Agenda Item 5-A

ISA 315 (Revised)[1]—Issues and Recommendations (Information Technology)

Objective of the Task Force Discussion

The objective of this agenda item is to obtain Board views on proposals to enhance the requirements and application material in ISA 315 (Revised) to address how an entity's use of Information Technology (IT) affects the auditor's work in identifying and assessing the risks of material misstatement. **Agenda Item 5-B** sets out the proposed changes.

Introduction and Background

1. ISA 315 (Revised) requires the auditor to identify and asses the risks of material misstatement (ROMM's) through risk assessment procedures. Most entities have an IT system in place for recording and processing financial information. These systems may range from non-customized off-the-shelf packages to highly customized and highly-integrated systems.

2. The overall objective and scope of an audit does not differ whether the entity operates in an entirely manual environment, a completely automated environment, or an environment involving some combination of manual and automated elements. However, an entity's use of IT affects the manner in which financial information is processed, stored and communicated and therefore affects the entity's information system and the manner in which the entity implements internal control relevant to financial reporting. At the March 2017 IAASB meeting, a brief introduction to IT in ISA 315 (Revised) was provided (see Appendix 2), but there have been no further Board discussions regarding changes relating to IT.

Extract from March 2017 Meeting Minutes (relating to IT)

INFORMATION TECHNOLOGY

In relation to the matters set out in Agenda Item 4-A relating to IT, Board members generally supported the direction, in particular updating the standard to be more fit-for-purpose in today's IT environment. Board members commented variously that:

- It is very important to illustrate scalability in respect of IT, demonstrating the difference in work effort between complex versus non-complex systems. It was suggested that further consideration be given to implementation guidance once the standard is finalized as appropriate.
- Consideration should be given to describing the benefits of understanding the IT system as this would help auditors understand why an understanding is needed.
- That it is important to maintain the balance on keeping the requirements principle-based and focused on the risks of material misstatement, and not a list of procedures that need to be performed that may result in more complexity than may be needed.
- Consideration should be given to how to emphasize the need for an IT expert – with the right expertise for the relevant system.
- The standard should be clearer on the work effort needed in relation to IT, in particular in relation to the evaluation of the implementation and design of the general IT controls. It was noted that it would be helpful to demonstrate how this would apply in IT systems that are 'off-the-shelf'

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

packages versus complex IT systems. Prof. Schilder added that 'think simple first' would be particularly important to emphasize scalability in the changes developed.

- The impact of artificial intelligence should be acknowledged.

3. Accordingly, the rest of this paper focuses on how ISA 315 (Revised) can be enhanced with regard to the entity's use of IT and the auditor's considerations when understanding the entity and its environment, the applicable financial reporting framework and internal control, and identifying and assessing the risks of material misstatement (ROMMs).

4. The Task Force has been working with a firm IT expert in developing its proposals.

Format of the Papers

5. This paper sets out the Task Force's initial views on changes to the auditor's understanding of each of the components of internal control. However, detailed drafting changes have not been presented (other than to certain definitions as explained later in this paper) as the Task Force is still deliberating the changes needed. This explanation has been provided as context for some of the changes relating to the auditor's considerations about IT that have been presented.

6. This paper then explains the changes that are being proposed and sets out the Task Force's views on IT-related matters.

7. **Agenda Item 5-B** sets out:

   (a) Revised changes to the definitions relating to the system of internal control and controls, mainly to obtain views about whether the revised definition of controls addresses the concerns expressed by the Board in its discussions in September 2017. The Task Force was of the view that these changes were integral to some of the changes proposed relating to IT and have therefore progressed the changes relating to the definition of controls.

   (b) The proposed changes to the existing requirements in ISA 315 (Revised), and proposed new or enhanced application material, for auditor considerations relating to IT. Application material in extant ISA 315 (Revised) has not been presented as no further changes to the existing application and other explanatory material have been considered by the Task Force—changes to all existing application material will be presented to the Board for discussion in December 2017. The new application material presented for discussion in **Agenda Item 5-B** is indicative of those areas where the Task Force believes additional guidance is needed, and is looking for the Board's views on these matters. However, further refinement of the drafting of these paragraphs as application and other explanatory material may be needed.

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

8. In developing changes to ISA 315 (Revised), including enhancing the auditor's considerations about IT, the Task Force is still working through broader revisions and enhancements to the application material, including:

   - Whether changes are needed to Appendix 1 of ISA 315 (Revised), which further explains the components of internal control, and whether those changes or some of the matters set out in Appendix 1, relating to IT but also more broadly, should be left in Appendix 1 or are better placed in application material.

   - How scalability can be more clearly illustrated in the application material.

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

Extract from draft September 2017 Meeting Minutes[2]

OBTAINING AN UNDERSTANDING OF INTERNAL CONTROL

In relation to the proposals to clarify the requirements in the components of internal control so that it is clear what each term in the standard relates to, and what procedures are required, Board members:

- Supported clarification but noted that the focus of understanding appeared to be on controls, which may not be where the focus should be, in particular where the focus should be on the process (such as the entity's risk assessment process) or flow of transactions (when understanding the information system).

- Emphasized the need to further clarify the control activities component, including considering whether this needed to be defined.

- Asked that further consideration be given to what is meant by 'controls relevant to the audit' for each component of internal control, so that auditors could focus on what needs to be done on smaller, less complex audits where controls may not be relied on.

9. The Task Force has been deliberating how to clarify that obtaining an understanding of internal control is done through obtaining an understanding of the five components of internal control, and what this involves. Concern had been expressed that the changes proposed by the Task Force at the September 2017 IAASB meeting focused on controls in each component, and was therefore not clear what is meant by 'obtaining an understanding' versus 'identifying controls relevant to the audit.' In addition, it was also noted that it was still not clear when controls are 'relevant to the audit.'

10. The Task Force therefore continues to deliberate how it can be made clearer what the auditor actions should be in relation to obtaining an understanding of internal control. In considering changes, the Task Force continues to consider if, and how, explicit considerations relevant to IT can be built into obtaining the relevant understanding of each component of internal control.

11. With regard to the requirement for obtaining an understanding of:

    - *The control environment*, the Task Force is of the view that this component is significant because of the impact of the control environment on the other components of internal control, and is continuing to consider how this requirement can be enhanced. The Task Force continues to debate how more fundamental matters relating to the control environment more broadly

[2] These draft minutes are still subject to review by the IAASB.

(such as related to the responsibilities for internal control, including oversight by those charged with governance) can be encompassed in the requirement, with additional guidance to support the enhanced requirement that is broader than just IT.

- *The entity's process to monitor controls*, the Task Force is considering how to describe the understanding required of the entity's process. In making changes, the Task Force will also continue to be mindful that the entity's monitoring process includes how the entity identifies and remediates deficiencies in controls, and how the entity monitors the effectiveness of its controls.
- *The information system, including related business processes*, the Task Force is reconsidering how to refocus the auditor's understanding on the 'flow of transactions' through the information system for the identified relevant classes of transactions and account balances, and related policies and procedures that address accounting records, and the financial reporting process. The Task Force also plans to continue to consider clarifications to distinguish between this component and the control activities component.

12. Changes made to the definitions of 'internal control' and 'controls' (Agenda Item 5-B, paragraph 4)

- In relation to the definition of '*internal control'*:
  - o It was agreed at the September 2017 IAASB meeting that internal control should be referred to as a 'system of internal control' as this presents all of the related aspects more fully than referring to it as a process. Changes have been made accordingly, but other changes to the definition to address Board comments or concerns will be further considered for the December 2017 Board meeting.
- In relation to the definition of '*controls*':
  - o Although not specifically related to IT, the Task Force is of the view that this definition is integral to many of the discussions related to understanding the components of internal control, and would therefore value the Board's further input on whether the revisions to the definition as presented at the September 2017 Board meeting address the concerns that have been raised.
  - o The definition as presented at the September 2017 Board meeting was based on the description of 'controls' in the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) 2013 *Internal Control – Integrated Framework*,[3] with changes as appropriate to put the concept into the context of the ISAs. However, it was highlighted by the Board that controls consist of more than 'policies and procedures,' for example aspects of governance (such as tone at the top) and other aspects of an entity's systems (such as the risk assessment process) could be a 'control' but were not a policy or procedure necessarily.
  - o After further deliberation, the Task Force agreed that it was important to highlight that controls are effected by people (including management and those charged with

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

governance), and could encompass formal or informal policies (i.e., could be formal statements or implied through actions), and that procedures are actions to implement the policies. The Task Force has therefore revised the definition of 'controls' to embed these concepts, thereby clarifying that it is not only formal documented policies and procedures but could also include other aspects of the entity's systems.[4]

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

II. How IT Impacts the Required Understanding

14. ISA 315 (Revised)[5] requires the auditor to obtain an understanding of:

    (a) The entity and its environment;

    (b) The applicable financial reporting framework; and

    (c) The entity's internal control. In obtaining an understanding of the entity's internal control, the auditor is required to obtain an understanding of the five components of internal control:

    (i) Control environment;

    (ii) The entity's risk assessment process;

    (iii) The entity's process to monitor controls;

    (iv) The information system, including the related business processes relevant to financial reporting, and communication; and

    (v) Control activities.

15. The Task Force has considered how IT impacts the required understanding of each of these areas and changes have been proposed. Overall, the Task Force is of the view that only limited amendments are needed to the requirements. However, additional guidance in the application and other explanatory material is essential to help auditors focus on the effects of IT in their considerations related to the various requirements in the standard. The Task Force is also of the view that considerations around IT are to be embedded into each relevant section, and should not be presented as separate "considerations about IT" so as to suggest that considerations around IT are a separate exercise.

16. Appendix 1 to this paper sets out a flowchart to illustrate how the information gathered when 'obtaining an understanding of internal control' (including IT-related information) is used in assessing control risk, and subsequently as a basis for further audit procedures under ISA 330.[6] This also

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

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

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

includes identifying general IT controls, and how this impacts the auditor's assessment of control risk, to help explain the Task Force's views relating to general IT controls.

17. The following sets out the Task Force's views on the proposed changes presented in **Agenda Item 5-B** for discussion.

18. *Risk assessment procedures* (Agenda Item 5-B, paragraph 5)

    - Changes are still to be considered relating to the requirement to address Board comments from the September 2017 discussions. However, the Task Force is of the view that additional application material to this paragraph related to IT be added to make it more prominent that IT considerations are an integral part of the auditor's work and should not be considered a separate exercise. In particular, this emphasis is important for small- and medium- practices who may see IT considerations during an audit as a separate, and not integrated, exercise.

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

    - Most businesses today use IT for commercial purposes as well as internal information processing. A change has been proposed to the requirement to understand the business and operations of the entity to require an understanding about the extent to which the business model integrates the use of IT. The Task Force is of a view that this change recognizes that in today's environment, IT is often integral to the business and may be highly pervasive through the operations of the business.

    - Application guidance has been proposed to enhance the auditor's considerations of IT when obtaining an understanding of the entity and its environment in order to recognize the importance of IT in today's environment. The proposed application material highlights that the understanding of the entity will help the auditor start to create expectations in relation to the extent to which IT is involved in the entity's financial reporting and the related effects on the audit (for example, recognizing that an entity where the business model involves web-based transactions or an entity utilizing blockchain technology in making and receiving payments will likely have effects on the audit, as well as recognizing that in many jurisdictions now there are laws or regulations around IT related matters such as data security).

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

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

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

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

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

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

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

- Additional guidance has been developed about the types of matters that need to be considered related to IT when obtaining an understanding of the entity's monitoring process, including emphasizing that controls could be controls over automated controls in highly automated and complex IT systems, as well as controls that monitor access and segregation of duties.
- It is also noted that further application guidance is to be developed recognizing that internal audit may use IT in undertaking their procedures, as well as to recognize the IT impacts on sources of information.

24. *Understanding the information system, including related business processes, relevant to financial reporting, and communication* (Agenda item 5-B, paragraph 18):

- Suggestions of matters that may need to be considered related to IT when obtaining an understanding of the information system, including related business processes, have been proposed in the application material to emphasize attributes related to entity's use of IT that could be considered. As the Task Force works through distinguishing between this component and the control activities component, some of the matters proposed may move to application material in the control activities component as relevant.

25. *Understanding control activities* (Agenda Item 5-B, paragraphs 20 and 21)

- The Task Force continues to explore how best to describe this category of internal control, in particular when controls are relevant to the audit (including general IT controls) and will present further changes for Board consideration in December 2017 (as noted above). Furthermore, the Task Force is still considering how to provide application material to provide guidance about how an understanding of control activities is obtained, in the context of the changes made in this, and the other components, of internal control.
- In relation to IT related matters, in its deliberations the Task Force has agreed that there are a number of circumstances when general IT controls would be relevant to the audit, and these circumstances have been incorporated in the proposed revised requirement and supporting application material (although the requirement is subject to further refinements as noted in the prior bullet, and therefore the Board should focus on the concepts presented versus the drafting). The Task Force is also of the view that such an approach is helpful to illustrate scalability–in clarifying specific circumstances when general IT controls are relevant to the audit, in smaller entities with less complex IT systems, if the auditor is not going to rely on the automated controls as part of the audit, and if the automated controls do not meet the other proposed described circumstances, the auditor would not need to further consider the general IT controls.

Matters for IAASB Consideration

1. The IAASB is asked for views regarding the proposed changes to the definition of controls as explained in paragraph 12 above, specifically whether this is broad enough to capture other matters that Board members were concerned would be omitted by a more narrow definition.

2. The IAASB is asked for views regarding the proposed changes to ISA 315 (Revised) relating to enhancing the auditor's considerations of IT as explained in paragraphs 18–25 above. In particular, in relation to the proposed requirement to identify and understand general IT controls (as described in paragraph 25), do Board members have the view that describing circumstances that may be indicative of when general IT controls are relevant to the audit should be included in the requirement as presented? Are there other circumstances that should be included?

3. Are there other matters related to IT that the Task Force should be considering in finalizing the proposals for discussion at the December IAASB meeting?

Identifying and Assessing the Risks of Material Misstatement

26. Proposed new paragraph 25D requires that the auditor assesses control risk by:

    (a) Relating the controls relevant to the audit that the auditor intends to test to what can go wrong at the assertion level; and

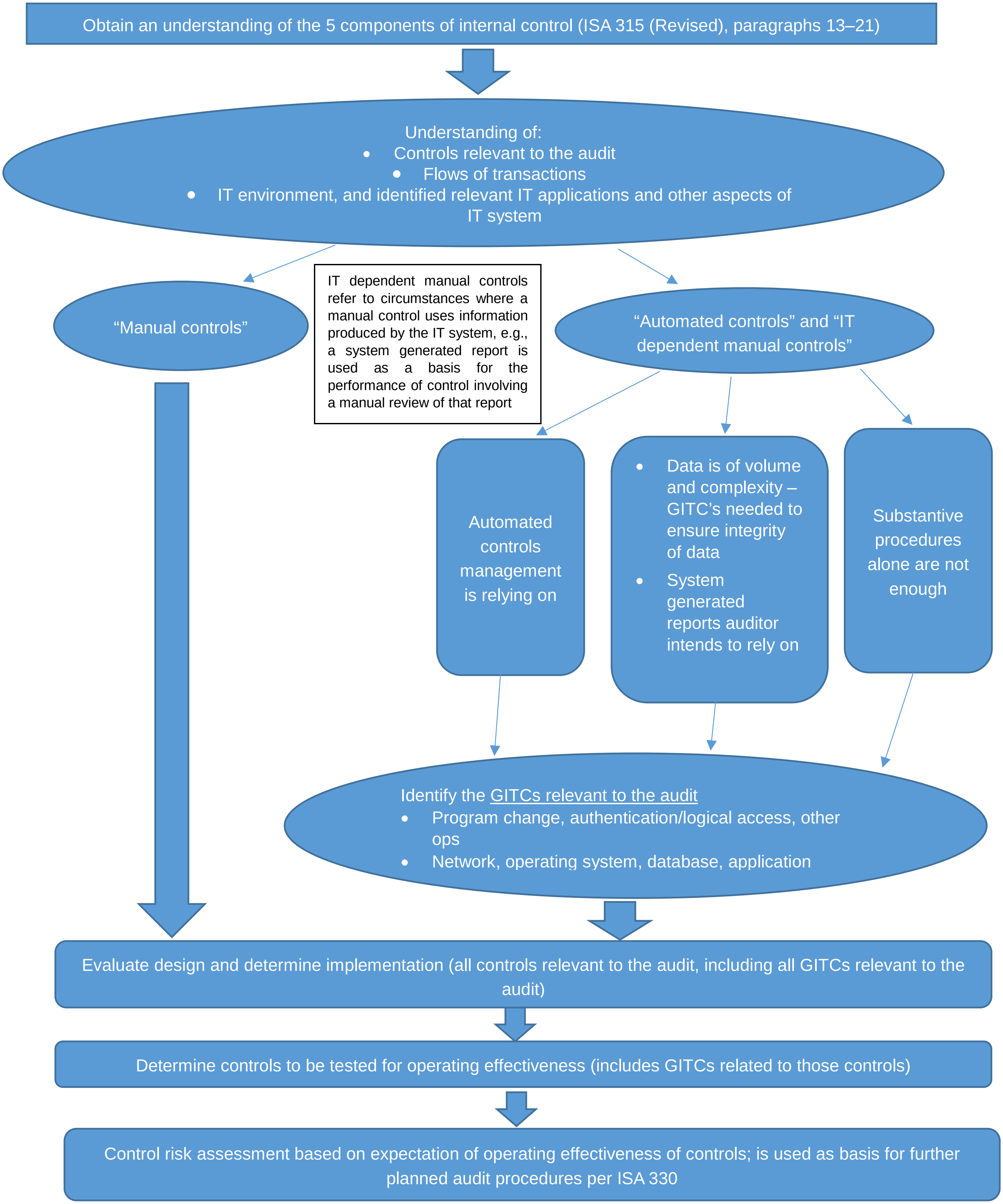
    (b) Considering whether controls identified address inherent risks assessed.

27. In its deliberations, the Task Force has agreed that a separate risk assessment for risks arising from IT is not required, but agreed that the link between general IT controls and the control risk assessment needs to be made (and relevant application material developed), including to address circumstances when GITCs are not present or are found to be ineffective. In addition, the Task Force is still considering whether changes are needed in respect of risks where substantive procedures alone are not sufficient (with any proposed revisions presented in December 2017 for discussion).

Appendix 1

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

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



Obtain an understanding of the 5 components of internal control (ISA 315 (Revised), paragraphs 13–21)

Understanding of:

- Controls relevant to the audit
- Flows of transactions
- IT environment, and identified relevant IT applications and other aspects of IT system

“Manual controls”

IT dependent manual controls refer to circumstances where a manual control uses information produced by the IT system, e.g., a system generated report is used as a basis for the performance of control involving a manual review of that report

“Automated controls” and “IT dependent manual controls”

Automated controls management is relying on

- Data is of volume and complexity – GITC’s needed to ensure integrity of data
- System generated reports auditor intends to rely on

Substantive procedures alone are not enough

Identify the <u>GITCs relevant to the audit</u>

- Program change, authentication/logical access, other ops
- Network, operating system, database, application

Evaluate design and determine implementation (all controls relevant to the audit, including all GITCs relevant to the audit)

Determine controls to be tested for operating effectiveness (includes GITCs related to those controls)

Control risk assessment based on expectation of operating effectiveness of controls; is used as basis for further planned audit procedures per ISA 330

Appendix 2

Extract from March 2017 IAASB Agenda Item 4-A (Information Technology)

1. Respondents to the IAASB's ISA Implementation Monitoring project noted that as a result of developments in IT (explained further below), the complexity of the information systems used by many entities, and the related risks associated with IT, are not sufficiently emphasized in ISA 315 (Revised). Respondents also highlighted that auditors may not be adequately considering the:

   (a) Extent to which the entity utilizes IT and the influence this may have on the auditor's identification and assessment of the risks of material misstatement; and

   (b) Impact of general IT controls on the audit[7] and whether the auditor intends to rely on application controls[8] or not.

2. Accordingly, the Task Force has commenced discussions about the impact of IT on the way that the auditor identifies and assesses the risks of material misstatement, including considerations about what may need to change in ISA 315 (Revised). The following sets out the background to the Task Force's considerations.

3. The Task Force will continue to progress its deliberations about possible changes to ISA 315 (Revised) for discussion with the IAASB at a later meeting, including a more detailed discussion about the impact of general IT controls on the audit and whether the auditor intends to rely on application controls. In exploring how the extent and complexity of the entity's use of IT could be enhanced in the auditor's assessment of the risks of material misstatement, the Task Force is being assisted by a subject-matter expert.

Background–the Need for Modernization of ISA 315 (Revised)

4. IT encompasses the infrastructure and processes to create, process, store, secure, retrieve, study and communicate data and information. It involves the use of a wide range of physical devices such as computers, data and information storage media, networking and communications equipment (such as cables, routers, servers, and Wi-Fi and data network enabled transmitters and receivers) as well as the operating system, data warehousing, database management and application programs that automate the management and communication of data and information.

5. The 'IT revolution' has been a gradual and continual trend toward a broader use of information technology by businesses, governments and society at large. This has been fueled by expediential advances in the speed of data processing and the miniaturization of media for data processing and storage. Also critical has been the subsequent emergence and rapid expansion of wired and wireless digital communications networks, and investment in the capacity and accessibility of the internet including "cloud computing". Taken together with the scale of investment, the application of these advances has been achieved at an ever-reducing cost. While a distinction was once made between "Information Technology" and "Information and Communications Technology" (the latter including voice and video telecommunications technology), in practice these technologies have been merging for some time, with the digitalization of communications and the use of data networks for mobile data distribution and retrieval.

[7] ISA 315 (Revised), paragraph A108

[8] ISA 315 (Revised), paragraph A109

6. As a result, there:

- Are richer and deeper sources of data (whether about an entity themselves or other entities);
- Is much greater capacity to analyze that data to produce information that is more targeted, relevant and reliable; and
- Is more timely accessibility to, and communication of, that data and information.

IT is gradually becoming the medium for all data and information creation, processing, storage and communication. There is a complementary major decline in the use of paper-based records in these processes and a major shift in the skills and expertise needed to manage businesses and other entities, and their IT strategy, architecture and operations.

7. As IT becomes the medium in which nearly all audit evidence is established, it becomes increasingly important to understand an entity's IT system, including how the integrity of the information is maintained. This is the case whether such audit evidence is produced by, or available from sources external to, the audited entity. As a result, the relevance and reliability (appropriateness) of audit evidence is becoming more critically dependent on the IT processes and controls that shape its creation, processing, storage and communication. For example:

- There is an increasing trend for business processes to be "paperless" such that verification of electronic transactions to hard copy accounting records (e.g., shipping documents, price lists) may not be possible. Even if paper documents are prepared these are often converted to digital form.
- Risks of unauthorized access to systems have evolved and increased, with cyber-security a focus for many entities, which increases the importance of the auditor understanding the entity's authentication protocols and how access to financial reporting applications is controlled.
- Methods of data storage and data security have changed significantly due to the ease with which entities may store large volumes of data. This increases the importance of managing data risk including that related to the transfer of data relevant to financial reporting from applications to separate data warehouses.
- Entities are outsourcing IT operations to service providers, which may include outsourcing an entire IT environment to an external hosting service provider, or outsourcing certain aspects, such as moving applications to, or storing data within, "cloud" environments. This means that relevant controls over such applications or data may include controls located outside the entity and for which complementary "user-side" controls in the entity's IT environment may be needed.

Impact of IT on an entity's controls

8. Controls are aspects of one or more of the components of an entity's internal control. They are the policies and procedures that in effect define the internal control process that management and those charged with governance have established to address the identified business risks that threaten the achievement of the entity's objectives with regard to the reliability of financial reporting, the effectiveness and efficiency of operations, and the entity's compliance with applicable laws and regulations.[9]

[9] Paragraph 4(c) of ISA 315 (Revised) defines internal control as "the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting., effectiveness and efficiency of operations, and compliance with applicable laws and regulations. The term "controls" refers to any aspects of one or more of the components of internal control."

9. Entities often make extensive use of IT in applying both the policies and procedures that define the financial information preparation processes in the information system relevant to financial reporting and those that define control activities over the financial information preparation processes. Entities also make use of IT in applying the policies and procedures that define other components of the entity's internal control. The use of IT in any of these applications of policies and procedures may be an important consideration for the auditor, when those policies and procedures (controls) are relevant to the auditor's consideration of audit evidence.

10. Controls could be automated controls (e.g., controls embedded in computer programs), manual controls, or a combination. Both manual and automated controls are relevant to the auditor's risk assessment and further audit procedures based thereon.[10] Manual controls may be independent of IT (referred to hereafter as "manual controls"), may use information produced by IT (referred to hereafter as "IT-dependent manual controls"), or may be limited to monitoring the effective functioning of IT and of automated controls, and to handling exceptions.[11] The nature and extent of controls, whether they are manual or automated vary with the nature and complexity of the entity's use of IT.

The Impact of IT on Identifying and Assessing the Risks of Material Misstatement

11. Developments in IT, including the information systems used by entities to initiate, record, process and report transactions or other financial information, have been significant since ISA 315 (Revised) was issued in 2003, requiring a renewed focus by auditors of the impact of IT on the audit of entities of all sizes.

12. The overall objective and scope of an audit does not differ whether the entity operates in an entirely manual environment, a completely automated environment, or some combination of manual and automated environment. However, an entity's use of IT affects the manner in which financial information is processed, stored and communicated and therefore affects the entity's information system and the manner in which the entity implements internal control relevant to financial reporting.

13. From the auditor's perspective, the entity's use of IT affects:

    (a) The procedures performed by the auditor in obtaining an understanding of the entity and its environment, including its internal control;

    (b) The consideration of inherent risk and control risk through which the auditor identifies and assesses the risks of material misstatement;

    (c) The auditor's design of the nature, timing and extent of further audit procedures; and

    (d) The performance of those procedures to obtain sufficient appropriate audit evidence.

    The auditor's considerations about IT and related work effort is directly impacted by the complexity of the IT system being used. It may range in complexity from 'off the shelf-packages' to highly-customized and highly-integrated systems, including integration with systems and applications external to the entity.

[10] Paragraph A61 of ISA 315 (Revised)

[11] From paragraph A62 of ISA 315 (Revised)

Task Force Views

14. As IT has become much more integrated into the information systems and business processes of the entity, the Task Force is of the view that the pervasiveness of IT should be more specifically recognized in the requirements and application material in ISA 315 (Revised):

    - With regard to the requirements in paragraphs 11–24 of ISA 315 (Revised), the Task Force plans to consider how IT can be explicitly recognized in the requirements for understanding the entity and its environment, and related internal control, as changes to these paragraphs are made.
    - With regard to the application material, the Task Force is of the view that the related application material to 11–24 of ISA 315 (Revised) be substantially enhanced (including as it relates to general IT controls as discussed further below).

    In making changes, the Task Force also intends to consider the impact of decentralization of IT (e.g., outsourcing the IT function to third-party service organizations), and the impact of mobile and web-enabled technologies.[12] Further discussion about some specific aspects where changes have been considered by the Task Force is set out below.

15. The Task Force is also of the view that various terminology changes are needed to reflect developments in technologies and systems that have occurred since ISA 315 (Revised) was first issued (including within Appendix 1 of ISA 315 (Revised)), and the Task Force will continue to explore changes as necessary.

Obtaining an Understanding of Internal Control

Requirements and Guidance in Extant ISA 315 (Revised)

16. Paragraph 12 of ISA 315 (Revised) requires the auditor to obtain an understanding of internal control relevant to the audit. The implementation of this requirement is further explained by detailing the five components of internal control (see footnote 12 of this paper for the five components) and what is required for each of these components (paragraphs 14–24 of ISA 315 (Revised)). The application material associated with Paragraph 12 of ISA 315 (Revised) contains guidance[13] related to IT considerations in obtaining an understanding of internal control, however, that guidance is not specific to each of the five components of internal control (i.e., relates to obtaining an understanding of internal control in general). Appendix 1 of ISA 315 (Revised) contains internal control component-specific guidance, however it does not contain much guidance relevant to IT considerations within each component of internal control.

Task Force Views

17. Because of the significant impact of IT on internal control, the Task Force is of the view that there are aspects of IT and how the entity uses IT that need to be understood related to each of the five components of internal control, in order for the auditor to effectively identify risks arising from IT that may affect the auditor's identification and assessment of inherent risk or control risk, and ultimately the identification and assessment of the risks of material misstatement. The extent to which the application guidance for to the requirements in paragraphs 14–24 of ISA 315 (Revised) related to understanding each of the components of internal control specifically addresses IT considerations varies.

[12] In considering the changes, the Task Force will also be mindful of the updates that have been made within the 2013 *Internal Control – Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), in particular those relating to general computer controls and information technology controls.

[13] Paragraphs A61–A67 of ISA 315 (Revised)

18. Although the application material to paragraph 12 of ISA 315 (Revised) is useful to the auditor's overall understanding of risks related to IT and types of controls that might be relevant to the audit, enhancing the application material in relation to each of the five components of internal control for relevant considerations about IT could be improved. The most obvious area for understanding the impact of IT on the entity is the auditor's required understanding of the entity's information system and business processes, which is discussed in further detail below. However, the guidance to the auditor's understanding of the other components of internal control could also be enhanced to include considerations about IT, for example:

- In relation to the control environment—the auditor could consider whether the importance and governance the entity places on IT is commensurate with the nature and size of the entity and its business. This could include understanding the extent of governance over IT functions, the management organizational structure regarding IT and the resources allocated to IT (such as investment in appropriate systems and related maintenance, and employing a sufficient number of appropriately skilled individuals).
- In relation to the entity's risk assessment process—the auditor could consider the elements of the entity's risk assessment process relating to IT, for example:
    - Risk related to IT in the context of the business (e.g., technological obsolescence);
    - The entity's core business activities (i.e., the extent that an entity's business model and operations rely on IT);
    - Whether the entity's risk assessment process adequately addresses risk factors related to IT, for example, implementation of new IT systems, implementation of an identity and access system, consideration of IT risk related to wire transfers; and
    - Whether there is, in the context of the complexity of the entity's IT systems, adequate focus by the entity on IT or technology risks.
- In relation to monitoring of controls—the auditor could consider how the entity monitors internal control, in particular when more sophisticated software applications are part of the financial reporting process. For example, monitoring of automated controls and general IT controls is performed in some entities through automation or "real-time monitoring" applications.

19. The Task Force will continue to explore how best the standard can be enhanced to better explain the impacts of IT on each of the components of internal control.

Obtaining an Understanding of the Information System Relevant to Financial Reporting

20. The entity's information system relevant to financial reporting is a part of the entity's broader information system, and is included within the components of internal control relevant to the audit.[14] It includes the policies and procedures (including the related methods and records) that define how information relevant to financial reporting is prepared. This includes the processes for initiating or capturing the underlying data (relating to transactions, other events and conditions), storing and processing that data, reporting related information, securing the integrity of the data and information, and preparing the financial statements (together referred to hereafter as "financial information preparation processes"). It includes related

[14] One of the components of internal control is the information system, including related business processes, relevant to financial reporting and communication (see paragraph 18 of ISA 315 (Revised)).

business processes in which such financial information preparation processes occur and other aspects of the entity's information system relating to information disclosed in the financial statements, whether obtained from within or outside of the general and subsidiary ledgers.

21. Through obtaining an understanding of the information system, including the related business processes, is primarily how an auditor gathers information about the IT applications, databases and other electronic sources (or related IT service providers) that an entity uses to capture events and process transactions relevant to financial reporting. This understanding in turn provides important context to the auditor's identification of control activities relevant to the audit, including general IT control activities.

Requirements and Guidance in Extant ISA 315 (Revised)

22. Paragraph 18 of ISA 315 (Revised) requires the auditor to obtain an understanding of the information system, including the related business processes, relevant to financial reporting. Included in paragraph 18(b) of ISA 315 (Revised) is the requirement for the auditor to obtain an understanding of the procedures, within both IT and manual systems, by which the classes of transactions that are significant to the financial statements are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in the financial statements. Paragraphs 18 (c), (d) and (e) require an understanding of the related accounting records, supporting information and specific accounts in the financial statements that are used to initiate, record, process and report transactions; how the information system captures events and conditions, other than transactions that are significant to the financial statements; and the financial reporting process used to prepare the entity's financial statements, all of which may also be impacted by the entity's IT system being used. Paragraph 19 requires the auditor to understand how the entity communicates financial reporting roles and responsibilities, which may also be relevant to understanding how IT may be used to accomplish effective communication.

23. Although not specifically emphasized in ISA 315 (Revised), the discussion related to manual and automated elements in paragraphs A61 and A62 of ISA 315 (Revised) in practice applies to paragraph 18 of ISA 315 (Revised). This is in relation to paragraph 18(c) of ISA 315 (Revised), which refers to manual or electronic forms of accounting records, information and specific accounts in the financial statements, paragraph 18(e) of ISA 315 (Revised) which refers to the financial reporting process used to prepare the entity's financial statements, which may include use of IT, ranging from IT systems that may include some automation to systems that are fully automated, and paragraph 18(f) of ISA 315 (Revised) related to understanding controls around journal entries, which likely have some form of automation associated with them.

24. Paragraph 5 of Appendix 1 of ISA 315 (Revised) indicates that an information system "consists of infrastructure (physical and hardware components), software, people, procedures and data and includes reference to the fact that many information systems make extensive use of IT.

Task Force Views

25. As part of understanding the information system including relevant business processes, the auditor gathers information about the IT applications, databases and other electronic sources (or related IT service providers) that an entity uses to capture events and process transactions that are relevant to financial reporting. Beyond identifying the accounting and other applications that are used in the business processes, auditors also typically understand:

- Data—how the entity stores the electronic data produced by the applications or obtained through other means (e.g., application databases, data warehouses or data storage through use of external service providers);
- System-generated reports—whether separate applications exist that access, use or format this data for financial reporting purposes (e.g., report-writer applications).

26. In obtaining this understanding, the auditor considers the different elements of the entity's IT environment, some of which may be relatively straightforward (in particular where the entity may use "off-the-shelf" packages or applications within which data is stored and may include some functions to create system-generated reports).

27. The Task Force is of the view that appropriate principle-based requirements for the auditor's understanding of IT as it relates to the entity's information system, allowing for scalability from less complex IT systems to those that may require a deeper understanding because of their complexity, would enhance the auditor's understanding of how the information in the financial statements is generated, thus helpful for identifying and assessing the risks of material misstatement. Supporting application material explaining different types of systems and the related work effort could be developed to distinguish the nature and extent of work for complex versus less-complex systems. For example, if outside IT service providers are used, examples of the matters that could be considered by the auditor about the integrity of the information generated could help illustrate what is needed in these situations. The Task Force will continue to explore more specific changes in ISA 315 (Revised).

Identification of General IT Controls Relevant to the Audit

28. The guidance in ISA 315 (Revised) related to general IT controls describes how general IT controls could be effective when they maintain the integrity of information and the security of the data the IT systems processes, but provides little guidance regarding the auditor's determination of how they are relevant to the identification and assessment of risks of material misstatement. Paragraph A108 of ISA 315 (Revised) sets out examples of general IT controls, which are likely to be more relevant in those audits where the IT system is not an "off-the-shelf" system.

29. The Task Force is of the view that in order to promote consistency in the auditor's identification and understanding of general IT controls when they are relevant to the audit, the guidance related to general IT controls in ISA 315 (Revised) needs to be substantially enhanced.

30. As an outcome of the auditor's understanding of the information system, an understanding of the IT environment and the relevant applications is obtained. These are the possible elements of IT for which the auditor may determine that general IT controls relevant to the audit exist. In the Task Force's view, the determination of which applications and other elements of the IT environment the auditor should obtain an understanding of the general IT controls (and are therefore relevant to the audit) is driven by the following factors:

    (a) The nature, extent of change, and level of interaction among the IT elements in the IT environment (i.e., what extent of auditor understanding may be needed based on the complexity of the IT environment);

    (b) Controls enabled by IT that are included in the auditor's determination of control activities relevant to the audit and the audit strategy decisions taken that influenced their selection; and

(c) The extent of the auditor's planned use of information produced by the entity's IT applications in performing further audit procedures.

31. In particular, highlighting that general IT controls may still be relevant in less complex environments and when the auditor is not planning to take account of the operating effectiveness of controls, and plans to pursue a primarily substantive strategy, will also help auditors understand the nature and extent of work to be undertaken in respect of general IT controls.

32. The extent of an auditor's effort that is required to identify and obtain and understanding of the general IT controls relevant to the audit depends largely on the complexity of the IT environment. For example, it is likely to involve less effort for a small and medium-sized entity's (SME) environment because auditors of SMEs are more likely to encounter "off-the-shelf "or packaged software where the entity does not have the ability to, or has limited ability to, make changes to the application as there is no access to the source code. In the absence of access to the application source code, program change controls would likely not exist. However, most off-the-shelf software applications do allow for a certain amount of configuration, and the process and controls relevant to changing configurations may be relevant. In all cases, the applications should be secured with authentication (i.e., passwords) and access controls and these would likely be general IT controls relevant to the audit. Accordingly, supporting application material could be developed to address the least complex IT environments for which there may be few general IT controls relevant to the audit. Further enhancements to the application material could then deal with more complex IT environments and how such complexity affects the nature and extent of general IT controls relevant the audit.

33. The Task Force will continue to explore the auditor's consideration of general IT controls and the impact on the nature and extent of work required for the identification and assessment of the risks of material misstatement.