ISA 315 (Revised)[1] – Revised Definitions

This Agenda Item sets out the revised definitions marked-up to definitions presented at the June 2019 Board meeting (**Agenda Item 2-B** and **Agenda Item 2-F (Updated)**, as applicable).

Definitions

16. For purposes of the ISAs, the following terms have the meanings attributed below:

(a) [*Moved*]

(b) *Assertions* – Representations, explicit or otherwise, with respect to the recognition, measurement, presentation and disclosure of information in the financial statements which are inherent in management representing that the financial statements are prepared in accordance with the applicable financial reporting framework. Assertions are used by the auditor to consider the different types of potential misstatements that may occur when identifying, assessing and in responding to the risks of material misstatement. (Ref. Para: A1–A2).

(c) *Business risk* – A risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.

(d) *Controls* – Policies or procedures that an entity establishes ~~are embedded within the components of the system of internal control~~ to achieve the control objectives of management or those charged with governance. In this context: (Ref: Para. A2a–A4a)

(i) Policies are statements of what should, or should not, be done within the entity to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

(ii) Procedures are actions to implement policies. ~~(Ref: Para. A3–A4)~~

(e) *General information technology (IT) controls* – Controls ~~activities~~ over the entity's IT processes that support the continued proper operation of the IT environment, including the continued effective functioning of information processing controls ~~or~~ and the integrity of information (i.e. the completeness, accuracy and validity of information) in the entity's information system. ~~General IT controls are controls over the entity's IT processes.~~ Also see the definition of *IT environment*.

(ea) *Information processing controls* – Controls ~~activities~~ in the control activities component that directly ~~support the actions to mitigate transactions and information processing~~ address risks to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information) throughout processing in IT applications or manual information processes in the entity's information system. ~~They may operate at the assertion level or may support the operation of other control activities at the assertion level. The objectives of information processing controls which are to maintain the completeness, accuracy and validity of transactions and other information throughout processing. Such controls may be automated or manual and may rely on information, or other controls, including other information processing controls that maintain the integrity of information.~~ (Ref: Para. A4b)

[1] Proposed ISA 315 (Revised), *Identifying and Assessing the Risks of Material Misstatement* (ED-315)

(f) *Inherent risk factors* – Characteristics of events or conditions that affect susceptibility to misstatement, whether due to fraud or error, of an assertion about a class of transactions, account balance or disclosure, before consideration of controls. Such factors may be qualitative or quantitative, and include complexity, subjectivity, change, uncertainty or susceptibility to misstatement due to management bias or other fraud risk factors[2] insofar as they affect inherent risk. (Ref: Para. A5–A6)

(g) *IT environment* – The IT applications and supporting IT infrastructure, as well as the IT processes and personnel involved in those processes, that an entity uses to support business operations and achieve business strategies. For the purposes of this ISA:

(i) An IT application is a program or a set of programs that is used in the initiation, processing, recording and reporting of transactions or information. IT applications include data warehouses ~~or~~ and report writers.

(ii) The IT infrastructure comprises the network, operating systems, and databases and their related hardware and software.

(iii) The IT processes are the entity's processes to manage access to the IT environment, manage program changes or changes to the IT environment and manage IT operations.

(h) *Relevant assertions* – An assertion about a class of transactions, account balance or disclosure is relevant when it has an identified risk of material misstatement. The determination of whether an assertion is a relevant assertion is made without taking into account any plans by the auditor to test the operating effectiveness ~~before consideration~~ of controls. (Ref: Para. A9)

(ha) *Risks arising from the use of IT* – Susceptibility of information processing controls to ineffective design or operation, or risks to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information)~~to the integrity of the entity's information~~ in the entity's information system, due to ~~the~~ ineffective design or operation of controls in the entity's IT processes (see IT environment).

(i) *Risk assessment procedures* – The audit procedures designed and performed to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels.

(j) *Significant class of transactions, account balance or disclosure* – A class of transactions, account balance or disclosure for which there is one or more relevant assertions.

(k) *Significant risk* – An identified risk of material misstatement: (Ref: Para. A10)

(i) For which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk due to the degree to which the inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur; or

(ii) That is to be treated as a significant risk in accordance with the requirements of other ISAs.[3]

(l) *System of Internal Control* – The system designed, implemented and maintained by those charged with governance, management and other personnel, to provide reasonable

---

[2] ISA 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*, paragraphs A24–A27

[3] ISA 240, paragraph 27 and ISA 550, *Related Parties*, paragraph 18

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. For the purposes of the ISAs, the system of internal control consists of five inter-related components:

(i) Control environment.

(ii) The entity's risk assessment process.

(iii) The entity's process to monitor the system of internal control.

(iv) The information system and communication.

(v) Control activities.