Exposure Draft ISA 315 (Revised)¹ – Revised Definitions

This paper sets out the new and revised definitions:

- For definitions presented in ED-315, marked-up to ED-315.
- New definitions based on the drafting approach agreed to by the Board in March 2019 (shown in mark-up with an indication of where the definition was moved from).

Definitions

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

(a) **Application controls** – Controls of a preventative or detective nature that support the initiation, recording, processing and reporting of transactions or other information in the entity’s information system, the objectives of which are to maintain the reliability of such transactions and other information. Such controls may rely on information, or other controls that maintain the integrity of information, or may rely on the operation of other controls.  

[Moved to para. 16(ea)]

(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.

(ca) **New** **Control activities** – The entity’s procedures to implement its policies that relate to the other components of the entity’s system of internal control. (Ref. Para: A4a)

(d) **Controls** – Policies or procedures that 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:

(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)

---

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

*Prepared by: Bev Bahlmann and Phil Minnaar (May 2019)*
(e) *General information technology (IT) controls* – Controls activities related to that support the continued proper operation of the IT environment, including that support the continued effective functioning of application information processing controls or the integrity of information (i.e., the completeness, accuracy and validity of information) in by helping to maintain the continued operation, as designed, of the entity’s information system. General IT controls are include controls over the entity’s IT processes. Also see the definition of IT environment.

(ea) *Information processing Application controls* – Controls activities of a preventative or detective nature that directly support the actions to mitigate initiation, recording, processing and reporting of transactions and information processing risks or other information 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 reliability of such transactions and other information throughout processing. Such controls may be automated or manual and may rely on information, or other controls, including other that maintain the integrity of information processing controls that maintain the integrity of information, or may rely on the operation of other controls.

[Moved from para. 16(a)]

(f) *Inherent risk factors* – Characteristics of events or conditions that affect susceptibility to misstatement 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 misappropriation of assets or fraud. (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 report writers.

(ii) The IT infrastructure is comprised of 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, which includes monitoring the IT environment.

(ga) *Other relevant sources of audit evidence* — Information that is relevant to identifying and assessing risks of material misstatement from:

(i) The auditor’s acceptance or continuance of the client relationship or the audit engagement;

(ii) Other engagements performed by the engagement partner for the entity, where applicable.
(gb) **Relevant aspects of the control environment** – The set of controls, processes and structures that address:

(i) How management’s oversight responsibilities are carried out, such as the entity’s culture and management’s commitment to integrity and ethical values;

(ii) When those charged with governance are separate from management, the independence of, and oversight over the entity’s system of internal control by, those charged with governance;

(iii) The entity’s assignment of authority and responsibility;

(iv) How the entity attracts, develops, and retains competent individuals; and

(v) How the entity holds individuals accountable for their responsibilities in the pursuit of the objectives of the system of internal control.

*Moved from para. 27 of ED–315*

(gc) **Relevant aspects of the entity and its environment** – These comprise:

(i) The entity’s organizational structure, ownership and governance, and its business model, including the extent to which the business model integrates the use of IT;

(ii) Industry, regulatory and other external factors; and

(iii) The measures used, internally and externally, to assess the entity’s financial performance.

*Moved from para. 23(a) of ED–315*

(gd) **Relevant aspects of the entity’s process to monitor the system of internal control** – Those aspects of the entity’s process that address:

(i) Ongoing and separate evaluations for monitoring the effectiveness of controls, and the identification and remediation of control deficiencies identified; and

(ii) The entity’s internal audit function, if any, including its nature, responsibilities and activities.

*Moved from para. 32 of ED–315*

(ge) **Relevant aspects of the entity’s risk assessment process** – Those aspects of the entity’s process that address:

(i) Identifying business risks relevant to financial reporting objectives;

(ii) Assessing the significance of those risks, including the likelihood of their occurrence; and

(iii) Addressing those risks.

*Moved from para. 29 of ED–315*

(gf) **Relevant aspects of the information system and communication**

**Relevant aspects of the information system** – The entity’s information processing activities, including its data and information, the resources to be used in such activities and the policies that define, for significant classes of transactions, account balances and disclosures:

(i) How information flows through the entity’s information system, including how:
a. Transactions are initiated, and how information about them is recorded, processed, corrected as necessary, and incorporated in the general ledger and reported in the financial statements; and

b. Information about events and conditions, other than transactions, is captured, processed and disclosed in the financial statements.

(ii) The accounting records, specific accounts in the financial statements and other supporting records relating to the flows of information in the information system;

(iii) The financial reporting process used to prepare the entity’s financial statements, including disclosures; and

(iv) The entity’s resources, including the IT environment, relevant to (i)–(iii) above.

Moved from para. 35 of ED–315

New Relevant aspects of communication – Communications in relation to significant matters that support the preparation of the financial statements and other reporting responsibilities in the information system and other components of the system of internal control:

(i) Between people within the entity, including how financial reporting roles and responsibilities are communicated;

(ii) Between management and those charged with governance; and

(iii) With external parties, such as those with regulatory authorities.

Moved from para. 37 of ED–315

(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 before consideration of controls.2 (Ref: Para. A9)

(ha) New Risks arising from IT – Susceptibility of information processing controls to ineffective design or operation, or risks to the integrity of the entity’s information in the entity’s information system, due to the ineffective design or operation of 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 risk3 – An identified risk of material misstatement:

(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 one or a combination of the inherent risk factors affect the likelihood of a misstatement occurring and the magnitude of potential misstatement should that misstatement occur; or

---

2 Definition as agreed to by the IAASB previously – see para. 101 in Agenda Item 4 of March 2019

3 Definition as agreed to by the IAASB previously – see para. 111 in Agenda Item 4 of March 2019
(ii) That is to be treated as a significant risk in accordance with the requirements of other ISAs.4 (Ref: Para. A10)

(i) **System of Internal Control** – The system 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. For the purposes of the ISAs, the system of internal control consists of five inter-related components: (Ref: Para. A11)

(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.

---