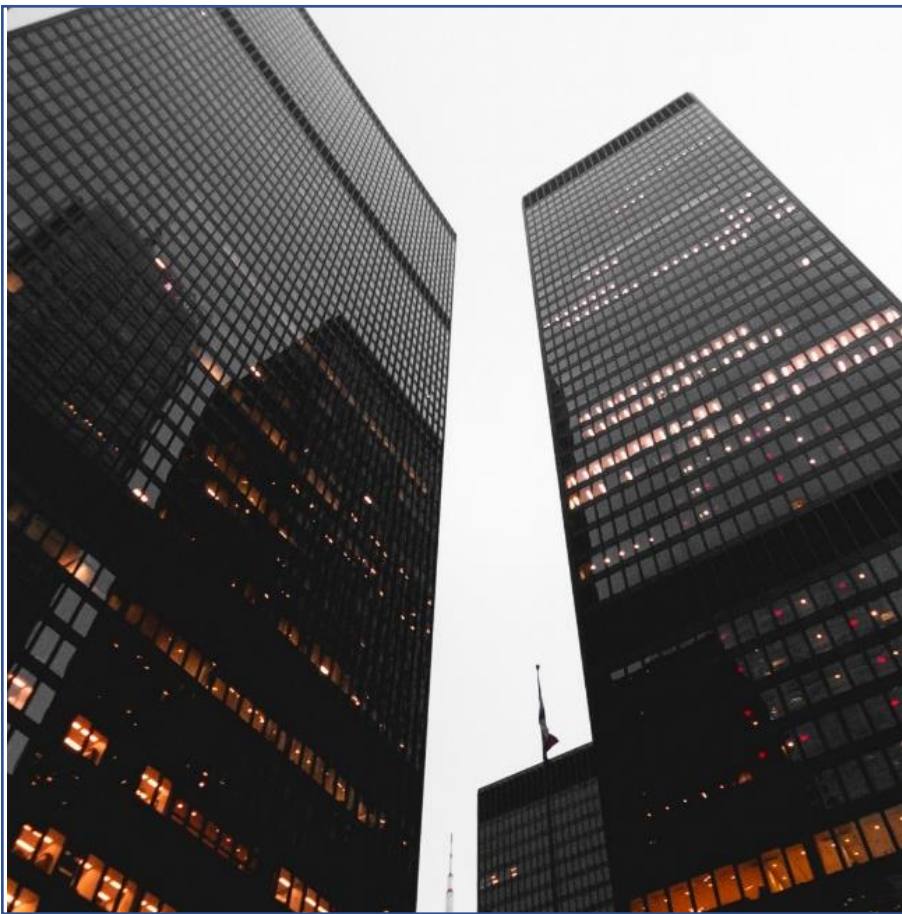


Newsletter

Issue No. 05 | February 2023



In this Issue

ISA 315 (Revised 2019) has been enhanced to form a stronger foundation for the audit, in particular better quality risk identification and assessment is expected to enhance the procedures required by other standards such as ISA 330 and ISA 540 (Revised). Conforming and consequential amendments were also made to a number of other ISAs resulting from the changes made to ISA 315 (Revised), including ISA 330, ISA 2405 and ISA 540 (Revised).

Contents

ISA 315 (Revised 2019), Identifying and Assessing the Risks of Material Misstatement	3
REASONS FOR STANDARD REVISION.....	3
EFFECTIVITY	3
KEY CHANGES.....	4
WHAT HAS CHANGED?	4
NATURE AND EXTENT OF RISK ASSESSMENT PROCEDURES.....	5
NEW DEFINITIONS AND CONCEPTS IN ISA 315 (REVISED 2019)	5
DOCUMENTATION AS PER ISA 315 (REVISED)	10
Editorial Board	11

ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement*

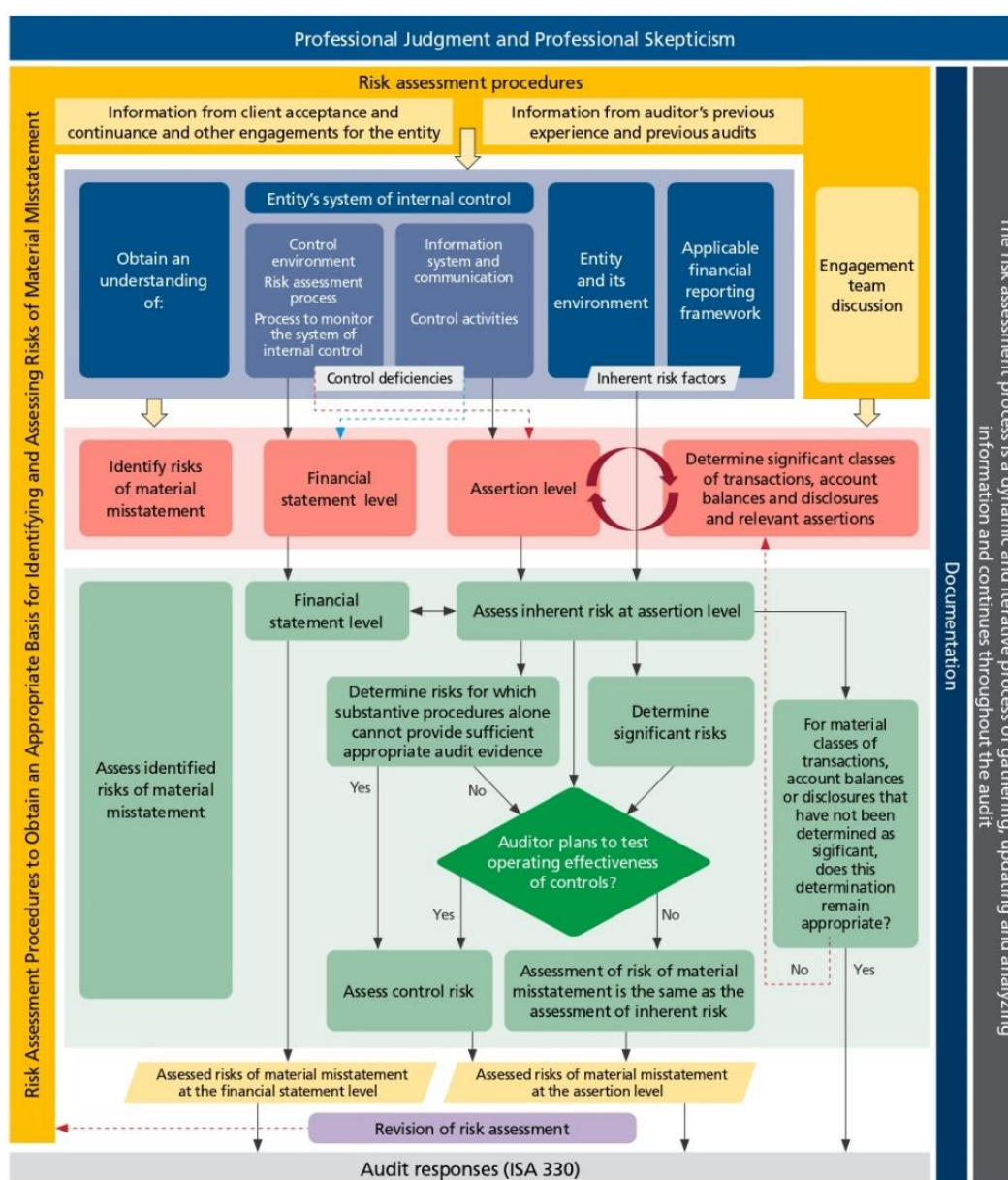
REASONS FOR STANDARD REVISION

- Inconsistency existed in the nature and number of significant risks identified in practice.
- Obtaining an understanding of the system of internal control was difficult to apply in practice.
- Information Technology (IT) risks were not sufficiently addressed in the standard.

EFFECTIVITY

This takes effect **beginning on or after December 15, 2021.**

OVERVIEW OF ISA 315 (REVISED 2019)



Source: [INTRODUCTION TO: ISA 315 \(REVISED 2019\) Identifying and Assessing the Risks of Material Misstatement](#)

KEY CHANGES

1. Understanding system of internal control
2. Entity's use of Information Technology (IT)
3. Risk assessment procedures
4. Documentation

WHAT HAS CHANGED?

- **Inherent Risk, Control Risk, Detection Risk**

UNCHANGED	CHANGED
<p>The concepts of inherent risk, control risk and detection risk as described in ISA 200.</p>	<p>A separate assessment of inherent risk and control risk is now required.</p> <p>The concept of the spectrum of inherent risk has been introduced to assist with the assessment of inherent risk. The spectrum of inherent risk assists the auditor in making a judgment, based on the likelihood and magnitude of a possible misstatement, on a range from lower to higher risk, for the purpose of assessing risks of material misstatement. Inherent risk factors have been introduced to help auditors consider risks of material misstatement on the spectrum of inherent risk.</p>

- **Risk of Material Misstatement**

UNCHANGED	CHANGED
<p>The definition of the risk of material misstatement has not changed:</p> <p>The risk that the financial statements are materially misstated prior to the audit. This consists of two components, described as follows at the assertion level:</p> <ul style="list-style-type: none"> (i) Inherent risk... (ii) Control risk... 	<p>Although the definition of the risk of material misstatement has not changed, in the application material to ISA 200 the 'threshold' for the identification of a possible misstatement has been clarified and explained.</p> <p>By including this clarification in ISA 200, it supports the definition of risk of material misstatement in ISA 200. The clarification explained in the application material to ISA 200 is that a risk of material misstatement exists where there is a reasonable possibility of both a misstatement occurring (i.e., its likelihood), and being material if it were to occur (i.e., its magnitude). Based on this clarification in ISA 200, the term 'reasonably possible' is used within ISA 315 (Revised 2019) as it relates to the threshold for identifying risks of material misstatement.</p>

- **Professional Skepticism**

UNCHANGED	CHANGED
Auditors are required to exercise professional skepticism when designing and performing audit procedures.	There are enhanced procedures to encourage behavioral change for auditors when undertaking audit procedures, as well as strengthened documentation requirements.

- **Considerations Specific to Smaller Entities**

UNCHANGED	CHANGED
<p>The concept of scalability (<i>i.e. being able to apply the ISAs to entities of varying sizes and complexities</i>) is inherent within the IAASB’s standards, and the IAASB always focuses on what more can be done to assist with all entities being able to apply its standards.</p> <p>The IAASB has continued to distinguish the auditor’s considerations in relation to scalability and proportionality within separate paragraphs within the revised standard.</p>	<p>The revised standard focuses on complexity rather than size (<i>i.e., ‘less complex entities’ rather than ‘smaller entities’ in line with the IAASB’s approach to such entities</i>).</p> <p>Scalability has been illustrated through the use of contrasting examples throughout the standard (<i>i.e., illustrating both ends of the complexity spectrum</i>) rather than only focusing on ‘smaller entities’.</p>

- **Considerations Specific to “Public Sector Entities”**

UNCHANGED	CHANGED
Considerations for public sector entities have been maintained.	These paragraphs have been updated where appropriate (<i>i.e., to reflect unique public sector considerations</i>).

NATURE AND EXTENT OF RISK ASSESSMENT PROCEDURES

ISA 315 (Revised 2019) clarifies that the nature and extent of risk assessment procedures required will vary based on the nature and circumstances of the entity. The auditor uses professional judgment to determine the nature and extent of the risk assessment procedures to be performed to meet the requirements of the standard.

NEW DEFINITIONS AND CONCEPTS IN ISA 315 (REVISED 2019)

Several new definitions have been introduced to help with clarity of the requirements. These new definitions have been set out in this guide where relevant (see below tables for reference). Where definitions have been revised, this has also been explained.

Changes to the Required Understanding

NEW RELEVANT DEFINITION	DESCRIPTION	FURTHER EXPLANATORY MATERIAL
Inherent risk factors	<p>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 insofar as they affect inherent risk.</p>	<p>Inherent risk factors may be qualitative or quantitative and affect the susceptibility of assertions to misstatement. Qualitative inherent risk factors relating to the preparation of information required by the applicable financial reporting framework include:</p> <ul style="list-style-type: none"> • Complexity; • Subjectivity; • Change; • Uncertainty; or • Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk. <p>Other inherent risk factors, that affect susceptibility to misstatement of an assertion about a class of transactions, account balance or disclosure may include:</p> <ul style="list-style-type: none"> • The quantitative or qualitative significance of the class of transactions, account balance or disclosure; or • The volume or a lack of uniformity in the composition of the items to be processed through the class of transactions or account balance, or to be reflected in the disclosure.

In ISA 315 (Revised 2019), there are broadly three (3) distinct areas for the auditor's understanding:

- The entity and its environment.
- The applicable financial reporting framework.
- The entity's system of internal control.

In the previous version of the standard, ISA 315 (Revised), the applicable financial reporting framework was not separately distinguished (it was included as part of the understanding of the entity and its environment). This has now been separated and has a distinct focus.

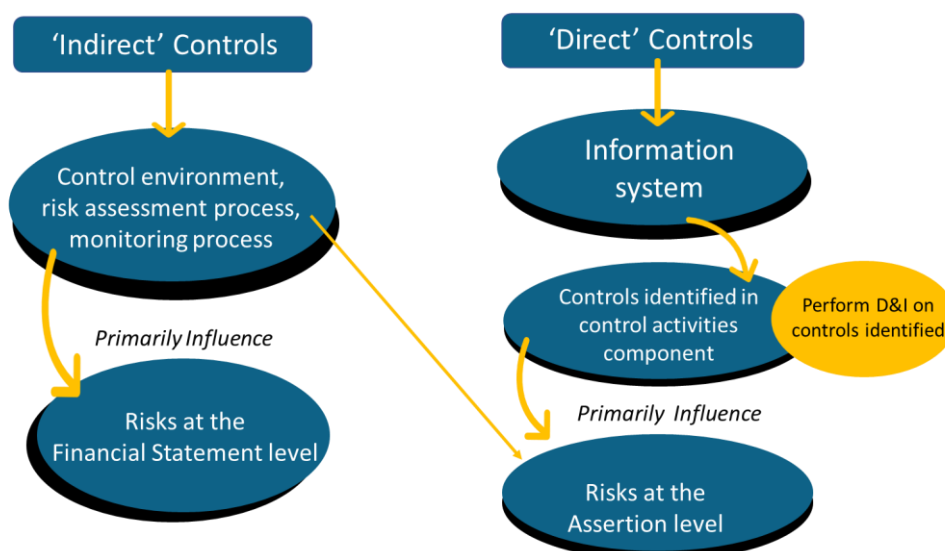
Changes to Understanding the Entity's System of Internal Control

NEW RELEVANT DEFINITION	DESCRIPTION	FURTHER EXPLANATORY MATERIAL
Controls	<p>Policies or procedures that an entity establishes to achieve the control objectives of management or those charged with governance. In this context:</p> <ul style="list-style-type: none"> 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. 	<p>Controls are embedded within the components of the entity's system of internal control.</p> <p>Policies are implemented through the actions of personnel within the entity, or through the restraint of personnel from taking actions that would conflict with such policies.</p> <p>Procedures may be mandated, through formal documentation or other communication by management or those charged with governance or may result from behaviors that are not mandated but are rather conditioned by the entity's culture. Procedures may be enforced through the actions permitted by the IT applications used by the entity or other aspects of the entity's IT environment.</p> <p>Controls may be direct or indirect. Direct controls are controls that are precise enough to address risks of material misstatement at the assertion level. Indirect controls are controls that support direct controls.</p>

Although the approach to understanding the entity's system of control is broadly the same as was required under ISA 315 (Revised) (*i.e., understand the five (5) components of the system of internal control*), many changes have been made about what this understanding entails for each component.

The auditor is still required to understand the five (5) components of the entity's system of internal control. These components of internal control have been split into two (2) types that align with the nature of the controls within each component, and may affect the auditor's identification and assessment of risks of material misstatement, as well as responding to the assessed risks:

- In the control environment, the entity's risk assessment process and the entity's process to monitor the system of internal control components, the controls are primarily indirect controls (although there may be some direct controls these are likely less in these components).
- In the information system and communication, and control activities components, the controls are primarily direct controls.



Information Technology Considerations

NEW RELEVANT DEFINITION	DESCRIPTION	FURTHER EXPLANATORY MATERIAL
General Information Technology (IT) Controls	Controls 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 and the integrity of information (i.e., the completeness, accuracy and validity of information) in the entity’s information system. Also see the definition of IT environment.	N/A
Information Processing Controls	Controls relating to the processing of information in IT applications or manual information processes in the entity’s information system that directly address risks to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information).	Risks to the integrity of information arise from susceptibility to ineffective implementation of the entity’s information policies, which are policies that define the information flows, records and reporting processes in the entity’s information system. Information processing controls are procedures that support effective implementation of the entity’s information policies. Information processing controls may be automated (i.e., embedded in IT applications) or manual (e.g., input or output controls) and may rely on other controls, including other information processing controls or general IT controls.

(continued on the next page)

<p>IT Environment</p>	<p>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:</p> <ul style="list-style-type: none"> 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 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. 	<p>N/A</p>
<p>Risks arising from the use of IT</p>	<p>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) in the entity's information system, due to ineffective design or operation of controls in the entity's IT processes (see IT environment).</p>	<p>N/A</p>

ISA 315 (Revised 2019) has substantially changed and enhanced the requirements and application use and complexity of IT for many entities.

Paragraph A170 in ISA 315 (Revised 2019) explains that the extent of the auditor's understanding of the IT processes, including the extent to which the entity has general IT controls in place, will vary with the nature and circumstances of the entity and its IT environment, as well as based on the nature and extent of the controls identified by the auditor. It is also noted that as the entity's IT environment and IT systems become more complex, the work performed will likely involve team members with specialized IT skills material in relation to the auditor's considerations about IT.

The main changes with regard to IT can be found in the auditor’s required understanding of the information system and control activities components.

Changes to the Identification and Assessment of the Risks of Material Misstatement

NEW RELEVANT DEFINITION	DESCRIPTION	FURTHER EXPLANATORY MATERIAL
Relevant assertion	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 any related controls (i.e., the inherent risk).	A risk of material misstatement may relate to more than one assertion, in which case all the assertions to which such a risk relates are relevant assertions. If an assertion does not have an identified risk of material misstatement, then it is not a relevant assertion. (Para. A9).
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.	N/A

ISA 315 (Revised 2019) has separated the requirements for identifying risks of material misstatement from the requirements for assessing those risks. They are aimed at developing a framework for auditors to identify and assess risks of material misstatement in a robust manner.

DOCUMENTATION AS PER ISA 315 (REVISED)

- Key elements of the auditor’s understanding of the entity and its environment, the applicable financial reporting framework and each of the components of the entity’s system of internal control (the specific paragraphs where the aspects are required to be documented have been noted). The documentation should include the source of the information as well as the risk assessment procedures performed.
- D&I of controls in the control activities component.
- The identified and assessed risks of material misstatement at the financial statement and assertion levels. This also includes significant risks and risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. The rationale for significant judgments made also need to be documented.
- Paragraph A238 in ISA 315 (Revised 2019) also notes various matters that could be documented to demonstrate the exercise of professional skepticism by the auditor.

Our View:

ISA 315 (Revised) forms the foundation in obtaining a comprehensive understanding of the entity and its environment, providing an appropriate basis on which to make an informed risk assessment and to perform an effective risk-based audit. Given its significance, the auditors should have a complete understanding of all revisions made and new concepts presented. The introduction to the new inherent risk factors may help the auditors in assessing the susceptibility of the assertions to misstatement. This will help the auditors in identifying the areas with higher inherent risk for more accurate computation of risk of material misstatement. ISA 315 (Revised) introduced Information Technology (IT) considerations such as general IT controls and information processing controls which helps in addressing risks to the integrity of information. This will help the auditors to effectively implement information policies to improve the quality of audits.

Refer to the links below for reference.

Philippine Standard on Auditing 315 (Redrafted) *Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and its Environment* : <https://www.aasc.org.ph/downloads/psa/publications/PDFs/PSA-315-Redrafted.pdf>

ISA 315 (Revised 2019) *Identifying and Assessing the Risks of Material Misstatement*.
<https://www.ifac.org/system/files/publications/files/IAASB-ISA-135-first-time-implementation-guidance.pdf>

This Newsletter is the official publication of R.S. Bernaldo & Associates to keep the Firm's professional staff informed of the issues affecting the practice. The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The Firm cannot be held liable for any losses suffered as a result of reliance upon information contained in this memo.

This is a property of R.S. Bernaldo & Associates. Reproduction of any material included in the memo should be subject to the approval of the Editorial Board.

R.S. Bernaldo & Associates is a member firm of the PKF International Limited family of legally independent firms and does not accept any responsibility or liability for the actions or inactions of any individual member or correspondent firm or firms.

Comments and suggestions are welcome.

Editorial Board

- Anthony D. Paño
Partner/Head of Quality Assurance Unit
anthony.pano@pkfrsbernaldo.com
- Mary Rose A. Lorilla
Quality Assurance Manager/
Quality Assurance Leader
maryrose.lorilla@pkfrsbernaldo.com
- Charmaine S. de Guzman
Assistant Quality Assurance Manager /
Assistant Quality Assurance Leader
charmaine.deguzman@pkfrsbernaldo.com
- Cherry Joy V. Andallon
Senior Quality Assurance Associate/
Technical Consultation Leader
cherryjoy.andallon@pkfrsbernaldo.com
- Janna J. Pacis
Senior Quality Assurance Associate/
Learning and Training Leader
janna.pacis@pkfrsbernaldo.com
- Baby Joy A. Bautista
Senior Quality Assurance Associate/
Engagement Quality Control
Review Leader
babyjoy.bautista@pkfrsbernaldo.com
- Faye Coleen R. Pardo
Quality Assurance Associate/
Ethics Leader
fayecoleen.pardo@pkfrsbernaldo.com

BOA /PRC No. 0300 • BIR Accredited • SEC Group A Accredited • BSP Group B Accredited • IC Accredited
 18/F Cityland Condominium 10 Tower 1, 156 H.V. dela Costa Street, Ayala North, Makati City, Philippines 1226
Tel: +632 8812-1718 to 22 **Fax:** +632 8813-6539 **Email:** rsbassoc@pkfrsbernaldo.com
www.pkfrsbernaldo.com