Chapter 3

ISA 315 (Revised) - Key requirements

This article aims to:

Provide an overview of the key changes introduced by the revised ISA 315.

The International Auditing and Assurance Standards Board (IAASB) has issued revised International Standard on Auditing (ISA) 315, *Identifying and Assessing the Risks of Material Misstatement* in December 2019. This ISA will be effective for audits of financial statements of all entities for periods beginning on or after 15 December 2021. The ISA has been revised to respond to challenges and issues with the current ISA 315, *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment* by making changes for clarity and consistent application.

With the changes in the environment, including financial reporting frameworks becoming more complex, technology being used to a greater extent and entities and their governance structures becoming more complex, there was an urgent need to have a robust and comprehensive risk identification and assessment mechanism. Also, the current standards on auditing did not address the potential benefits and implications of using automated tools and techniques by the entities at large in the current times.

Therefore, the revised standard addresses these issues by significantly enhancing the auditor's considerations in relation to an entity's use of Information Technology (IT) and its impact on the audit. It also clarifies the auditor's understanding of the entity's control environment and how this forms a foundation for the rest of the entity's system of internal control.

In this article, we aim to summarise the key changes introduced by revised ISA 315 with respect to identification and assessment of material misstatement in the financial statements.

Overview of revised ISA 315

Understanding system of internal control

The IAASB is of an opinion that understanding an entity's system of internal control is integral to the auditor's identification and assessment of the risks of material misstatement. Therefore, the term *internal control,* as it is used in extant ISA 315, has been revised to the entity's *system of internal controls.* The definition has been extended to reflect that the entity's system of internal control comprises of following five components:

a. Control environment

b. Entity's risk assessment process

c. Entity's process to monitor the system of internal control

d. Information system and communication and

e. Control activities.

Therefore, understanding all components to the extent implemented by an entity is vital to understand the entity's system of internal control relevant to financial reporting. Financial reporting system is relevant to the preparation of the financial statements in accordance with the requirements of the applicable financial reporting framework.

An important management responsibility is to establish and maintain an entity's system of internal control on an ongoing basis. Management's process to monitor the system of internal control could include considering whether controls are operating as intended and they are modified appropriately for changes in conditions.

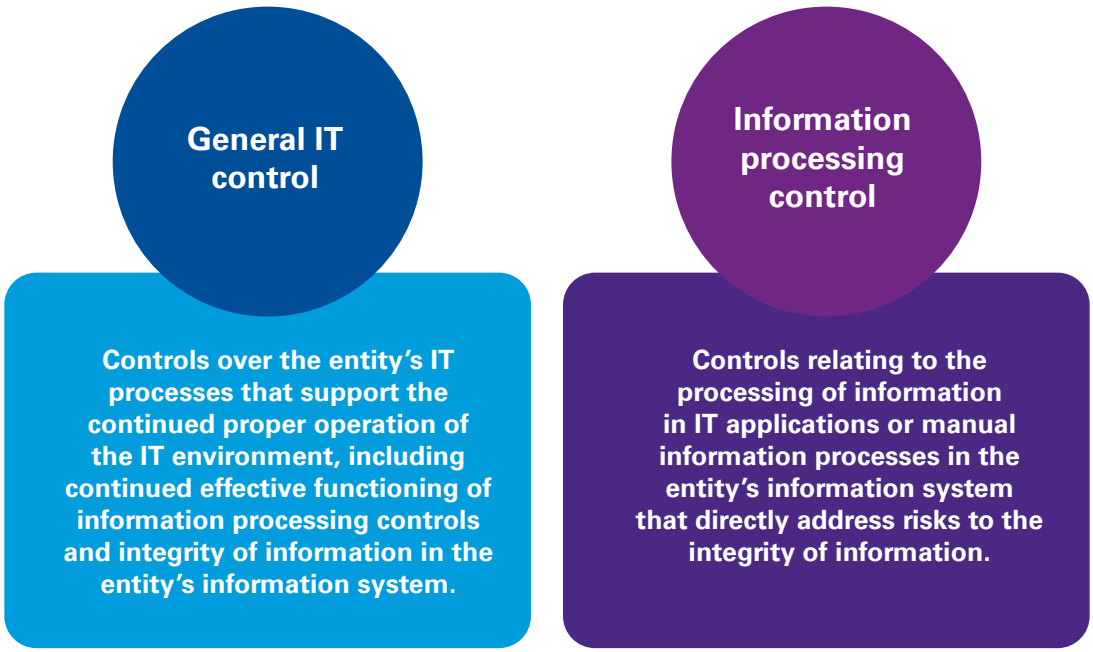
The entity's process to monitor the system of internal control may include activities such as management's review of whether bank reconciliations are being prepared on a timely basis, internal auditors' evaluation of sales personnel's compliance with the entity's policies on terms of sales contracts, and a legal department's oversight of compliance with the entity's ethical or business practice policies.

The auditor, on the other hand, would evaluate the Design of each control relevant to the audit and determine whether it has been Implemented (D&I). Based on the D&I, it may plan to test the operating effectiveness of these controls.

Entity's use of Information Technology (IT)

In current times, there are significant changes in economic, technological and regulatory aspects of the markets and environment in which entities and audit firms operate. Additionally, there is a continuing evolution of entities' use of IT. The standard recognises that there could be risks of material misstatement from the entity's use of IT such as, risks to the integrity of information in the entity's information system due to ineffective design or operation of controls in the entity's IT processes.

Therefore, there is a need for more robust understanding of the entity's control environment including its IT controls. Accordingly, the standard introduces new definition of 'general IT controls' and 'information processing controls' which are explained in the figure below:



The auditor's understanding of the IT environment may focus on identifying, and understanding the nature and number of, the specific IT applications and other aspects of the IT environment that are relevant to the flows of transactions and processing of information in the information system. Changes in the flow of transactions, or information within the information system may result from program changes to IT applications, or direct changes to data in databases involved in processing, or storing those transactions or information.

The increasing use of automated tools and techniques by auditors when performing risk assessment procedures necessitated changes in the standard to recognise usage of such tools and techniques explicitly. Accordingly, the standard allows an auditor to use automated techniques to obtain direct access to or a digital download from the databases in the entity's information system that store accounting transactions. Analysis of complete or large sets of transactions through application of automated tools or techniques may result in the identification of variations from the normal or expected processing procedures or such transactions which may result in the identification of risk of material misstatement.

Risk assessment procedures

Risks of material misstatement could include both those due to error and those due to fraud. The standard requires that risk assessment procedures should be performed to obtain audit evidence to support identification and assessment of the risks of material misstatement in an unbiased manner. Audit evidence from risk assessment procedures comprise both information that supports and corroborates management's assertions and any information that contradicts such assertions. This may involve obtaining evidence from multiple sources within and outside entity. The sources of information for risk assessment may include:

a. Interactions with the management, those charged with governance and other key entity personnel such as internal auditors

b. Certain external parties such as regulators whether obtained directly or indirectly

c. Publicly available information about the entity, for instance, press releases issued by entity, analysts' reports or information about trading activity.

The risk assessment procedures should be performed to obtain an understanding of the entity's organisational structure, ownership and governance, and its business model, including the extent to which the business model integrates the use of IT, applicable financial reporting framework and entity's accounting policies and reasons for changes thereto.

The standard also introduces the requirement of 'stand-back' once the risk assessment procedures have been performed. It requires an auditor to reconsider whether all significant classes of transactions, account balances and disclosures have been identified once the initial risk identification and assessment has been completed. For material classes of transactions, account balances or disclosures that have not been determined to be significant classes of transactions, account balances or disclosures, the auditor shall evaluate whether the auditor's determination remains appropriate.

Documentation

The revised standard strengthened the documentation requirements relating to the exercise of professional skepticism by an auditor. For instance, when the audit evidence obtained from risk assessment procedures includes evidence that both corroborates and contradicts management's assertions, the documentation may include how the auditor evaluated that evidence, including the professional judgements made in evaluating whether the audit evidence provides an appropriate basis for the auditor's identification and assessment of the risks of material misstatement.

Way forward

The entities should take note of the requirements envisaged by the revised standard, in particular, developing a robust control environment with a focus on IT and related application processing controls.