Agenda Item 4-A

ISA 315 (Revised)[1]—Issues and Task Force Recommendations

A draft summary of the IAASB's discussions and decisions at its December 2016 meeting can be found in Appendix II to this paper.

Objective of the IAASB Discussion

The objective of this agenda item is to obtain the Board's views on the ISA 315 (Revised) Task Force's views and recommendations related to various matters described in this paper.

I. Issues Explored by the Task Force and Structure of this Paper

1. The IAASB considered recommendations from the ISA 315 (Revised) Task Force (the Task Force) at its December 2016 meeting related to various matters including the identification of inherent risks, the identification of significant classes of transactions, account balances and disclosures, spectrum of risk, significant risks and understanding internal control. The Task Force Chair noted that issues related to control risk would be addressed at the March 2017 IAASB meeting. A significant aspect of control risk relates to considerations around information technology (IT), which is also an important aspect when obtaining an understanding the entity. The Task Force's initial views and discussions relating to internal control and information technology, as well as various other matters, are set out below.

2. This paper explores issues and Task Force views and recommendations related to the following topics:

   (a) *Information Technology*—initial discussions about the necessary understanding by the auditor of IT in obtaining the required understanding of the entity and its environment, including the entity's internal control (Section II).

   (b) *Internal Control: Control Activities Relevant to the Audit*—Further consideration of guidance to assist auditors in identifying control activities relevant to the audit (Section III).

   (c) *Risk Assessment*—Separate or combined assessment of inherent risk and control risk (Section IV).

   (d) *Significant Risk*—Exploring a new proposed working definition of significant risk in addition to consequences, impediments and benefits of the proposed direction in clarifying the concept of significant risk (Section V).

   (e) *Data Analytics*—With input from the IAASB's Data Analytics Working Group (DAWG), exploring how the use of technology, specifically data analytics, is able to support the auditor's risk assessment procedures, including initial discussions on how data analytics could best be incorporated into ISA 315 (Revised) (Section VI).

   (f) *Professional Skepticism*—Building off of the Professional Skepticism Working Group's (PSWG) discussions with the IAASB at the June, September and December 2016 IAASB meetings,[2] initial

[1] International Standard on Auditing (ISA) 315 (Revised), *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment*. References to the ISAs in this paper are to the 2016—2017 IAASB Handbook, a copy of which has been provided as a Supplement to Agenda Item 4.

[2] The Task Force's initial consideration about professional skepticism has also been informed by the PSWG's Professional Skepticism Matrix presented to the Board for discussion in June 2016 (see Agenda Item 2-B).

Task Force considerations of possible enhancements to ISA 315 (Revised) to enhance the application of professional skepticism when performing risk assessment procedures during the audit (Section VII).

II. Information Technology

3. 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[3] and whether the auditor intends to rely on application controls[4] or not.

4. 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.

5. 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)

6. 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.

7. 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.

---

[3] ISA 315 (Revised), paragraph A108

[4] ISA 315 (Revised), paragraph A109

8. 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.

9. 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

10. 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.[5]

[5] 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."

11. 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.

12. 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.[6] 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.[7] 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

13. 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.

14. 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.

15. 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.

[6] Paragraph A61 of ISA 315 (Revised)

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

Task Force Views

16. 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.[8] Further discussion about some specific aspects where changes have been considered by the Task Force is set out below.

17. 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)

18. 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[9] 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

19. 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.

---

[8] 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.

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

20. 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.

21. 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

22. 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.[10] 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

[10] 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.

23. 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)

24. 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.

25. 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.

26. 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

27. 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).

28. 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).

29. 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

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

Matter for IAASB Consideration

1. The IAASB is asked for its views on the Task Force's deliberations about the impact of IT on the auditor's risk assessment procedures, and whether there are other specific considerations that the Task Force should explore as it progresses its thinking on possible changes to ISA 315 (Revised).

III. Internal Control–Control Activities Relevant to the Audit

Introduction

36. The Task Force has continued its discussions related to the requirement in ISA 315 (Revised) for the auditor to obtain an understanding of internal control relevant to the audit.[11]

37. In its previous discussions, the IAASB agreed that the five components of internal control[12] are interlinked and therefore are relevant to the audit, to the extent they exist. Controls exist within each component of internal control and it is the determination of which of those controls are "relevant to the audit" that has been challenging for auditors. The Task Force has started exploring ways to provide further clarification of what is meant by "controls relevant to the audit" for each of the five components of internal control. In

[11] Paragraph 12 of ISA 315 (Revised) requires the auditor to "obtain an understanding of internal control relevant to the audit."

[12] (i) Control environment; (ii) the entity's risk assessment process; (iii) the information system, including the related business processes, relevant to financial reporting, and communication; (iv) control activities relevant to the audit and (v) monitoring of controls.

exploring the impact of IT in the auditor's understanding of internal control as set out in **Section II**, the Task Force identified that the relevance of general IT controls to the audit is in part dependent on the control activities relevant to the audit (see paragraph 32). The Task Force discussions since the IAASB's December 2016 meeting have accordingly focused specifically on the words "relevant to the audit" in the control activities component. The Task Force's views on controls relevant to the audit within the other four components of internal control will be discussed at a future IAASB meeting.

38. Paragraph A100 of ISA 315 (Revised) notes that control activities relevant to the audit are those:

    (a) That are considered to be relevant to the audit in the judgement of the auditor (as per paragraph 20 of ISA 315 (Revised));

    (b) Related to significant risks (as per paragraph 29 of ISA 315 (Revised)); and

    (c) Related to risks for which substantive procedures alone do not provide sufficient appropriate audit evidence (as per paragraph 30 of ISA 315 (Revised)).

Control Activities Relevant to the Audit–Relevant in the Judgment of the Auditor

39. At the September 2016 IAASB meeting, the Task Force presented the findings from the ISA Implementation Project for Board discussion that the requirement relating to identification of control activities relevant to the audit can be difficult to apply in practice. It was noted that there are different views regarding the extent to which control activities are relevant to the audit when the auditor plans to take a primarily substantive approach to the audit, in particular in audits of SMEs.

40. Paragraph 20 of ISA 315 (Revised) requires the auditor to "obtain an understanding of control activities relevant to the audit, being those that the auditor judges it necessary to understand in order to assess the risks of material misstatement at the assertion level and design further procedures responsive to assessed risks." The Task Force is of the view that additional guidance should be provided to clarify what those situations may be when the auditor uses judgment to determine control activities that are relevant to the audit, such as when, for example:

    - The auditor's understanding of the information system, including the related business processes, indicate that in order to assess the risks of material misstatement an enhanced understanding of control activities is needed, even if the auditor plans to undertake a substantive approach to address the assessed risk.
    - The auditor plans to test controls as part of the response to assessed risks.

Task Force Views[13]

41. Based on the auditor's understanding of the four components of internal control (other than the control activities component), the Task Force is of a view that the auditor gathers a substantial amount of information about the risks of material misstatement (both inherent risk and control risk). Further, the auditor is likely to have formed a view on the audit strategy(ies) that may be most effective to address those risks of material misstatement. At this stage, the auditor may intend to rely on the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures. If so, the auditor's judgment of which control activities are relevant to the audit includes identifying the controls that

[13] The analysis of control activities relevant to the audit in this Section of the paper is without consideration of the relevance of general IT controls to the audit which are subject to separate Task Force consideration as explained in **Section II** of this paper.

the auditor plans to take account of the operating effectiveness thereof. When the auditor intends to take account of the effectiveness of the operating effectiveness of controls, it appears to be clear in practice that those control activities that the auditor intends to take into account are relevant to the audit. Nevertheless, the Task Force is of the view that paragraph A101 of ISA 315 (Revised) should be enhanced to state this more explicitly.

42. If the auditor plans to take a primarily substantive approach, the judgment of which control activities are relevant to the audit is more challenging as highlighted in the ISA Implementation Monitoring findings and accordingly is an issue that the Task Force is specifically exploring.

43. When the auditor intends to take a substantive approach to the audit (whether to all relevant assertions or only certain assertions), the Task Force is of the view that the auditor's judgment of which control activities are relevant to the audit is primarily based on the extent to which the auditor has obtained sufficient information through understanding of the entity and its environment, and the other four components of internal control, to be able to effectively assess the risks of material misstatement at the assertion level, and design substantive procedures in response to assessed risks.

44. In regard to the auditor's determination of whether enough information has been obtained related to risks at the assertion level, the Task Force is of the view that the understanding of the information system, including the related business processes, which includes obtaining an understanding of the flow of transactions from initiation to reporting and the preparation of disclosures in the entity's financial statements (essentially paragraphs 18(a) to 18(f) of ISA 315 (Revised)) has the most influence on this determination. This includes paragraph 18(b) of ISA 315 (Revised) related to understanding the IT aspects of the information system, which as noted previously in this paper, is important when understanding relevant controls.

45. For less complex information systems and business processes, experiences in practice have been that the risks of material misstatement at the assertion level are able to be identified to a sufficient extent after obtaining the auditor's required understanding of the information system. Further, the auditor often has sufficient information from obtaining the required understanding of the information system to determine the nature, timing and extent of the substantive procedures to respond to the risks of material misstatement related to the assertions that are primarily affected by less complex information systems and business processes. The Task Force view is therefore that the auditor may make the judgment that there are no control activities relevant to the audit related to those non-complex information systems and business processes. However, the Task Force is also of the view that the auditor should take into consideration the extent of information produced by the entity that is likely to be used as audit evidence and whether substantively testing such information is most effective to evaluate whether the information is sufficiently reliable for the auditor's purposes. In some cases, the auditor may identify control activities relevant to the audit that address, for example, the accuracy and completeness of certain of the information produced by the entity.

46. As the complexity of the entity, or the information system or a particular business process within an entity, increases (in other words, the identified risk is more likely to be on the upper end of the spectrum of risk), the Task Force is of the view that there is a greater chance that the auditor may identify control activities that are relevant. In addition, there may be regulatory or other expectations regarding the need for auditors to focus on internal controls when performing audits of entity's in certain industries (e.g., the expectations of regulators in the banking and insurance industries) that may result in the auditor needing to obtain an understanding of control activities relevant to the audit regardless of whether the auditor intends to take account of their operating effectiveness.

47. In summary, the Task Force is of the view, that it is likely that the auditor would judge that certain control activities within the information system and business processes are relevant to the audit when:

    - The information system and business processes become more complex;
    - The auditor determines they do not have sufficient information to assess the risk of material misstatement at the assertion level to determine the substantive procedures to respond to the risks of material misstatement after understanding the information system; or
    - The auditor determines that substantively testing information produced by the entity will not be an effective strategy to evaluate whether the information is sufficiently reliable for the auditor's purposes.

48. For these control activities judged to be relevant to the audit, the auditor obtains an understanding of them for the purpose of identifying and assessing risks of material misstatement. If the auditor determines that a substantive approach to further audit procedures is to be adopted, the auditor would not be required to test the operating effectiveness of controls.

49. It is therefore possible, especially for entities with non-complex information systems and business processes, that there are no control activities relevant to the audit other than those for which the auditor has determined to test their operating effectiveness and those specifically required by ISA 315 (Revised). Further, for entities with non-complex information systems and business processes for which the auditor takes a primarily substantive approach to the audit, there may be no risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. Therefore, it is possible for audits of these entities that the only control activities that are relevant to the audit may be those that address significant risks, including fraud risks.

50. The Task Force is of the view that more guidance to clarify the matters noted above in ISA 315 (Revised) would be helpful for auditors to understand when control activities may be relevant. Specifically for audits of SMEs, these clarifications are viewed by the Task Force to be particularly beneficial as feedback suggests that it is not clear from the requirements and guidance in extant ISA 315 (Revised) the extent to which control activities are relevant to the audit when the auditor adopts a primarily substantive approach.

Control Activities Relevant to the Audit–Significant Risks

51. As this is a specific requirement in the ISAs,[14] regardless of the complexity of the IT environment, the information system or business processes, the auditor is required to obtain an understanding of the entity's controls, including control activities, relevant to the significant risks. Controls relevant to significant risks includes those relevant to fraud risks, including controls over journal entries. The Task Force has continued its deliberations related to significant risks, discussed in **Section V** of this paper. As the Task Force's exploration of significant risks continues, the requirement to obtain an understanding of control activities relevant to significant risks will also be considered. At this stage however, the Task Force is not proposing any changes to the extant requirement.

Control Activities Relevant to the Audit–Substantive Procedures Alone are Not Sufficient

52. Paragraph 30 of ISA 315 (Revised) notes that controls are relevant to the audit over risks where the auditor judges it not possible or practicable to obtain sufficient appropriate audit evidence by performing

[14] ISA 315 (Revised), paragraph 29

substantive procedures alone, and the auditor is required to obtain an understanding of the relevant controls. However there is little guidance in ISA 315 (Revised) to assist the auditor in making that judgment.

53. The Task Force is of the view that given the increased use of IT, both as part of an entity carrying out its business objectives, as well as related to the entity's information system relevant to financial reporting, that there are many more circumstances in the current environment where paragraph 30 of ISA 315 (Revised) could apply. The Task Force is of the view that providing more context, including examples, in ISA 315 (Revised) describing situations when substantive procedures alone are not likely to be sufficient to obtain sufficient appropriate audit evidence, would enhance the prominence of this requirement and also assist auditor's in applying judgment in identifying these situations.

Matters for IAASB Consideration

2. The IAASB is asked for its views on the matters relating to control activities that are relevant to the audit, specifically:
   (a) When control activities are judged by the auditor to be relevant to the audit (as set out in paragraphs 39–50).
   (b) Where the auditor judges that it is not possible or practicable to obtain sufficient appropriate audit evidence by performing substantive procedures alone (as set out in paragraphs 52–53).

IV. Risk Assessment

Separate or Combined Assessment of Inherent and Control Risk

54. At the December 2016 IAASB meeting, the Board asked the ISA 315 (Revised) Task Force to further consider whether a combined or separate assessment of inherent risk and control risk would continue to be permitted. This request arose out of the discussion related to introducing a spectrum of inherent risk into ISA 315 (Revised) and whether such introduction would have an effect on the auditor's ability to perform a combined assessment of the risks of material misstatement, as permitted under ISA 200.[15]

55. Paragraph A42 of ISA 200 (see Appendix I) describes how the auditor assesses risks of material misstatement through separate or combined assessments of inherent and control risks. ISA 200 then refers to ISA 315 (Revised) for the requirements and guidance for identifying and assessing the risks of material misstatement at the financial statement and assertion levels.

56. Paragraph 25 of ISA 315 (Revised) requires the auditor to *identify* and *assess* the risks of material misstatement to provide a basis for designing and performing further audit procedures. For this purpose, paragraph 26 (a) and (b) of ISA 315 (Revised) sets out that the auditor shall identify risks, then assess the identified risks:

- Paragraph 26(a): Risks are identified through the auditor's understanding of the entity and its environment. This includes identifying relevant controls that relate to the identified risks.

[15] ISA 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*

- Paragraph 26(b): Identified risks are assessed and the auditor evaluates whether they relate more pervasively to the financial statements as a whole and potentially affect many assertions.

57. To address the assessed risks identified by the procedures in ISA 315 (Revised), paragraph 7 of ISA 330[16] (see Appendix I) requires the auditor to consider the reasons for the assessment given to the risk of material misstatement at the assertion level separately for inherent risk and control risk in order to design appropriate audit procedures to be performed to respond to the assessed risks.

Task Force Views

58. Because paragraph 7 of ISA 330 requires the auditor to consider inherent risk and control risk separately (in order to respond appropriately to assessed risk of material misstatement), the Task Force is of the view that the drivers of each element of the risk of material misstatement (i.e., the driver(s) of inherent risk and the driver(s) of control risk), need to be identified separately by the auditor when performing the risk assessment procedures required by ISA 315 (Revised).

59. From a practical standpoint, in understanding the entity and its environment, including internal control, the Task Force is of the view that the auditor gathers information that leads to, and results in, the auditor's separate identification of inherent risks and control risks. Using the separately identified inherent risks and control risks, the auditor has two options under ISA 200 to perform the assessment of the risks of material misstatement. The assessment of inherent risk and control risk may be performed separately to arrive at the assessment of the risk of material misstatement at the assertion level, or the assessment of the risk of material misstatement at the assertion level may be done simultaneously without the separate underlying assessments of inherent risk and control risk. The Task Force therefore views a "combined" assessment of inherent risk and control risk as resulting from the auditor making the assessments of inherent risk and control risk "simultaneously" but with consideration given to both the underlying inherent risks and control risks that have been identified.

60. Accordingly, the Task Force is of the view that possible changes to ISA 315 (Revised) could include:

- Clarification in paragraphs 25 and 26 of ISA 315 (Revised) to:
  - (i) Focus auditors on the separate *identification* of inherent risk and control risk.
  - (ii) Help auditors understand that the *assessment* of the risk of material misstatement at the assertion level may either be done separately or simultaneously, explaining in the application material that the outcome of either approach is intended to result in the same responses to the identified risks. The Task Force is of the view that rather than referring to "separate or combined", the wording be revised to refer to "separate or simultaneous" assessments of inherent and control risk, as they are not 'joined' but rather done at the same time.
- Moving the guidance in paragraph A42 of ISA 200 to ISA 315 (Revised) to include it in the context of the auditor's risk assessment procedures. The reference to ISA 315 (Revised) in ISA 200[17] would then drive auditors to the requirements and guidance around the assessment of the risk of material misstatement.

[16] ISA 330, *The Auditor`s Responses to Assessed Risks*

[17] ISA 200, paragraph A43

61. As the Task Force progresses possible changes, it will continue exploring through its outreach how 'combined' risk assessments may be performed in practice to validate its understanding and direction for the possible changes in ISA 315 (Revised) as noted in paragraph 60 above.

Matters for IAASB Consideration

3. Do IAASB members agree with Task Force's recommendations for possible changes to ISA 315 (Revised) in paragraph 60? IAASB members are asked:

   (a) To share their views as to why they do or do not agree.

   (b) Whether there are any further implications of these changes not yet considered by the Task Force?

   As the Task Force continues to explore the implications of a 'combined' risk assessment, Board members are asked to share examples of where a combined risk assessment is performed.

V. Significant Risk

62. Paragraph 4(e) of ISA 315 (Revised) defines significant risk as "an identified and assessed risk of material misstatement that, in the auditor's judgment, requires special audit consideration." Paragraph 27 of ISA 315 (Revised) adds further complexity to the determination of significant risks, as it requires the auditor to determine whether any of the risks identified are, in the auditor's judgment, significant risks and, in making this judgment, the auditor is required to exclude the effects of identified controls related to the risk. The IAASB has already discussed various aspects of challenges and issues identified relating to significant risks.

Summary of IAASB Discussions to Date

63. In its discussions at its September 2016 and December 2016 meetings, the IAASB agreed with the following in relation to significant risks:

   (a) The concept of significant risk should be retained (see further discussion in paragraphs 71–75 below);

   (b) Significant risk should continue to be a subset of inherent risks (that is, the auditor's judgment as to which risks are significant risks should continue to exclude the effects of the identified controls related to the risk); however, the Task Force should consider the implications on the auditor's ability to perform a combined assessment of the risk of material misstatement as contemplated for in paragraph A42 of ISA 200 (see paragraphs 54–61);

   (c) Auditor judgment in the determination of significant risks[18] should be retained (i.e., not having the ISAs specify issues that should automatically be considered significant risks in every audit (other than what is currently in the ISAs for fraud risks related to management override of controls and revenue recognition));

   (d) The matters that are addressed in paragraph 28 of ISA 315 (Revised)[19] should be retained as these continue to remain relevant in the auditor exercising judgment as to which risks are significant risks;

[18] ISA 315 (Revised), paragraph 27

[19] Paragraph 29 of ISA 315 (Revised) sets out matters that the auditor considers when judging risks as significant risks.

(e) The definition of significant risk is circular and the Task Force should explore revising the definition to focus instead on the nature of the risk;

(f) The qualitative inherent risk factors of complexity, ambiguity, change, uncertainty and susceptibility to fraud would provide a helpful framework for the auditor's understanding and identification of inherent risks, including significant risks, and in evaluating the relative likelihood and magnitude of the risk of material misstatement;

(g) Reference to the concept of "difficult for management to control" should be considered for inclusion in application material in ISA 315 (Revised) and not within the definition or the requirements related to significant risk in the standard; and

(h) Significant risks are those inherent risks that are the *highest* on the spectrum of inherent risks.

Further Matters to Consider—From IAASB Discussions

64. At the September 2016 and December 2016 IAASB meetings, the IAASB asked the Task Force to further consider:

(a) In relation to the Task Force recommendation that the determination of significant risk should be based on the relative likelihood and magnitude of misstatement, and on the nature of the risk in the context of the qualitative inherent risk factors (i.e., a high inherent risk driven by the relative likelihood and magnitude of misstatement and one or a combination of the qualitative inherent risks factors), whether a definition of significant risk that includes these concepts would sufficiently facilitate the auditor's determination of significant risks given these concepts are relevant to the assessment of all inherent risks;

(b) Whether those inherent risks that have a low likelihood of misstatement, but if that misstatement were to occur, it would be of high magnitude in terms of its materiality, would be considered to be a significant risk;

(c) The relationship between significant classes of transactions, account balances and disclosures, and significant risks;

(d) Whether the definition should continue to make reference to "risks of material misstatement," or whether this should be changed to refer to inherent risks;

(e) How to operationalize the auditor's consideration of the qualitative inherent risk factors, and the relative likelihood and magnitude of misstatement related to the risk, when identifying significant risks; and

(f) Further consider the addition of susceptibility to fraud as a qualitative inherent risk factor as it relates to aspects of both inherent risk and control risk.

65. A description of the qualitative inherent risk factors is set out below (and is consistent with what was presented for IAASB discussion at the IAASB December 2016 meeting) for reference. The Task Force has not considered these factors further since the December 2016 meeting, but will do so in response to

the feedback received as outlined above and include updated views, in particular about the addition of the susceptibility to fraud, at a future IAASB meeting.[20]

- Complexity: that arises when there are many items or relationships among such items that require integration in applying depiction methods to determine information required by the Financial Reporting Framework (FRF) (e.g., using a complex model to determine a fair value, complex patterns of trading in financial instruments or complex supplier relationships for a retailer).
- Ambiguity: that results from a lack of clarity or a degree of vagueness in exactly what is required by the FRF, resolved by making an election or judgment about the appropriate information to include. Where the matter is more subjective, the judgment may be more susceptible to management bias.
- Change: that results in changes in the information required by the FRF from one point in time to another during or between financial reporting periods – this includes changes in the FRF or in the entity or its business model or in the environment in which the entity operates.
- Uncertainty: that arises from circumstances not within the control of the preparer of the financial information and that affect the determination of information required by the FRF and relate to the past, present or future condition of a transaction or event.
- Susceptibility to Fraud: that results from fraud risk factors and is a quality or state of being susceptible to misappropriation of the entity's assets or fraudulent financial reporting within the context of the FRF, including being susceptible to management override of control.

66. The Task Force has continued to discuss aspects related to significant risks. This paper explores the following, with the Task Force seeking IAASB input on each of these to provide direction for the way forward:

    (a) Proposed 'working definition' of significant risk based on the IAASB direction to date;

    (b) Consequences and impediments of the direction to enhance the concept of significant risk; and

    (c) Whether inherent risks that have low relative likelihood for a material misstatement to occur with high magnitude of potential misstatement should be identified as significant risks (paragraph 64(b) above).

    The other matters set out in paragraph 64 above will be discussed with the IAASB at a later meeting.

Proposed Working Definition of Significant Risks

67. As noted in paragraph 63 above, the IAASB has to date agreed on a number of matters related to significant risks. One of the reasons that the concept of significant risk is not consistently applied by auditors is related to its definition. The current definition focuses the auditor on the identification of significant risks related to the nature, timing and extent of the response rather than the nature of the risk.

[20] The Task Force is mindful that the qualitative inherent risk factors being considered as set out above are slightly different to those being considered in the proposed changes to ISA 540. The Task Force will continue to monitor the discussions with the Board on the ISA 540 proposals as relevant to determine whether (a) changes may need to be considered in ISA 315 (Revised); (b) the qualitative inherent risk factors in ISA 540 are specific to judgments and estimates and therefore having different factors is appropriate, or (c) further consideration will be needed in revised ISA 540.

68. In its ongoing deliberations regarding possible revisions in ISA 315 (Revised) related to the concept of significant risk, the Task Force has considered the development of a working definition that could help further the Task Force's, and IAASB's, thinking regarding significant risks. The Task Force is not proposing at this time for this working definition to be the revised definition of significant risks. The Task Force has merely attempted to articulate concisely an enhanced concept of significant risks, taking into account the IAASB direction to date, in order to facilitate further discussions with the IAASB regarding whether the Task Force has understood the IAASB's input provided to date related to significant risks and the potential consequences, impediments and benefits to this direction – see paragraphs 71–75).

69. Accordingly, the Task Force's proposed working definition of significant risk, taking into account the IAASB's discussions to date, is as follows:

> Significant risks are those inherent risks that the auditor determines to be the highest inherent risks. The highest inherent risks are those with both higher likelihood for material misstatement to occur and higher magnitude of potential misstatement due to their increased susceptibility to material misstatement resulting from one or more of the qualitative inherent risk factors.

70. In developing the working definition, the Task Force has referred to significant risks in the plural (the extant definition of significant risk is in the singular). Using the plural "significant risks" is similar to how key audit matters are addressed in the IAASB's New and Revised Auditor Reporting standards (i.e., key audit matters defined as plural to indicate that they are those matters that are determined to be of most significance in the audit of the financial statements) and that approach would seem to align with the thinking that significant risks are the highest inherent risks.

Matter for IAASB Consideration

4. Does the IAASB agree that the proposed 'working definition' of significant risks captures the discussions with and input from the IAASB to date?

Consequences and Impediments of the Direction to Enhance the Concept of Significant Risk

71. While the IAASB has previously agreed that the concept of significant risk be retained, recent Task Force discussions (particularly in light of the proposed working definition) have included reflecting on the consequences and impediments of retaining the concept of significant risk in order to move forward in developing changes in ISA 315 (Revised). The purpose of these further reflections is to consider whether retaining the concept of significant risk consistent with the current direction will be of benefit. That is, will it enhance audit quality and also address the issues identified in paragraphs 26 and 43–45 in the ISA 315 (Revised) Project Proposal?

72. A question that has been raised consistently both during IAASB discussions and within Task Force discussions is, regardless of the revised definition, what is it that an auditor will do differently to address significant risks in comparison to other risks of material misstatement, in particular other higher inherent risks that might not be concluded to be significant risks? Although most of the audit consequences to identifying significant risks are not within the scope of ISA 315 (Revised), the Task Force agrees that it is appropriate to validate that any revisions to the determination of significant risks in ISA 315 (Revised) will have appropriate and meaningful effects on the procedures to be performed related to these 'special' risks under other ISAs.

73. The following is a summary of the requirements in the ISAs where the concept of significant risks has consequences, and the Task Force views in relation to them assuming that the concept of significant risks is enhanced as previously described:

    (a) Paragraph 29 of ISA 315 (Revised) requires the auditor to obtain an understanding of the entity's controls, including control activities, relevant to significant risks. Paragraph 15 of ISA 330 requires that, if the auditor plans to rely on controls over a significant risk, the auditor shall test those controls in the current period. In line with the IAASB discussions related to significant risks being inherently "difficult to control", the Task Force is of the view that it would be appropriate to retain these requirements.

    (b) Paragraph 21 of ISA 330 requires the auditor to perform substantive procedures that are specifically responsive to the significant risk. With the implementation of a spectrum of inherent risk in ISA 315 (Revised) that links to paragraph 7 of ISA 330, the Task Force view is that all risks of material misstatement essentially should be subject to substantive procedures that are appropriately responsive. Furthermore, as noted in prior IAASB discussions, there often is not something unique that is performed for significant risks that would not have been performed if the risk had been not designated as "significant." This is a similar challenge to what the ISA 540[21] Task Force encountered regarding what specific additional procedures might be required for accounting estimates that give rise to significant risks. In those deliberations, the conclusion reached was that it was not so much about the type or nature of the procedure to be performed in response to a significant risk, but rather the extent and timing of the procedure, who performed the procedure, who reviewed the work performed and the persuasiveness of the evidence obtained.

    (c) Paragraph 21 of ISA 330 also requires that, when the approach to a significant risk consists only of substantive procedures, those procedures shall include tests of details. The Task Force view is that more persuasive audit evidence should be obtained for significant risks – requiring tests of details may be one method to achieve that. However, this requirement likely needs further consideration, including in conjunction with ISA 540 as it relates to auditing accounting estimates that are significant risks and the effects of data analytics on the audit.

    (d) Paragraph 8(c) of ISA 230 requires audit documentation specific to significant matters arising during the audit. A significant risk is specified to be a significant matter in paragraph A8 of ISA 230. Paragraph 19 of ISA 220 requires the engagement partner to discuss significant matters with the engagement quality control reviewer. The Task Force views these requirements to be appropriate in relation to significant risks, but not at the expense of appropriate levels of documentation and review for other areas of higher risks of material misstatement.

    (e) In the new and revised Auditor Reporting Standards, identification of significant risks resulted in:

        (i) ISA 260 (Revised)[22] requiring the auditor to communicate significant risks, identified by the auditor, to those charged with governance. The Task Force is of the view that this communication to those charged with governance should be beneficial to the quality of the discussions between the auditor and those charged with governance.

---

21 ISA 540, *Auditing Accounting Estimates, Including Fair Value Accounting Estimates, and Related Disclosures*

22 ISA 260 (Revised), *Communication with Those Charged with Governance,* paragraphs 15 and A12–A13

(ii) In accordance with paragraph 9 of ISA 701,[23] the auditor is required to determine, from the matters communicated with those charged with governance, those matters that required significant auditor attention in performing the audit. In making this determination, the auditor is required to take into account (among other items) areas of higher assessed risk of material misstatement, or significant risks identified in accordance with ISA 315 (Revised). The Task Force view is that communication of significant risks within the auditor's reports when determined to be key audit matters in accordance with ISA 701 is a recent consequence for significant risks that needs to be specifically considered. The Task Force will liaise on an ongoing basis with the IAASB's Auditor Reporting Implementation Working Group to understand any feedback specific to the relationship between significant risks and key audit matters.

74. The Task Force has identified the following impediments should the concept of significant risk be retained in line with the current direction:

- In the context of the proposed spectrum of inherent risks in ISA 315 (Revised), as previously discussed with the IAASB, significant risks will be those inherent risks that are at the highest end of the spectrum of inherent risks, effectively requiring a threshold that will need to be defined. The Task Force is of the view that defining that threshold will be challenging (consistent with the challenges the ISA 540 Task Force has had with defining lower risk in relation to the audit of accounting estimates and related disclosures).
- The Task Force is of the view that significant auditor judgment will continue to be required when identifying significant risks. This judgment will arise from the determination of the influences of the qualitative inherent risk factors and that a new definition is not going to remove the need for auditor judgment, which means the risk of inconsistent application will not be completely mitigated.
- By continuing to stress the importance of the identification of significant risks, this may continue to have unintended consequences for some audits, such that other risks of material misstatement not receiving an appropriate amount of auditor focus or attention.
- In revising the definition of significant risk, it may be difficult to revise the definition to adequately capture the appropriate consideration of fraud risks, i.e., will moving toward a more precise definition of significant risk result in the ability of the nature of fraud risks to be captured by that definition? The Task Force needs to further discuss and develop its thinking in this area but is of the view that capturing fraud risks in a revised definition will be challenging (e.g., are fraud risks higher in likelihood, particularly in all cases).

75. The Task Force is of the view that, in order to continue progressing the revised concept of significant risks, the consequences of the determination of significant risks for the audit (described in paragraph 73 or other consequences that the IAASB believes should be considered by the Task Force) need to be viewed by the IAASB as benefits and those benefits need to be viewed as being great enough to overcome the impediments (as outlined above or others that the IAASB may identify). The Task Force seeks further direction from the IAASB regarding the next steps that the Task Force should consider in progressing revisions to the concept of significant risk.

[23] ISA 701, *Communicating Key Audit Matters in the Independent Auditor's Report*

Matters for IAASB Consideration

5. With input from discussions on significant risk at three IAASB meetings, the Task Force is seeking IAASB input on the appropriate way forward with respect to significant risks:

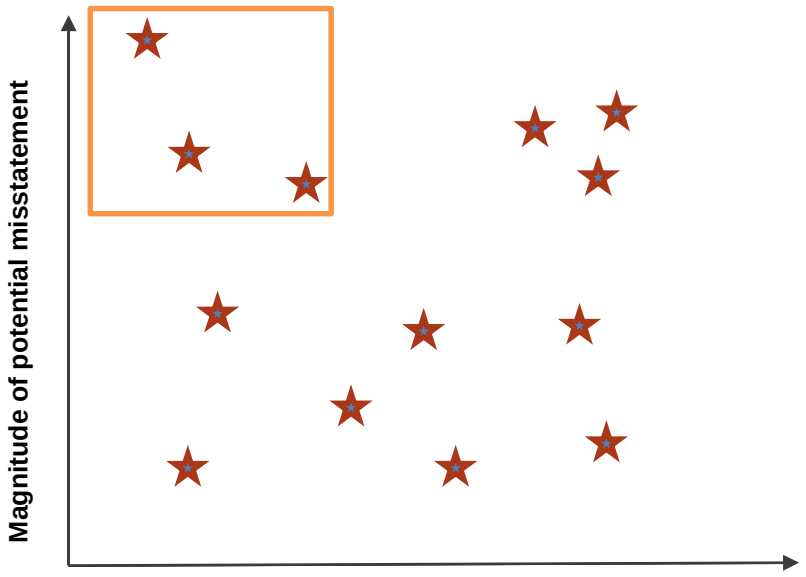
   (a) In the context of the consequences and impediments identified by the Task Force in paragraphs 73–74 above, are there other consequences, impediments or benefits not considered by the Task Force if the concept of significant risks is to be retained?

   (b) Should the Task Force continue in the current direction, progressing with revising the requirements and the definition of significant risks taking into account the input to date from the IAASB, or does the Board recommend consideration for a change in direction on significant risks (e.g., abandon the concept of significant risks, revise requirements etc.)?

Inherent Risks–Low Likelihood for a Material Misstatement to Occur with High Magnitude of Potential Misstatement

76. As noted, the introduction of the concept of a spectrum of inherent risk into ISA 315 (Revised) was supported by the IAASB. The Task Force is of the view that all inherent risks can be visualized on a spectrum of inherent risk such as illustrated below.

77. To respond to IAASB feedback from the December 2016 meeting, the Task Force has further considered whether those inherent risks that are identified as having a low likelihood for a material misstatement to occur, but a high magnitude of potential misstatement should be identified as significant risks (the inherent risks in question being illustrated, for example, in the orange box in the diagram depicting the spectrum of inherent risks).



78. All risks above an acceptably low level, including those risks that have low likelihood for a material misstatement to occur and high magnitude of potential misstatement, require an appropriate response to the assessed risk, with the auditor needing to understand the reasons for the assessed risk of material misstatement in order to design further audit procedures. The Task Force view is that this understanding

would be enhanced as a result of the proposed inclusion of a spectrum of inherent risk in ISA 315 (Revised) and therefore may improve the auditor's responses to all assessed risks of material misstatement at the assertion level.

79. In developing the working definition of significant risks (see paragraphs 67–70 above), it is noted that the Task Force continues to be of the view that only those inherent risks that the auditor considers to be of high likelihood for a material misstatement to occur, and high magnitude of potential misstatement should be identified as significant risks, such that only the highest risks would have specific audit consequences. As a consequence, the Task Force is of the view that those inherent risks with a low likelihood for potential misstatement to occur but a high magnitude of potential misstatement would not be considered a significant risk.

Matter for IAASB Consideration

6. Does the IAASB agree that that those inherent risks with a low likelihood for potential misstatement to occur but a high magnitude of potential misstatement should not be considered a significant risk should the concept be retained?

VI. Data Analytics

80. The Task Force notes that ISA 315 (Revised) does not explicitly preclude nor specifically encourage the use of data analytics by the auditor when performing risk assessment procedures. This is an area where practice is rapidly evolving, and the Task Force is mindful that consideration about the impact of data analytics needs to be taken into account as changes to ISA 315 (Revised) are explored.

81. As noted in the Project Proposal, the Task Force, with input from the DAWG, is exploring the impact of using data analytics when gaining the understanding of the entity and its environment in identifying and assessing the risks of material misstatement as required by ISA 315 (Revised).

Input from the Data Analytics Working Group

82. The DAWG provided the Task Force with its initial views on considerations about how data analytics may be used to support the auditor's risk assessment procedures (including in identifying and assessing risks of material misstatement), and where changes to ISA 315 (Revised) could be considered. The DAWG will continue to consider appropriate responses in light of the input from the comment letters received to the Request for Input, *Exploring the Growing Use of Technology in the Audit, with a Focus on Data Analytics*. Accordingly, the DAWG may make additional recommendations for the Task Force's further consideration regarding potential enhancements to ISA 315 (Revised).

83. The input to the Task Force from the DAWG included the following DAWG views on how:

- The use of data analytics in the risk assessment process may enhance the quality of some risk identification and assessment procedures, including describing the anticipated benefits of using data analytics (e.g., a more fulsome analysis of the data than would occur using manual techniques or improved mechanisms for understanding flows of transactions, including identifying alternative paths for transactions).
- Data analytics can be used to analyze data to assist in undertaking risk identification and assessment procedures (e.g., analytical procedures using visualizations, reperformance and recalculation of routines on data obtained from the entity and predictive modelling techniques).

- It may be difficult to distinguish risk assessment procedures using data analytics from performing procedures to respond to identified risks (i.e., further audit procedures) because of the way procedures are performed when using data analytics (because, for example, different procedures may be performed at the same time).
- Issues and challenges relating to how procedures using data analytics are documented.

84. The DAWG recommended that the Task Force give further consideration to enhancing ISA 315 (Revised) to:

    (a) Refer to the ability to use data analytics when describing the types of procedures that could be used to perform risk assessment procedures;[24]

    (b) Better describe how risk assessment procedures using data analytics can be distinguished from procedures to respond to identified risks of material misstatement so that the appropriate work effort is carried out at each stage; and

    (c) Address the appropriate documentation of risk assessment procedures performed using data analytics.

85. The Task Force, from its initial consideration of the matters highlighted by the DAWG and subject to further discussion and coordination with the DAWG, agreed in principle that consideration should be given to changes in ISA 315 (Revised) to more directly address the ability of the auditor to make use of data analytics when performing risk assessment procedures.

86. The Task Force's initial view, without pre-judging further information that may be obtained from the DAWG, including based on analysis of responses to the Request for Input, is that no changes to the requirements in ISA 315 (Revised) in relation to performing risk assessment procedures using data analytics are considered necessary. The Task Force, with the exception of one member who is of the view that further consideration of the underlying issues is needed before any decisions are made about how what is known as data analytics can be addressed in the ISAs, including in ISA 315 (Revised), did agree that additional application material would be helpful, including as follows:

    - Examples of how to perform risk assessment procedures using data analytics in the application material (e.g., including the application material to paragraph 6 of ISA 315 (Revised) that describes the various types of risk assessment procedures). These examples could include describing typical uses of data analytics, but could also highlight the anticipated benefits of using data analytics over more traditional techniques.
    - Describing how data analytics may be used to understand the flow of transactions and trace transactions through the information system, and also to aid in evaluating the design of controls and determining whether they have been implemented.
    - Emphasize the importance of evaluating whether the data being used is sufficiently reliable for the auditor's purpose (i.e., risk assessment procedures). This may include providing examples of how the auditor might obtain evidence about the completeness and accuracy of the information and how the auditor might evaluate whether the data is sufficiently precise and detailed for the purpose of the auditor's risk assessment procedures.

[24] Paragraph 6 of ISA 315 (Revised) describes risk assessment procedures as including inquiries, analytical procedures, observation and inspection.

- Describing how risk assessment procedures using data analytics could be documented (including matters such as the information used and the results of the analysis performed for risk assessment purposes).
- Providing guidance to help auditors distinguish between risk assessment procedures and further audit procedures when data analytics techniques are applied to the same data set for both purposes, including to:
    - Appropriately document the procedures performed (e.g., how the documentation requirements of ISA 315 (Revised) may be achieved when iterative data analytic techniques are used that involve performing risk assessment procedures and procedures to respond to identified risks of material misstatement concurrently).
    - Determine the appropriate work effort for evaluating whether the data being used is sufficiently reliable for the auditor's purpose (e.g., testing completeness and accuracy) when data analytics are applied to the same data set for both risk assessment purposes and for the purposes of responding to the identified risks of material misstatement.

87. In addition, the DAWG recommended that consideration should be given to developing a "definition" of data analytics for inclusion in the ISAs, noting that this definition would help auditors understand what is meant by using "data analytics" as there are likely varying interpretations about what this term may mean. The Task Force agreed that it would not be appropriate to create a definition of data analytics in isolation in the context of risk assessment procedures. However, an explanation of how the use of data analytics relates to the current terminology in the ISAs related to audit procedures may be helpful.

88. The topic of data analytics has broader implications to the entire audit process, and in particular to audit evidence. The Task Force has the view that further consideration should be given to whether the term "data analytics" is truly representative of the broad range of techniques it is intended to capture and accordingly, whether it may be more appropriate to describe the techniques more precisely and in the context of individual ISAs, or whether this approach should be used in addition to, or instead of, using a defined term. The Task Force notes that such further consideration can be given as this topic is further explored by other IAASB working groups and task forces (including through the DAWG and also by the group that will be assigned to work on the audit evidence project once that project commences). However, regardless of the approach taken to the definition, the Task Force has the view that including examples of using data analytics for risk assessment procedures in the application material of ISA 315 (Revised) as described above, will assist auditors in better understanding how data analytics might be useful in performing risk assessment procedures and may encourage auditors to further consider how and whether using such tools may be beneficial and appropriate.

89. Other matters highlighted by the DAWG, not specifically related to ISA 315 (Revised), included using data analytics to test journal entries, test the operating effectiveness of controls, and to test complete populations of data. The Task Force will share its views on these other matters as relevant with other IAASB task forces and working groups. The Task Force will continue to liaise with the DAWG as it further develops the amendments to ISA 315 (Revised).

Matter for IAASB Consideration

7. The IAASB is asked for its views on:

   (a) The proposed approach to considering possible changes to ISA 315 (Revised) relating to data analytics, specifically the Task Force's initial view that no changes are necessary to the requirements; and

   (b) Whether there are specific areas where changes need to be considered with regard to the auditor's risk assessment procedures in addition to those noted in paragraphs 86–88 above.

VII. Professional Skepticism

Input from the Professional Skepticism Working Group

84. The Task Force discussed its initial thinking on the topic of professional skepticism and ISA 315 (Revised) at its December 2016 Task Force meeting. A key input in the Task Force's considerations was the matrix prepared by the PSWG that was discussed by the IAASB at its June 2016 meeting (Agenda Item 2-B of the June 2016 IAASB meeting, referred to hereafter as the PSWG Matrix).

Summary of PSWG's June 2016 Discussions with the IAASB

90. The Board agreed that the exercise of professional skepticism when identifying and assessing risks is critical, given the impact the auditor's identification and assessment of the risks of material misstatement has on the audit.

91. The PSWG noted that the responses to the IAASB's Invitation to Comment, *Enhancing Audit Quality: A Focus on Professional Skepticism, Quality Control and Group Audits*, highlighted that the ability to effectively exercise professional skepticism is premised upon an appropriate understanding of the entity's business model and related drivers, which assists the auditor in effectively identifying risks of material misstatement.

92. It was highlighted that the engagement team discussion, required by paragraph 10 of ISA 315 (Revised), regarding the susceptibility of the entity's financial statements to material misstatement and the application of the applicable financial reporting framework to the entity's facts and circumstances, is one of the important communications that occurs during the audit between the engagement partner and the engagement team. A lack of appropriate application of professional skepticism during the engagement team discussion may affect the auditor's ability to identify and consider inconsistencies in information obtained while performing risk assessment procedures, as well as the auditor not being appropriately alert for indicators of possible management bias (both intentional and unintentional) when discussing the susceptibility of the entity's financial statements to material misstatement. In both cases, this may lead to improper, incomplete or inaccurate identification and assessment of the risks of material misstatement. In the Board's view, emphasizing the exercise of professional skepticism during the discussion among the engagement team members, including the engagement partner, when performing risk assessment procedures may therefore help mitigate the potential for that outcome.

93. Paragraph 11 of ISA 315 (Revised) sets out matters related to the entity and its environment of which the auditor is required to obtain an understanding. In obtaining this understanding, the auditor is expected to apply professional skepticism in considering the consistency of information gathered or obtained with

other known information and in deciding whether the auditor's understanding is sufficient for the purposes of identifying and assessing the risks of material misstatement. Unresolved inconsistencies in information may indicate either that the auditor has not exercised appropriate professional skepticism in evaluating the information obtained in performing the risk assessment procedures, or in determining whether the information obtained may not be sufficiently reliable for the auditor's purposes.

94. Accordingly, the PSWG suggested that the following approaches may be effective in facilitating the appropriate application of professional skepticism in the performance of risk assessment procedures:

- Strengthening paragraph 10 of ISA 315 (Revised) to reinforce the importance of the exercise of professional skepticism during the engagement team discussion and to remind all engagement team members about the importance of exercising professional skepticism throughout the audit.
- Providing further guidance to paragraph 10 of ISA 315 (Revised) about matters that may be discussed to help encourage the exercise of professional skepticism during the engagement team discussion, such as identifying inconsistent or contradictory information gathered during the risk assessment procedures.
- Restructuring paragraph 11 of ISA 315 (Revised) to promote a greater understanding of the business model when understanding the entity and its environment. The suggested restructuring would result in the auditor being required to first obtain an understanding of the entity's business model, objectives, and strategies,[25] and then to explicitly consider whether that understanding is consistent with the information and further understanding obtained in addressing the remaining matters within paragraph 11 of ISA 315 (Revised).
- Requiring the auditor to remain alert to potential management bias (including indicators of management bias) throughout the risk assessment process and not just related to the risk assessment process for specific areas (e.g., accounting estimates under ISA 540).
- Documentation requirements that:
  - Explicitly require the auditor to consider the nature of the different types of evidence obtained through performing risk assessment procedures and which forms the basis for the auditor's understanding of the entity and its environment.
  - Demonstrate how inconsistent evidence gathered during risk assessment procedures has been dealt with.
  - Demonstrate how potential management bias has been considered and dealt with in planning the engagement.

Risk Assessment and Professional Skepticism in the IAASB's Extant Standards

95. The exercise of professional skepticism by the auditor in performing risk assessment procedures during the audit is currently addressed in ISA 315 (Revised) and other related IAASB standards in the following ways:

(a) Two references in ISA 315 (Revised) to the exercise of professional skepticism, being in:

(i) Paragraph A120 of ISA 315 (Revised) in the context of the auditor obtaining an understanding of the monitoring of controls component of internal control, specifically

[25] ISA 315 (Revised), paragraph 11(d)

how communication with the internal audit function (when the entity has such a function) may result in information being brought to the auditor's attention that brings into question the reliability of documents and responses to inquiries to be used as audit evidence; and

(ii) Paragraph A132 of ISA 315 (Revised) in the context of identifying the risks of material misstatement in the financial statements, it is noted that the auditor exercises professional skepticism in accordance with ISA 200.[26, 27]

(b) The Professional Skepticism Staff Q&A makes reference to professional skepticism in the following ways as it relates to risk assessment:

(i) It would be an ideal opportunity to discuss professional skepticism during the discussion among the engagement team regarding the susceptibility of the financial statements to material misstatement as required by paragraph 10 of ISA 315 (Revised).

(ii) Professional skepticism is relevant and necessary throughout the audit, in particular in the revision of risk assessment required by paragraph 31 of ISA 315 (Revised).

(c) Other standards and guidance that provide for the exercise of professional skepticism when identifying circumstances or conditions that increase risks of material misstatement include:

(i) Paragraphs 12–14 of ISA 240[28] make reference to the requirement in ISA 200 for the auditor to maintain professional skepticism throughout the audit, recognizing that the possibility of material misstatement due to fraud could exist. In addition, it is noted that unless the auditor has reason to believe to the contrary, the auditor may accept records and documents as genuine. However if the auditor identifies conditions during the audit to cause the auditor to believe the documents are not authentic or have been modified, the auditor shall investigate further. It also add that the auditor shall also investigate further if inquiries of management or those charged with governance appear inconsistent.

(ii) Paragraph A40 of ISA 540, reference is made to professional skepticism related to the review of prior period accounting estimates and emphasizes that the exercise of professional skepticism assists the auditor in identifying circumstances or conditions that increase the susceptibility in the current year of accounting estimates to, or indicate the presence of, possible management bias and in determining the nature, timing and extent of audit procedures. The review of prior period accounting estimates, however, may only be one indicator of management bias.[29]

(iii) Paragraph 71 of IAPN 1000[30] that notes that professional skepticism is necessary to the critical assessment of audit evidence and assists the auditor in remaining alert for possible indications of management bias. Paragraph 113 of IAPN 1000 explicitly

---

[26] ISA 200, paragraph 15

[27] This was an addition to paragraph A132 of ISA 315 (Revised) that arose from the Disclosures Project.

[28] ISA 240, *The Auditor`s Responsibilities Relating to Fraud in an Audit of Financial Statements*

[29] Further changes have been made to encourage the auditor's exercise of professional skepticism when auditing accounting estimates in the proposed revised ISA 540 (see Agenda Item 2).

[30] International Auditing Practice Note (IAPN) 1000, *Special Considerations in Auditing Financial Instruments*

addresses intentional and unintentional management bias and provides examples of what the auditor can look for to determine whether management may be biased.

Task Force Views Regarding Risk Assessment and Professional Skepticism

Overall Task Force View

96. The Task Force is of the view that while it is good and helpful to remind auditors to exercise appropriate professional skepticism, simply increasing references to the application of professional skepticism throughout ISA 315 (Revised) will not result in the desired extent of change in auditor behavior regarding the exercise of professional skepticism in performing risk assessment procedures. In considering the appropriate approach to take to enhance ISA 315 (Revised) to drive the appropriate exercise of professional skepticism when performing risk assessment procedures, the Task Force considered the following options:

    (a) Drafting requirements, similar to the approach that is taken in paragraphs 12–14 of ISA 240, that would explain what an auditor who exercises appropriate professional skepticism would be expected to do in identifying and assessing risks of material misstatement with a view to drive changes in behavior (i.e., require behavior or responses that would be expected to enhance the auditor's application of professional skepticism).

    (b) Considering how the requirements are structured to encourage a more challenging approach to audit evidence (as opposed to requirements that drive the need for more corroborative evidence).

    (c) Emphasizing the importance of exercising professional skepticism during the auditor's performance of risk assessment procedures by providing examples or illustrations of actions in the context of the requirements that the auditor may take to achieve the appropriate application of professional skepticism.

97. In progressing revisions to ISA 315 (Revised), the Task Force continues to be of the view (similar to the approach taken in other IAASB projects) that facilitating and promoting the appropriate exercise of professional skepticism through consideration about how the requirements are drafted (as noted in paragraph 96(b) above) and through examples in the application material to illustrate the principles in the requirements (as noted in paragraph 96(c) above) is the preferred approach. Drafting requirements similar to the approach taken in ISA 240 might require too much specificity for the engagement team discussion, and may not result in the desired change in behavior.

98. Accordingly, the Task Force intends to pursue possible changes to ISA 315 (Revised) in relation to the requirements (and related application material) that address the engagement team discussion, the auditor's sources of information for the understanding the entity and its environment, and the auditor's use of qualitative inherent risk factors, each of which is expanded on in the following sections.

99. The Task Force will continue to work with the IAASB PSWG as it continues to consider changes to ISA 315 (Revised).

Engagement Team Discussion–Susceptibility of Financial Statements to Material Misstatement

100. Similar to the views expressed by the PSWG, the Task Force is of the view that the extant requirement in paragraph 10 of ISA 315 (Revised) to conduct the required discussion between the engagement partner

and other key members of the engagement team is key to the exercise of professional skepticism as part of the auditor's risk assessment.

101. The Task Force is of the view that there is scope for improvement in the application material associated with the extant requirement in paragraph 10 of ISA 315 (Revised), with regard to how to promote behavior that reflects the appropriate exercise of professional skepticism by all engagement team members at the engagement team discussion, and which would help encourage a more effective discussion and improved identification of risks of material misstatement. This could include examples of matters for consideration by the engagement team about:

    (a) Threats to the appropriate exercise of professional skepticism, such as dominance of the discussion by the engagement partner and other key engagement team members who may be very familiar with the client, and who may not therefore encourage or facilitate appropriate professional skepticism from others during the engagement team discussion. Responses to those threats may include, for example, having an appropriately experienced and qualified individual (who has had little to no prior experience with the audit of the entity)[31] attend the engagement team discussion to help address familiarity concerns by challenging the more experienced members of the engagement team. The Task Force noted that this approach may be more effective than brainstorming driven primarily by the engagement partner and other senior members of the engagement team. Another alternative could involve an additional separate team discussion without the engagement partner and other key members of the engagement team so as to not have the views of the more senior members of the team cloud or bias those of others.

    (b) Whether potential risks of material misstatement have also been discussed by the entity.

    (c) Matters that could be discussed to promote behavior that reflects the appropriate exercise of professional skepticism, such as:

        - Has the auditor learned enough about the business and its risks and do the various aspects of what the auditor has learned align with each other?
        - Having identified risks of material misstatement, is the auditor too ready to accept those risks as lower than they actually are?
        - Considering whether sensitivity analysis or stress testing (i.e., considering the impact on the risk assessment of changes in risk factors, including those that could affect the assessment significantly and less significantly) or reverse stress testing (i.e., 'anchoring' to the hypothesis that the risk has materialized and considering what combination of factors would need to occur to give rise to that outcome), would provide appropriate context.
        - Whether sufficient information has been obtained to support the risk assessment in the current year, in particular in recurring engagements where it may just be assumed that the risks in the current year are the same as the previous year.

[31] Intended to be a person other than the Engagement Quality Control Reviewer.

Source of Auditor's Information in Carrying Out Risk Assessment Procedures

102. In obtaining an understanding of the entity and its environment, as required by paragraph 11 of ISA 315 (Revised), the Task Force is of the view that the entity (or its management) should not be the auditor's sole source of information about the entity and its environment. Further, the Task Force is of the view that the auditor should not "filter" information obtained from sources outside the entity based solely on management's views of its relevance.

103. In the first instance, it will likely be helpful for the auditor to determine whether management has identified the possible risks of material misstatement, and if not, the reasons for not identifying them (being mindful that the auditor does not have, and is not required to have, the same depth of knowledge about the entity and its environment as management, and the auditor may identify risks or have views about them that differ from management). The auditor would also look to other sources when performing risk assessment procedures, with the Task Force having the view that this should be further emphasized in the standard. The following sets out matters that could be included as application material in ISA 315 (Revised) to emphasize that the auditor should not only consider management as its sole source of information, and what some of the other sources of information for the auditor could be:

- Examples of sources that provide information about the entity's industry (e.g., industry journals), general business and market conditions (e.g., financial press), implications of changes to the applicable financial reporting framework (e.g., releases from national standard setters or accounting member body organizations), or views about the entity (e.g., from analysts).
- Using data analytics to analyze the entity's data, which may in turn reveal information not disclosed to the auditor by management that is relevant to the auditor's understanding of the entity and its environment, including the entity's internal control.
- Highlighting that multiple sources of information may also assist the auditor in evaluating the potential for management bias, which will further inform the auditor's risk assessment.

Qualitative Inherent Risk Factors

104. The Task Force has discussed the use of qualitative inherent risk factors (see paragraph 65 in **Section V** of this paper) in the auditor's identification of inherent risks and the auditor's identification of significant risks. The Task Force is of the view that the qualitative inherent risk factors would provide a useful reference for the auditor to consider and to provide context for what has been learned from the auditor's risk assessment procedures and facilitate the exercise of professional skepticism, in particular helping the auditor to apply a challenging mindset.

105. The consideration of the qualitative inherent risk factors could aid the auditor in exercising professional skepticism by giving the auditor an objective set of criteria to consider when evaluating the information the auditor has obtained from performing their risk assessment procedures. For example, the auditor could ask themselves whether they have appropriately exercised professional skepticism when considering the impact of complexity on the susceptibility to misstatement. While the qualitative inherent risk factors are listed in paragraph 65 above separately, there may be an element of overlap between some of the factors (e.g., the susceptibility to fraud almost always exists in conjunction with one or more of the other qualitative inherent risk factors and therefore consideration of these factors together may assist the auditor in a more thorough identification of risks).

Documentation

106. The Task Force's objective in considering documentation aspects is to encourage better auditor behavior by having the auditor explain the auditor's thought process and the trail of logic that was followed in making judgements and exercising professional skepticism, and thereby enable the auditor to better demonstrate the exercise of professional skepticism when performing risk assessment procedures.

107. While the Task Force has not reached any conclusions as yet related to documentation, it is of the initial view that the auditor's documentation of the risk assessment process will assist the auditor in evidencing the exercise of professional skepticism (i.e., when the thinking behind the auditor's risk assessment is documented appropriately, the documentation has the ability to evidence the appropriate behavior related to the exercise of professional skepticism). This may include encouraging documentation of the matters the auditor has considered throughout the performance of their risk assessment procedures and creating better linkages between that information and judgments the auditor made in factoring that information into the auditor's risk assessment.

Matter for Board Consideration

8. The IAASB is asked for its views on the matters set out in paragraphs 96–107 above.

VIII. Way Forward

108. The Task Force will continue to work through those aspects of ISA 315 (Revised) that need further consideration that have not yet been discussed with the Board, as well as those aspects where Board feedback has been obtained but where further reflection is needed. The Task Force intends to present a complete depiction of the possible changes to ISA 315 (Revised) identified to date later in 2017.

109. As the Task Force continues exploring possible changes to ISA 315 (Revised), including how to address challenges in applying the standard in a wide variety of circumstances (e.g., how to effectively apply the standard in non-complex entities), further consideration will also be given to how the standard is structured, in particular the section on internal controls.

Appendix I

Extracts of relevant ISA references noted throughput the paper (except those from ISA 315 (Revised), which can be found in the Supplement to Agenda Item 4)

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

Requirements

Professional Skepticism

15. The auditor shall plan and perform an audit with professional skepticism recognizing that circumstances may exist that cause the financial statements to be materially misstated. (Ref: Para. A20–A24)

Application and Other Explanatory Material

Risk of Material Misstatement

A42. The ISAs do not ordinarily refer to inherent risk and control risk separately, but rather to a combined assessment of the "risks of material misstatement." However, the auditor may make separate or combined assessments of inherent and control risk depending on preferred audit techniques or methodologies and practical considerations. The assessment of the risks of material misstatement may be expressed in quantitative terms, such as in percentages, or in non-quantitative terms. In any case, the need for the auditor to make appropriate risk assessments is more important than the different approaches by which they may be made.

A43. ISA 315 (Revised) establishes requirements and provides guidance on identifying and assessing the risks of material misstatement at the financial statement and assertion levels.

ISA 220, Quality Control for an Audit of Financial Statements

Requirements

Engagement Quality Control Reviewer

19. For audits of financial statements of listed entities, and those other audit engagements, if any, for which the firm has determined that an engagement quality control review is required, the engagement partner shall:

    (a) Determine that an engagement quality control reviewer has been appointed;

    (b) Discuss significant matters arising during the audit engagement, including those identified during the engagement quality control review, with the engagement quality control reviewer; and

    (c) Not date the auditor's report until the completion of the engagement quality control review. (Ref: Para. A23–A25)

ISA 230, Audit Documentation

Requirements

Form, Content and Extent of Audit Documentation

8. The auditor shall prepare audit documentation that is sufficient to enable an experienced auditor, having no previous connection with the audit, to understand: (Ref: Para. A2–A5, A16–A17)

   (a) The nature, timing and extent of the audit procedures performed to comply with the ISAs and applicable legal and regulatory requirements; (Ref: Para. A6–A7)

   (b) The results of the audit procedures performed, and the audit evidence obtained; and

   (c) Significant matters arising during the audit, the conclusions reached thereon, and significant professional judgments made in reaching those conclusions. (Ref: Para. A8–A11)

Application and Other Explanatory Material

Documentation of Significant Matters and Related Significant Professional Judgments (Ref: Para. 8(c))

A8. Judging the significance of a matter requires an objective analysis of the facts and circumstances. Examples of significant matters include:

- Matters that give rise to significant risks (as defined in ISA 315 (Revised)).
- Results of audit procedures indicating (a) that the financial statements could be materially misstated, or (b) a need to revise the auditor's previous assessment of the risks of material misstatement and the auditor's responses to those risks.
- Circumstances that cause the auditor significant difficulty in applying necessary audit procedures.
- Findings that could result in a modification to the audit opinion or the inclusion of an Emphasis of Matter paragraph in the auditor's report.

ISA 240, The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements

Requirements

Professional Skepticism

12 In accordance with ISA 200[32], the auditor shall maintain professional skepticism throughout the audit, recognizing the possibility that a material misstatement due to fraud could exist, notwithstanding the auditor's past experience of the honesty and integrity of the entity's management and those charged with governance. (Ref: Para. A7–A8)

13. Unless the auditor has reason to believe the contrary, the auditor may accept records and documents as genuine. If conditions identified during the audit cause the auditor to believe that a document may not be authentic or that terms in a document have been modified but not disclosed to the auditor, the auditor shall investigate further. (Ref: Para. A9)

14. Where responses to inquiries of management or those charged with governance are inconsistent, the auditor shall investigate the inconsistencies.

[32] ISA 200, paragraph 15

ISA 260, Communication with Those Charged with Governance

Requirements

Planned Scope and Timing of the Audit

15. The auditor shall communicate with those charged with governance an overview of the planned scope and timing of the audit, which includes communicating about the significant risks identified by the auditor. (Ref: Para. A11–A16)

Application and Other Explanatory Material

Planned Scope and Timing of the Audit (Ref: Para. 15)

A12. Communicating significant risks identified by the auditor helps those charged with governance understand those matters and why they require special audit consideration. The communication about significant risks may assist those charged with governance in fulfilling their responsibility to oversee the financial reporting process.

A13. Matters communicated may include:

- How the auditor plans to address the significant risks of material misstatement, whether due to fraud or error.
- How the auditor plans to address areas of higher assessed risks of material misstatement.
- The auditor's approach to internal control relevant to the audit.
- The application of the concept of materiality in the context of an audit.[33]
- The nature and extent of specialized skill or knowledge needed to perform the planned audit procedures or evaluate the audit results, including the use of an auditor's expert.[34]
- When ISA 701 applies, the auditor's preliminary views about matters that may be areas of significant auditor attention in the audit and therefore may be key audit matters.
- The auditor's planned approach to addressing the implications on the individual statements and the disclosures of any significant changes within the applicable financial reporting framework or in the entity's environment, financial condition or activities.

ISA 330, The Auditor's Responses to Assessed Risks

Requirements

Audit Procedures Responsive to the Assessed Risks of Material Misstatement at the Assertion Level

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

   (a) Consider the reasons for the assessment given to the risk of material misstatement at the assertion level for each class of transactions, account balance, and disclosure, including:

33 ISA 320, *Materiality in Planning and Performing an Audit*

34 See ISA 620, *Using the Work of an Auditor's Expert.*

(i) The likelihood of material misstatement due to the particular characteristics of the relevant class of transactions, account balance, or disclosure (that is, the inherent risk); and

(ii) Whether the risk assessment takes account of relevant controls (that is, the control risk), thereby requiring the auditor to obtain audit evidence to determine whether the controls are operating effectively (that is, the auditor intends to rely on the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures); and (Ref: Para. A9–A18)

(b) Obtain more persuasive audit evidence the higher the auditor's assessment of risk. (Ref: Para. A19)

Controls over significant risks

15. If the auditor plans to rely on controls over a risk the auditor has determined to be a significant risk, the auditor shall test those controls in the current period.

Substantive Procedures Responsive to Significant Risks

21. If the auditor has determined that an assessed risk of material misstatement at the assertion level is a significant risk, the auditor shall perform substantive procedures that are specifically responsive to that risk. When the approach to a significant risk consists only of substantive procedures, those procedures shall include tests of details. (Ref: Para. A53)

ISA 540, Auditing Accounting Estimates, Including Fair Value Accounting Estimates, and Related Disclosures

Application and Other Explanatory Material

Reviewing Prior Period Accounting Estimates (Ref: Para. 9)

A40. The review of prior period accounting estimates may also assist the auditor, in the current period, in identifying circumstances or conditions that increase the susceptibility of accounting estimates to, or indicate the presence of, possible management bias. The auditor's professional skepticism assists in identifying such circumstances or conditions and in determining the nature, timing and extent of further audit procedures.

ISA 701, Communicating Key Audit Matters in the Independent Auditor's Report

Requirements

Determining Key Audit Matters

9. The auditor shall determine, from the matters communicated with those charged with governance, those matters that required significant auditor attention in performing the audit. In making this determination, the auditor shall take into account the following: (Ref: Para. A9–A18)

(a) Areas of higher assessed risk of material misstatement, or significant risks identified in accordance with ISA 315 (Revised). (Ref: Para. A19–A22)

(b) Significant auditor judgments relating to areas in the financial statements that involved significant management judgment, including accounting estimates that have been identified as having high estimation uncertainty. (Ref: Para. A23–A24)

(c) The effect on the audit of significant events or transactions that occurred during the period. (Ref: Para. A25–A26)

IAPN 1000, Special Considerations in Auditing Financial Instruments

Professional Skepticism

71. Professional skepticism is necessary to the critical assessment of audit evidence and assists the auditor in remaining alert for possible indications of management bias. This includes questioning contradictory audit evidence and the reliability of documents, responses to inquiries and other information obtained from management and those charged with governance. It also includes being alert to conditions that may indicate possible misstatement due to error or fraud and considering the sufficiency and appropriateness of audit evidence obtained in light of the circumstances.

Assessing the Risk of Material Misstatement Related to Valuation

113. The susceptibility to management bias, whether intentional or unintentional, increases with the subjectivity of the valuation and the degree of measurement uncertainty. For example, management may tend to ignore observable marketplace assumptions or data and instead use their own internally-developed model if the model yields more favorable results. Even without fraudulent intent, there may be a natural temptation to bias judgments towards the most favorable end of what may be a wide spectrum, rather than the point in the spectrum that might be considered to be most consistent with the applicable financial reporting framework. Changing the valuation technique from period to period without a clear and appropriate reason for doing so may also be an indicator of management bias. Although some form of management bias is inherent in subjective decisions relating to the valuation of financial instruments, when there is intention to mislead, management bias is fraudulent in nature.

Appendix II

Draft summary of the IAASB's discussions at its December 2016 meeting[35]

ISA 315 (Revised)

Ms. Campbell provided the Board with an overview of **Agenda Item 10-A**, including a summary of the outreach performed by the ISA 315 (Revised) Task Force since the IAASB's September 2016 meeting. Ms. Campbell highlighted that the small- and medium-sized practices (SMP) Committee, in a letter to the IAASB Chairman, expressed support for many of the ISA 315 (Revised) Task Force's recommendations. The SMP Committee did however express concern regarding potential unintended consequences of adding susceptibility to fraud as an additional qualitative inherent risk factor and expressed the view that the concept of "difficult for the entity to control" should not be included in a revised definition of significant risk, noting a preference that this concept be incorporated into application material to assist in explaining the nature of a significant risk.

The Board expressed support for many of the ISA 315 (Revised) Task Force's recommendations included in **Agenda Item 10-A**, including support for efforts to consider the ability of ISA 315 (Revised) to be applied to a wide range of circumstances and scalability with respect to the components of internal control. The Board provided additional matters for the ISA 315 (Revised) Task Force to consider as it progresses the project and in certain areas asked the ISA 315 (Revised) Task Force to consider additional points. Specifically, the Board:

- Asked the ISA 315 (Revised) Task Force to provide clarity as to how some of the proposals would be operationalized, particularly the recommendation to require the auditor to develop an expectation of the classes of transactions, account balances and disclosures expected to be in the entity's financial statements and the consideration of the qualitative inherent risk factors in the identification of significant risks.
- Suggested that the ISA 315 (Revised) Task Force continue to explore the implications of a combined or separate assessment of inherent risk and control risk.
- Recommended outreach with the Public Company Accounting Oversight Board (PCAOB) regarding the proposal to require the auditor to determine significant classes of transactions, account balances and disclosures, and their relevant assertions, to further understand how this is applied in practice.
- Expressed mixed views regarding the ISA 315 (Revised) Task Force's recommendations related to paragraph 18 of ISA 330 to change the requirement for substantive procedures from 'material' classes of transactions, account balances and disclosures to those that are 'significant'. Board members noted variously that the recommendations may result in the purpose of that paragraph being completely different than what is currently intended.
- Expressed mixed views regarding adding the susceptibility to fraud as an additional qualitative inherent risk factor, with some expressing support as being a needed addition, while others noted the risk of confusion regarding the extent of the consideration of controls related to inherent risks (as certain aspects of fraud, such as opportunity, relate to consideration of controls).

[35] These draft minutes are still subject to IAASB review and may be subject to further change.

- Asked the ISA 315 (Revised) Task Force to further consider and clarify the interactions between the qualitative inherent risk factors being proposed for ISA 315 (Revised) and the qualitative factors noted within the ISA 540 project.
- In relation to the Task Force recommendation that the determination of significant risk should be based on the relative likelihood and magnitude of misstatement, and on the nature of the risk in the context of the qualitative inherent risk factors (i.e., a high inherent risk driven by the relative likelihood and magnitude of misstatement and one or a combination of the qualitative inherent risks factors), whether a definition of significant risk that includes these concepts would sufficiently facilitate the auditor's determination of significant risks given these concepts are relevant to the assessment of all inherent risks;
- Queried whether those inherent risks that have a low likelihood of misstatement, but if that misstatement were to occur, it would be of high magnitude in terms of its materiality, would be considered to be a significant risk;
- Provided various suggestions for the ISA 315 (Revised) Task Force to consider related to the definition of significant risk, including that:
    - Significant risk should remain a subset of inherent risks; and
    - Reference to "difficult for management to control" be considered for application material and not within the definition or the requirements.

PIOB OBSERVER REMARKS

Prof. Van Hulle commented on the addition of susceptibility to fraud as a qualitative inherent risk factor, noting that from a public interest perspective there is an expectation that the susceptibility of fraud be a part of the auditor's considerations in the identification and assessment of risks.

WAY FORWARD

The ISA 315 (Revised) Task Force will continue to progress possible changes to ISA 315 (Revised), taking into account the Board's feedback. The ISA 315 (Revised) Task Force will bring further matters for discussion to the March 2017 IAASB Consultative Advisory Group (CAG) and IAASB meetings on issues identified in the project proposal that have not yet been discussed such as matters related to information technology, data analytics and professional skepticism in the context of the auditor's risk assessment procedures.