

## **ISA (UK) 315 (Lecture A808 – 22.54 minutes)**

ISA (UK) 315 (Revised July 2020) *Identifying and Assessing the Risks of Material Misstatement* is effective for audits of financial statements for periods beginning on or after 15 December 2021 (i.e. December 2022 year ends onwards, or short periods) and early adoption is permissible.

Previous quarterly updates have discussed the changes arising from ISA (UK) 315 (Revised) which can be summarised as follows:

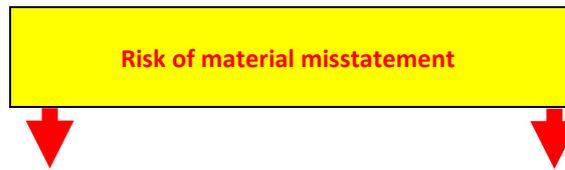
- Five new inherent risk factors to aid in risk assessment
- A new 'spectrum of risk' at the higher end of which lies significant risks
- Sufficient and appropriate audit evidence to be obtained from risk assessment procedures as the basis for the risk assessment
- Significant enhances on IT general controls
- More controls relevant to the audit on the design and implementation work required for such controls
- Inclusion of considerations specific to smaller entities within the main body of the standard and removal of the separate section related to this
- Requirement for inherent and control risk to be assessed separately
- Distinguishing between direct and indirect control components
- New stand-back requirement which requires the auditor to reconsider their assessment if they deem material classes of transactions, account balances and disclosures as insignificant

This section of the course does not examine the detailed technical requirements of ISA (UK) 315 but aims to 'bring together' the five risk factors noted above and briefly examines the new controls over IT.

### **1.1 Risk assessment**

The objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels. This provides a basis for designing and implementing responses to the risk of material misstatement.

Many auditors will be familiar with the audit risk model (which has not been affected by the changes to ISA (UK) 315) and remains as follows:



$$\text{Audit risk (AR)} = \text{Inherent risk (IR)} \times \text{Control risk (CR)} \times \text{Detection risk (DR)}$$

While there

have been no changes to the audit risk model, there have been changes as to how these risks are evaluated. ISA (UK) 315 (Revised) enhances the requirement for the auditor to understand the audit risk of the client by obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control.

Using the audit risk model above, these can be considered as follows:

### **Inherent risk**

- Understanding the entity and its environment, including assessment and evaluation as appropriate
- Understanding the applicable financial reporting framework (e.g. IFRS or FRS 102 *The Financial Reporting Standard applicable in the UK and Republic of Ireland*)

### **Control risk**

- Understanding the entity's system of internal control

## **1.2 Risk factors**

Inherent risk is described as the susceptibility of an assertion about a class of transaction, account balance or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls.

There are five risk factors that must be considered as follows:

Defined inherent risk factor	Example
Complexity	This arises due to the nature of the information or the way that the information is prepared. For example, a complex accounting treatment such as non-basic financial instruments or the fact that the entity is a complex entity or has a complex group structure.

Subjectivity	Results from inherent limitations in the ability to prepare information objectively. For example, a choice of valuation methodology or accounting estimates.
Change	Events or conditions which affect the entity's business, industry, regulatory or economic environment. For example, a change in customer base or geographical expansion.
Uncertainty	This arises when the required information cannot be prepared based on sufficiently precise and comprehensive data. For example, a contingent liability or uncertainty over key issues. Other examples include environmental, legal or financial issues such as the audit of a company with ongoing litigation which requires material provisions and estimations of liabilities.
Susceptibility to misstatement due to management bias or other fraud risk factors	Conditions which create susceptibility for intentional or unintentional failure by management to maintain neutrality. For example, transactions with related parties, the use of manual adjustments and bonus schemes which are dependent on financial results.

Remember, inherent risk is considered BEFORE the auditor considers any related controls. Inherent risk and control risk are both elements of the risk of material misstatement at the assertion level.

### 1.3 Spectrum of inherent risk

For the identified risks of material misstatement at the assertion level, ISA (UK) 315 (Revised) requires the auditor to carry out a **separate** assessment of inherent and control risk. This separate assessment was introduced into ISA (UK) 315 (Revised) to maintain consistency with ISA (UK) 330 *The Auditor's Responses to Assessed Risks* which also requires the auditor to consider inherent risk and control risk separately in order to respond appropriately to the assessed risks of material misstatement at the assertion level.

It is accepted that inherent risk will be higher for some assertions and related classes of transactions, account balances and disclosures than for others and so the auditor will be required to exercise professional judgement in this respect. The degree to which inherent risk varies is referred to in ISA (UK) 315 (Revised) as the **spectrum of inherent risk**.

The spectrum of inherent risk assists the auditor in determining whether an identified risk is a significant risk. ISA (UK) 315 introduces the concept of a significant risk, which is an identified risk of material misstatement for which the assessment of risk is close to the upper end of the spectrum of inherent risk. This is due to the degree to which inherent risk factors affect the combination of the **likelihood and the magnitude** of a potential misstatement.

When planning responses to identified risks, the auditor may need to prioritise risks so as to obtain more evidence in relation to significant risks. Effectively, the higher on the spectrum of inherent risk a risk is assessed, the more persuasive the audit evidence will need to be.

#### 1.4 Control risk

Control risk is the risk that the entity’s system of internal control will not prevent or detect and correct a misstatement on a timely basis. This can be down to weak or missing controls. ISA (UK) 315 (Revised) sets out the **components** of the entity’s system of internal control which is outlined in the table below:

Components of the entity’s system of internal control under ISA (UK) 315 (Revised)		Predominant type of control
<ul style="list-style-type: none"> <li>Control environment</li> <li>The entity’s risk assessment process</li> <li>The entity’s process to monitor the system of internal control</li> </ul>		<p><b>Indirect control</b></p> <p>Auditor’s understanding of these control components is likely to affect the risk of material misstatement at the financial statement level</p>
		<p><b>Direct controls (previously called ‘key’ controls)</b></p>
<ul style="list-style-type: none"> <li>Information system and communication</li> <li>Control activities</li> </ul>		<p>Auditor’s understanding of these control components is likely to affect the risk of material misstatement at the assertion level</p>

#### Direct and indirect controls

Direct controls are specific controls which are precise enough to address the risk of material misstatement at the assertion level. For example, performing a monthly bank reconciliation which is then reviewed and all differences are resolved. This is an example of a direct control because it ensures the existence and accuracy of the asset (bank) at the period end.

Indirect controls, such as general IT controls, are those which are not sufficiently precise enough to prevent, detect or correct a material misstatement at the assertion level. However, indirect controls may support direct controls and hence have an indirect effect on the likelihood that a misstatement can be detected or prevented.

## 1.5 Controls over the IT environment

ISA (UK) 315 contains enhanced requirements over IT and general IT controls. The auditor must understand how the entity processes information, and how this data is used throughout the business. There must be an understanding of the accounting records, how the information is captured and controlled and how all these data flow into the financial statements.

The internal control of an entity generally benefits from the use of an IT system as follows:

- Applying consistent business rules
- Performing complex or repetitive bulk calculations
- Facilitating analysis of information
- Improving timeliness, availability and accuracy of information
- Reducing the risk that controls can be avoided and enhancing the segregation of duties

An IT system is only as good as the controls that support it. Hence, it is important that an assessment is made of the related risks of using IT and the entity's general IT controls. General IT controls alone are inadequate, and an assessment must be made to understand how management monitor the IT controls, permissions, errors or control deficiencies across the entity's entire IT environment.

Larger businesses may have fully integrated and possibly bespoke ERP systems (Enterprise Resource Planning). Smaller businesses are likely to have less complex, commercial software. ISA (UK) 315 (Revised) provides examples of potential issues and possible tests in Appendices 5 and 6. The need to obtain an understanding of the IT environment within an entity remains important when assessing risks and designing relevant audit procedures.

## 1.6 Detection risk

The last element of the audit risk model is detection risk. This is the risk that the audit procedures carried out by the auditor to reduce audit risk (i.e. the risk the auditor expresses an incorrect opinion on the financial statements) to an acceptably low level will fail to detect a misstatement which exists that could be material. Detection risk is the **only** risk under the control of the auditor and is not part of the risk of material misstatement.

## 1.7 Stand-back requirement

Once the auditor has obtained the required level of understanding and has identified the significant classes of transactions, account balances and disclosures, they must 'stand back' and evaluate the audit evidence arising from their risk assessment.

Once this understanding has been obtained (and throughout the audit process), the auditor must apply professional scepticism in critically evaluating the audit evidence and knowledge.

For material classes of transactions, account balances and disclosures that have not been determined as significant, the auditor is required to assess, using professional judgement, whether this determination remains appropriate.

The stand-back requirement has been brought into ISA (UK) 315 (Revised) to prompt the auditor to confirm the **completeness** of the identified risks. In other words, requiring the auditor to focus their attention on material classes of transactions, account balances and disclosures that have not been determined as significant and to assess whether this remains the case on evaluating all of the evidence obtained from the risk assessment process that has been carried out.

### **1.8 Scalability**

Auditors should beware – ISA (UK) 315 (Revised) is three times the size of its predecessor. Hence, the requirements are extensive and will impact all audits. There are provisions throughout the standard which allow for scalability, whereby smaller audits will involve less onerous assessments.