting (not just those relevant to the audit);
− All the IT processes that manage program changes related to the above, that manage operations related to the above, and that monitor the above.

Accordingly, we recommend that the IAASB be explicit as to whether the understanding that is required to be obtained at paragraph 35(d) is intended to:

i. Involve “high-level understanding” to help identify IT applications that may be relevant to the audit, as suggested by A180, with the evaluation required at paragraph 36 being intended to address considerations such as whether the IT environment is appropriate to the size and complexity of the entity (in line with view i) set out in the preceding section).

This appears to be described in A151-7. Paragraphs 40- 41 appear to support this as they require that risks arising from IT and GITCs that are relevant to the audit are identified for the IT applications, IT
infrastructures, and IT processes that are relevant to the audit, and that such identification is “based on” the understanding obtained in accordance with paragraph 35(d) and the identification of controls relevant to the audit in accordance with paragraph 39. Furthermore, paragraph 42 only requires the design and implementation of these controls when they are relevant to the audit.

Paragraph 44 of the EM states that the IAASB is of the view that it is not necessary for the auditor to identify risks arising from the entity’s use of IT or GITCs unless there are IT applications that are determined to be relevant to the audit in accordance with the criteria set out at paragraph 40 of the ED. It would be helpful if the IAASB were to explicitly state this in the ED itself; or

ii. Enable the auditor to identify risks arising from the use of IT, and GITCs. A144 states that the auditor is required to understand the IT environment relevant to the entity's information system because [emphasis added] the entity’s use of IT applications or other aspects in the IT environment may give rise to risks arising from the use of IT.

We highlight that the application material is again unclear in this area, partly because it again co-mingles the concepts of obtaining an “understanding” with evaluation of design and implementation of controls.

We recommend that the IAASB clarify its intentions as to the extent of understanding that is expected regarding the entity’s IT environment, by including similar evaluation milestones to those at paragraphs 28 and 31, versus related requirements at paragraph 40, in particular, to set out explicitly when an auditor is required to identify risks arising from IT and whether this is only when IT applications and other aspects of the IT environment contain application controls relevant to the audit. Furthermore, we recommend that the IAASB distinguish between application material that relates to the understanding of the IT environment and application material that relates to the identification of IT applications and other aspects of the entity’s IT environment that contain application controls that are relevant to the audit and the identification of related risks arising from the use of IT and GITCs.

We suggest that the application material explain more clearly how the understanding of the IT environment would help an auditor to identify and assess the risks of material misstatements, in circumstances where the IT applications and other aspects of the entity’s IT environment do not contain application controls that are relevant to the audit. We also suggest that the IAASB clarify what is meant by a “high level understanding of IT processes and personnel”, as set out in A147.

We also highlight the following concerns with certain definitions:

- Application controls now appear to be defined as all controls (in the entity’s information system) not just controls within an application. We question whether this change is necessary as it may cause confusion;

- The definition of application controls states that “such controls may rely on information, or other controls that maintain the integrity of information, or may rely on the operation of other controls”. We suggest that the IAASB clarify their intention here such as by providing an illustrative example.

29. MNP LLP

The newly introduced IT-related concepts and definitions are, for the most part, easy to read and comprehend. However, we think the application of this material will prove to be challenging. We think that
there is likely to be a knowledge gap between the requirements of the auditor to understand the IT environment and IT applications and the training auditors typically have. Auditors are not, normally, also IT experts, and we believe it may be difficult for the average auditor to understand the IT environment in sufficient depth to translate that understanding into risks. While there is a list of risks arising from the use of IT, these risks are very general and for the most part, apply at the financial statement level (paragraph A145). We recommend that ED-315 be revised to add additional examples of risks at the assertion level. Adding this detail will be very beneficial for auditors to appreciate the benefit of obtaining this understanding and how it influences the risk assessment and overall audit approach.

We also recommend that ED-315 provide more direction on how the information system impacts the audit work. It is sometimes difficult for the auditor to translate understanding of information systems and controls into identifying risk and designing an appropriate audit approach. Further, as noted above, it may not be feasible to involve IT specialists in the majority of audits, especially when IT auditors are a scarce resource in the marketplace.

30. PwC International

Reference 1: (extract from response to question 5(b))

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.

Reference 2: (response to question 5(c))

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.

31. RSM International

- The new IT related concepts and definitions are welcome.
- The material relating to situations in which the entity uses an off the shelf accounting package with limited or no modifications could be given more prominence by including it in the standard itself rather than in the application material. This will often be the case in small or less complex entities.

32. Office of the Auditor-General of Alberta

We agree. We note the definition of application controls should say “detective and corrective” rather than only “detective.”

We note the definition of IT environment, in particular bullet three regarding IT processes, could be modernized. In general, the term IT that is used throughout is too narrow. The standard could better stress how information is a strategic asset of the organization as important as people, capital and infrastructure and that all organizations have a critical dependency on the technology systems that create, store, manipulate and retrieve information. The use of the word IT may bring too much focus onto technology (hardware and software) rather than on the information. A broader and more modern term we suggest is “information and related technology (IrT)” which would help expand auditor attention to issues of enterprise architecture, enterprise information management, governance and management of IrT, and IrT strategy, and related risks. Auditors may also need to consider issues such as privacy and identity management, not just from the integrity of data perspective but also from potential risks of material misstatement due to contingencies arising from inadequate privacy protection, for example.

We suggest guidance be added that the auditor should consider whether the entity uses a generally accepted good practice framework, such as COBIT, to manage its IrT, and to evaluate the risks if the entity does not use such a framework.

We are concerned about the use of the word “high-level” in A147 and A180. What is a “high-level” understanding and would it be appropriate for an auditor to have obtained a “high-level” understanding of the entity’s risk assessment process, to comply with paragraph 29, or a “high-level” understanding of how significant classes of transactions are processed to comply with paragraph 35? We suggest that the ED remove “high-level” as an adjective. The auditor should obtain an understanding.

We note the various items in paragraph 40 are too narrow. In particular, paragraph 40 (a) to (d) are connected by an "or" at the end of paragraph (c). It is unlikely the auditor would select only one of these. We suggest the Board consider how practically paragraphs 40 and 41 would be applied in the case of a spreadsheet that tracks sales, or the alternative case of an ERP on which all operations of the entity rely. In the former case the auditor may (incorrectly) not even consider the spreadsheet to be an IT application. In the latter case, the auditor may (incorrectly) only consider (a) automated controls but not (b) (c) and (d) because of the "or" logic used in paragraph 40. We suggest paragraph 40 and 41 be replaced by the very broad yet clear requirement in existing ISA315.21, which was that the auditor shall obtain an understanding of how the entity has responded to the risks arising from IT [IrT]. The detail in paragraph 40 could be added to the various proposed guidance paragraphs.
We find the guidance in A193 useful regarding specialists. We suggest the ED consider referring specifically to specialists such as Certified Information Systems Auditors that may need to be involved in the audit.

33. Office of the Auditor-General of Canada

Yes, we support the new IT-related concepts and definitions. The enhanced requirements 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.

We suggest the following further improvements:

− The enhanced application guidance found in Appendix 4 – Considerations for Understanding General IT Controls of the proposed standard offers only introductory level insight as to the matters the auditor may consider in understanding general IT controls – additional guidance would be helpful.

− The definition of General IT Controls could explicitly state these controls are indirect in nature, as confirmed by paragraph A197.

35. US Government Accountability Office

We support the introduction of the new IT-related concepts and definitions. We also generally support the enhanced requirements and application material related to the auditor’s understanding of the IT environment, identification of the risks arising from IT, and identification of general IT controls.

However, we believe that ED-315’s discussion of IT should recognize the potential effect of general controls on an IT environment consisting of commercial software. For example, inadequate access controls could result in inadequate segregation of duties.

36. Swedish National Audit Office

We support the approach taken and the use of flowchart to enhance the understanding. There are some areas that would benefit from some clarifications to ensure a more consistent understanding and approach by auditors:

• Paragraph 36. IS controls has a separate flow in the flowcharts – the purpose and impact of the separate flow is unclear. For example, the distinction between the definition of IS controls compared with the “controls relevant for the audit” is not clear (also refers to our comment under b).

• Application controls. We believe it is an advantage having one common term for all “process level controls”. It might be confusing to use the term “application controls” also for controls that are manual (with no automated component). We believe that the common use today of the term “application controls” refers to controls that are either automated or manual with an automated component, therefore, we find the new definition confusing. We would for example suggest using the term “process level controls”.

• Paragraph 40 d) There is a need to clarify why “controls that address RSPA” is a separate category. Does this category create specific requirements, or would it not already be covered in one of the categories paragraph 40 a-c)?

• Paragraph A 103. We believe there is a need to clarify the concept of "direct GITC"?
37. Wales Audit Office

- While the proposed Standard does appear to require an understanding of the IT environment as a whole before focussing in on those controls which are relevant to financial reporting, we believe that this could be stated more clearly than is currently the case.

- We consider that the distinction between commercially available software with no access to source coding and in-house developed software is particularly welcome. However, in paragraph A181, it would be helpful to confirm whether all the listed conditions should be met before dispensing with the need to test or evaluate controls.

- We would suggest that the reference to ‘general’ IT controls should be clarified by providing examples (eg access controls, security controls, change control) of controls which are applied across more than one system.

38. ACCA-CAANZ

We are broadly supportive in principle of the new material on IT-related concepts and definitions. However, it is unclear why some of the material has been included. For example, paragraph A7 refers to ‘data warehouses or report writers’, without articulating how this information will inform the procedures to be undertaken on the audit. On the other hand, we feel there could be more guidance on the boundary of the IT environment where some services are run on cloud services or are outsourced.

39. Accountancy Europe

In general, the introduction of the new IT-related concepts and definitions is helpful for the understanding of the IT environment for larger and more complex entities, but the level of complexity introduced here is wholly unwarranted for the vast majority of very small audits.

Therefore, we think that a conditional paragraph is necessary to introduce a clear exception for entities in a simple and low-risk environment (small or less complex entities, using only ‘off-the-shelf’ software packages). The standard should be clearer on the work effort required from practitioners in such cases – e.g. minimum requirement to assess the modifications or updates made to off-the-shelf software package or modification of standard reports functionalities.

40. AICPA (USA)

Paragraph 16(a) — This paragraph includes a new definition of application controls which includes manual and automated controls. We believe that, in practice, many auditors presume that application controls relate to automated controls and do not intuitively associate the term “application controls” with manual controls. Thus, we believe that the definition of application controls is not consistent with current practice. Because the term is not pervasively used in the ISAs, we recommend the IAASB reconsider whether the definition of application controls is needed. Alternatively, we suggest that the IAASB use another term (such as “transaction controls”, as used in the COSO framework) to refer to those controls.

41. Center for Audit Quality

Paragraph 16(a) of the Exposure Draft defines application controls, but the concept of transaction controls is not included. We are concerned that an auditor will see the term application controls and think the Exposure Draft is referring to automated controls only. We recommend adding an application paragraph to the Exposure Draft. This application paragraph related to understanding the entity and its control
environment could suggest the auditor think about the framework that management has used, if any, to
develop the entity’s control environment. The application paragraph could also include example
frameworks, such as COSO.

42. Chartered Institute of Public Finance & Accountancy

In line with our responses to Question 1, CIPFA considers that much of this material would be better placed
in application material.

43. CPA Australia

Yes, we support the introduction of IT-related concepts and definitions.

44. EFAA

We support the added emphasis on IT in ED-315. However, as we note under our general observations
above, ED-315 tends to treat IT as a stand-alone issue and describes its impact and application in a highly
complex and detailed manner. IT controls are the norm and so need to be seamlessly integrated into the
audit and ISAs. Accordingly, we suggest integrating IT controls and simplifying the text.

As noted in our response to Q2 we are concerned over the increase in material on IT and controls at a time
when technology seems to be encouraging firms to move towards tests of details. We encourage
simplification of the concepts, definitions and application material. Such is the pace of change we fear that
material will rapidly become obsolete and redundant so the simpler and more principles-based the better.

45. Finnish Association of Authorised Public Accountants

Majority of smaller Finnish companies use an ‘off-the-shelf’ software for accounting. They also generally
outsource their accounting. The level of complexity in the revised standard as regards to understanding
and evaluating the D&I of the IT environment is too heavy for a vast majority of Finnish companies.
Therefore, an exception to the requirements should be incorporated in the standard regarding smaller
entities using ‘off-the-shelf’ software. The Standard should be clearer on the work effort required from
auditors in such cases – e.g. a minimum requirement to assess the modifications or updates made to off-
the-shelf software package or the modification of standard report functionalities.

46. Fed of Prof Council of Economic Sciences (Argentina)

I believe that the introduction of new concepts and definitions related to IT improves the understanding of
the components of the internal control system applied to an IT environment. Likewise, Appendix 4 is very
useful to obtain an understanding of the IT environment and identify the relevant controls that should be
considered by the auditor.

47. FSR Danske Revisorer (Denmark)

In general, the introduction of the new IT-related concepts and definitions is helpful for the understanding
of the IT environment for larger and more complex entities. However, the level of complexity introduced is
not relevant for most audits of small and less complex entities.

In our view, the requirements in the standard should describe what, as a minimum, is required when auditing
small and less complex entities that use "off the shelf" software, and the requirements / application guidance
should include additional considerations that should be made when the entity has a more complex IT environment.

48. Interamerican accounting association (South America)

Yes, we fully support the introduction and the corrections proposed as new concepts and definitions related to IT; we understand that such incorporations are not complete, but for now they are sufficient, the immediate future and the accelerated application of artificial intelligence in the audit of financial statements will force the creation of new concepts and definitions related to IT and their incorporation in the ISA. We consider that the improved requirements and the application material that are intended to be incorporated into the NIA to be modified are related to the understanding of the IT environment, but to our point of view it would be necessary to link them with the general objectives of IT, not only with computer controls general however, we understand that for now they are sufficient to support the consideration of the effects of the use of IT by auditors in the entity, whose financial statements have been audited, have done for quite some time, in the evaluations of material errors related to the use of IT by entities.

49. Instituto dos Auditores Independentes do Brazil

The new requirements are helpful and reflect the fundamental importance of IT to financial reporting.

51. Institute of Chartered Accountants in England and Wales

The new IT related concepts and definitions are welcome, although we note in our answer to Q5 above, concerns about the inclusion of this volume of detail in the main body of the standard (rather than an appendix) given long-term trends away from controls testing, even in larger audits. This concern is compounded by terminology in this area not being standardised, and the material being untested. The helpful material relating to situations in which the entity uses an off-the-shelf accounting package with limited or no modifications needs to be given more prominence and, in particular, it needs to be brought to the beginning of the section entitled Understanding the entity’s use of IT, together with paragraph A150 on larger and more complex entities. This is important to avoid creating the impression that smaller firms need to routinely perform a detailed critical analysis of widely used accounting software packages. However, this needs to be balanced with an acknowledgement that in many cases there may well be some risks arising from IT, even though such risks may be low. The material should acknowledge that while the use of off-the-shelf packages does indeed eliminate some risks, other basic controls may be important, including those relating to the physical security of data, and simple controls over the customisation of reports, such as the reporting parameters for receivables listings. In such cases, there may be few IT general controls relevant to the audit and the material on IT general controls, including the material in appendix 4, may be of limited relevance.

IAASB should in the application material distinguish between limited modification – and note that limited modifications may be significant – and no modification, and note that management may not always be aware that modifications have in fact been made.

The statement in the Explanatory Memorandum to the effect that the IAASB is of the view that it is unnecessary for auditors to identify risks arising from the use of IT or IT general controls unless there are IT applications that are relevant to the audit, is helpful. However, over-reliance on untested IT general controls and a lack of understanding of the IT environment remains a widespread cause for concern among regulators and we welcome the enhanced focus on this area, despite the over-engineering.
52. Institute of Chartered Accountants (Ghana)

(i) Do you support the introduction of the new IT-related concepts and definitions?

We support the introduction of the new IT-related concepts and definition. We can infer from the fact that the IAASB introduced the new IT-related concepts and definition to enhance clarity in the application of controls during audit. These enhanced requirements and application materials are very helpful. The separation of information systems and communications from other components of the entity’s system of internal control is a significant shift that will increase focus and understanding in this area. The flowchart for “understanding the IT environment” further enhances our understanding by clearly illustrating the relationship between the IT environment, applications, and IT infrastructure (including database, operating systems, and networks). The guidance on general IT controls and their impact on risk assessment is also very insightful and will make us consider the impact that information processing has on risks and reported numbers that the auditor might not have otherwise considered.

(ii) Are the enhanced requirements and application materials 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?

No, we do not agree with this viewpoint. We are of the view that the identification of the risks arising from IT and the identification of general IT controls is not sufficient to support the auditor’s consideration of the effects of the entity’s use of IT as the auditor is also required to understand the entity’s use of IT in its business and system of internal control. This understanding will form the basis for the auditor’s identification of risks of material misstatement arising from the use of IT.

53. Institute of Chartered Accountants of Pakistan

We support the introduction of the new IT-related concepts and significant enhancement (including elevated definitions given in glossary of terms) to the auditor’s consideration of IT when obtaining an understanding of entity’s internal control. Flowchart 3 also elaborates entity’s use of IT for obtaining understanding of information system relevant to financial reporting and communication component.

54. Institute of Chartered Accountants of Scotland

Reference 1:

The section on IT controls and applications does rather state the obvious and demonstrates how the standard is becoming too explicit and excessively prescriptive by removing some of the reliance on the application of professional judgement. Some of this might be better located in the application material if retained at all.

Reference 2:

While we support the introduction of the new IT-related concepts and definitions, we believe that the section on IT controls and applications does rather state the obvious and demonstrates another example of how the standard is becoming too explicit and removing some of the reliance on the application of professional judgement. Some of this content might be better located in the application material if retained at all.
We would also welcome a conditional paragraph to introduce an exception in the case of entities in a simple and low-risk environment using only ‘off-the-shelf’ software packages. The standard should be clearer on the work effort required from practitioners in such cases – e.g. a minimum requirement to assess the modifications or updates made to an off-the-shelf software package.

55. Institute of Chartered Accountants (Zimbabwe)

Yes, the IT-related concepts and definitions are useful in the auditor’s understanding of the IT environment. The auditor can skeptically identify risks (what can go wrong) within the internal control environment and perform risk assessment effectively.

57. Institute of Public Accountants

The IPA supports the changes to ISA 315 relating to IT concepts and definitions and the related guidance. However, the IPA believes ISA 315 should address the implications of cloud-based services and particularly “software as a service” as they impact general controls and the need or otherwise to obtain ISAE 3402 reports.

58. Institute of Singapore Chartered Accountants

We support the introduction of the new IT-related concepts and definitions. We believe identifying risks arising from the entity’s use of IT is necessary in today’s environment. We are of the view that the IAASB should continue to monitor and assess the impact of entities’ use of IT on audits of financial statements, and provide timely and relevant guidance.

59. Malaysian Institute of CPAs

Yes, MICPA supports the introduction of the new IT-related concepts and definitions as that would help auditors to better appreciate the issues relating to an IT environment which is evolving at a fast pace. And 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 are 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.

Overall, the proposals made relating to the auditor’s understanding of the entity’s system of internal control, as set out in Para 25-44, do 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. The usefulness of the guidance materials could be enhanced if examples of the nature and extent of the understanding of the system of internal control for smaller entities with less sophisticated IT systems and informal documentation around the system of internal control can be provided.

60. New York state society of CPAs

We support the new IT-related concepts and definitions, except for the comments below as they relate to specific explanatory material:

As cited in Paragraph A181, “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 (emphasis added).” The hard
copy records are, in general, generated by the IT systems, so it is almost never the case where IT applications are not relevant to the audit.

We also note in Paragraph A181, “In such a case, the auditor is also likely to be able to obtain audit evidence about the completeness and accuracy of the information produced by the entity used as audit evidence through substantive testing without the need to test controls over its production (emphasis added).” If substantive testing relies on samples selected from data generated by the accounting system, then this would not be true.

Paragraph A184 states, “For system-generated reports to be used as audit evidence, the auditor may obtain audit evidence about the completeness and accuracy of the reports by substantively testing the inputs and outputs of the report. In other cases, the auditor may plan to test the operating effectiveness of the controls over the preparation and maintenance of the report, in which case the IT application from which it is produced is likely to be relevant to the audit (emphasis added).” This is not the case if substantive tests of inputs and outputs are performed by testing samples generated from a system-generated report.

In paragraph A188, we recommend removing the term “may be,” as other aspects of the IT environment are relevant. This doesn’t seem reasonable, as how could there be no IT applications relevant to the audit? This would only be the case in a business that maintains only hard copy records, has no accounting software, does not use email, has no internet connection, and does not use IT in its business. In today’s business environment, it is virtually impossible to operate under such conditions. We further recommend changing “often dependent” to “always dependent” or “almost always dependent.” Finally, the paragraph discusses “when an IT application interacts with vendors or external parties through the internet.” This example only relates to access to the network from the outside. It should also include the Local Area Network, which is always relevant to the audit.

Paragraph A193 states, “Identifying the risks arising from the use of IT and the general IT controls relevant to the audit is likely to require the involvement of team members with specialized skills in IT, other than for the simplest of IT environments (emphasis added).” How do firms determine this? What is the bright line below which IT audit involvement is not required? There is a gray area where it is difficult to determine if the IT environment is more complex or less complex. It takes an IT auditor to make this call.

Paragraph A237 says, “For example, the auditor may consider this to be the case in circumstances where a significant amount of an entity’s information is initiated, recorded, processed, or reported only in electronic form.” It is already the case that almost all financial information is initiated, recorded, processed, or reported only in electronic form. The paragraph also discusses the following:

“such as in an information system that involves a high-degree of integration across its IT applications. In such cases audit evidence may be available only in electronic form, and its sufficiency and appropriateness usually depend on the effectiveness of controls over its accuracy and completeness (emphasis added).”

This is already the case for almost all audits for companies of all sizes. This statement should be changed to “Audit evidence is generally available only in electronic form, and its sufficiency and appropriateness usually depend on the effectiveness of controls over accuracy and completeness.”

61. PAFA

PAFA supports the introduction of IT-related concepts and definitions, however, it is PAFA’s view that the 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 require further enhancement as it is currently not entirely clear how they fit together.

62. SAICA

SAICA agrees with the new IT related concepts and definitions. We further support the requirement to understand the IT environment in respect of the information system relevant to financial reporting (paragraph 35(d)), including the related business processes. We also agree with the requirements to (paragraphs 40-42):

- Identify IT applications and the other aspects of the entity’s IT environment that are relevant to the audit.
- Identify risks arising from the use of IT and general IT controls relevant to the audit.
- Evaluate their design and implementation.

On analysing some of the individual comments received from survey respondents, one gets a sense that although the broad principles may be understood that there is some uncertainty about matters related to their application. For example, the criteria to be taken into account in identifying IT applications relevant to the audit (paragraph 40(a)-(d)). Auditors’ understanding of how these criteria are applied, could be enhanced if the application material in paragraphs A183 to A187 are presented more directly in relation to each of the criteria, including contrasting examples for each in relation to smaller and less complex entities versus larger and complex entities, and more explicitly indicating the interaction between the criteria and when it may be appropriate to conclude that an IT application is not relevant to the audit or that there are no IT applications relevant to the audit.

Paragraphs A149 and A181 make reference to smaller and less complex entities that use commercial software with no or restricted access to the source code to make program changes. The guidance provided seems by some to indicate that the auditor would not plan to test IT application controls under these circumstances and would follow a substantive approach. We believe that guidance for audits of smaller and less complex entities should be expanded to indicate that the auditor could still identify IT applications relevant to the audit under these circumstances, should the auditor consider that testing the operating effectiveness of the controls could be a possible risk response.

SAICA believes that all the requirements relating to the entity’s system of internal controls, including IT controls and how they fit together should be further refined. For purposes of discussing the requirements of ED-ISA 315 in relation to direct controls with our members, SAICA developed the illustration below and suggests that a similar explanation may be useful.
63. SMPC

We note in our answer to question 2, above, our concerns regarding the increase in material on IT and controls at a time at which even larger firms are moving towards tests of details. While we support the new coverage in principle, the new IT-related concepts and definitions and the application material all warrant further work in order to simplify them. A lack of work on IT systems, which is a significant area in many audits reflects a lack of appropriate professional skepticism that the ED seeks to remedy. However, it will require considerable implementation assistance to operationalize.

Terminology in this area is notoriously loose and fast moving and we fear that if IAASB does not move some of this material to appendices, it is likely to bake in confusion and potentially lead to rapid redundancy. Given the length of application material, it would be helpful if more prominence at an early stage could be given to what aspects are relevant to situations in which an entity uses an off-the-shelf accounting package with limited or no modifications.

65. Chartered Accountants Academy (Zimbabwe)

Yes, the IT-related concepts and definitions are useful in the auditor’s understanding of the IT environment. The auditor can sceptically identify risks (what can go wrong) within the internal control environment and perform risk assessment effectively.

66. FocusRoi Inc.

Yes, but this will be a struggle for a lot of smaller practitioners to understand. New training programs are needed here.

67. Lynessa Dias

Agree.
69. Dr. Richard Wittsiepe - Germany

Generally, incorporating information technology, digitization, and artificial intelligence into audits and of using computer-assisted software is a welcome thing.

I have the following two general comments:

A. The concept of commercial software and the associated effects on audits have a conceptual flaw.

The term "commercial software" in A149 as well as in A181 apparently means software to whose source code the company has no access in spite of the option of customizing. This "commercial software" is only intended for small companies and simple processes according to the concept in ISA 315. Under A181, it leads to this software not being relevant to audits and the audit evidence then being obtained by substantive testing.

The advantages of consistently applying IT processes are pointed out in the current version of ISA 315.A76. This leads to the mere determination of the existence of automatic controls being sufficient to determine their effectiveness. Further audit procedures are then no longer necessary.

This approach is generally correct regardless of whether commercial software or customized software is used. However, new technologies allow a broadening of this approach.

Here is an example of this from online retail:

All necessary platforms and other services to operate an online shop can be rented by a company from providers. For example, if a company decides to use Amazon as a provider, the company is tied to Amazon's online order processes. This ensures that only complete data sets such as address data and payment data can be processed. The platform provider specifies a very specific workflow from the order to the delivery, billing, and payment from which the company cannot deviate.

Consequently, commercial software requires a very specific workflow within a company that cannot be deviated from since the workflows are automated, and interventions to the workflows are only made in the event of disruptions. Moreover, only complete data sets can be processed. The applications normally test at least the completeness of data as well as specific relations such as whether the postal code, street, or the credit card information are present. They also normally check delivery capacity, inventory, etc.

This means that even for what is known as commercial software, over whose source code the company has no influence, relevant control processes can be derived, and these control processes are important for auditing. Consistent application of the process and the forced workflow are an advantage in terms of ISA 315.A76 and are an auditing starting point that assumes that there are effective controls.

In principle, this aspect can also be applied to customized software, but normally a precise analysis is required to see whether the system can be circumvented. That is virtually ruled out for commercial software without access to the source code. Changing the predefined workflows is hardly conceivable, for example, when using platforms if the company would have to intervene in the workflow process with Amazon as a platform provider.

There is also another aspect that has not been considered up to this point:

If a company decides to use the Amazon platform, not only is its workflow specified, but there are consequences regarding the quality of information that are important for accounting and auditing. A customer that places its first order from the company via the platform is initially a new customer for this
company, but not for the platform. The customer is signed up with Amazon, has an order and payment history, and can be assessed regarding its payment practices. This also applies to the frequency of complaints and return shipments. The company would not have this information if it only had its own application, which would make new online business more expensive, such as from return shipments and default rates of accounts receivable.

The use of big data in company networks also affects the quality of the information.

I think this aspect should be included in A180 to A 187. The current approach contained in ISA 315.A76 should be maintained.

72. American Accounting Association

We believe the introduction of new IT-related concepts and definitions will improve the quality and relevance of audits. Academic research consistently shows the importance of strong IT controls in the achievement of organizational objectives. For example, Klamm and Watson (2009) suggest that weak IT controls have a pervasive negative impact on a company’s financial reporting process. Correspondingly, Stoel and Muhanna (2011) find that companies reporting IT-related internal control weaknesses report lower earnings and have lower earnings multiples than companies that do not report these weaknesses. Other research suggests that the effects of strong versus weak IT controls extend to management forecasts (e.g., Dorantes, Li, Peters, and Richardson 2012; Li, Peters, Richardson, and Watson 2012).

While we generally believe that the enhanced requirements proposed by ED-315 will support the auditor’s consideration of IT in assessing risks of material misstatement, we think there is room to improve clarity. The guidance in paragraphs A144 through A150 and A180 through A193 (all of which are cross-referenced to ED-315 paragraph 35d) seems disorganized and lacks focus. Each of these paragraphs appears to address one or more specific topics; however, it is difficult to identify the specific topics without reading entire paragraphs. This may make the guidance difficult for auditors to use. We encourage the use of additional headings in this section of the AEM that better organize and more precisely identify the specific topics addressed within each paragraph. Clarity may also be enhanced by grouping portions of the AEM by topic rather than mapping chronologically to ED-315 paragraphs.

Relatedly, we encourage the use of cross-references within the AEM, when applicable. As one example, paragraph A181 appears to refer to criteria that paragraph A149 discusses in further detail. Without a reference to paragraph A149, the wording in paragraph A181 seems vague. Cross-references that identify other related guidance are likely to be highly useful to auditors.

Paragraphs A145 and A148 include lists of items for auditors to consider in identifying and assessing risks. While we find these lists to be instructive, auditors may end up using them as checklists in the field. Research suggests that such decision aids may have deleterious effects on auditors’ performance (e.g., Pincus 1989; Hackenbrack 1992; Asare and Wright 2004; Hammersley 2011; Wood 2012; Dennis and Johnstone 2016; Boland et al. 2018). We encourage wording that more strongly encourages auditors to consider other potential risks/matters.

We also encourage specific discussion around the consideration of IT processes and risks that are centralized (e.g., system access and change management controls that are common across all a company’s applications managed by a central IT group) versus those that are decentralized. When a company manages these IT process-related risks at the entity-level, should auditors identify these risks at the entity-level or at the specific application level (or both)? If auditors can identify IT process-related risks
at the entity-level, would they still need to test these controls on every application that is relevant to the audit? Or is it acceptable for auditors identify IT process-related risks at the entity level and test these entity-level controls using only a sample of applications relevant to the audit? We encourage the Board to provide guidance to address these potential situations.

Conspicuously absent in the requirements of ED-315 is the explicit consideration of cybersecurity which may directly impact data and process integrity and the risk of material misstatement. Cybersecurity has been on the agenda of the PCAOB’s Standing Advisory Group (SAG) for some time, suggesting an expectation that the auditor has a role in considering cybersecurity in an audit (PCAOB 2018); and speaking at a meeting of the SAG in 2016, Chairman Schilder of the IAASB said, "We also have an innovation working group led by the IAASB Deputy Chair, Chuck Landes, where topics like corporate governance and cybersecurity are being explored at an early phase" (IAASB 2016). Further, although an auditor does not yet appear to have been named as a defendant, in 2017 the first four cybersecurity-related U.S. securities class action lawsuits were filed (PricewaterhouseCoopers 2018). Litigation increases risk to the auditor. These things underscore the importance of explicitly addressing cybersecurity risk in the ISA 315. In 2011, the Securities and Exchange Commission (SEC) issued guidance on how IT related incidents related to cybersecurity could result in a material misstatement (SEC 2011). At a minimum, ISA 315 should discuss the types of misstatements identified by the SEC that could result from cybersecurity incidents.

In 2017, the American Institute of Certified Public Accountants (AICPA) released a framework (Trust Services Criteria – the Framework) for assessing cybersecurity risk (AICPA 2017). The Framework was developed to be part of a System and Organizational Controls (SOC) for cybersecurity service but could also be applied to assessing risks of material misstatement related to an entity’s IT functions. It may be appropriate to include or reference elements of the Framework in the AEM to aid in the evaluation of the risk of material misstatement applicable to cybersecurity.