SA 300
Planning an Audit of Financial Statements

December 1, 2023

Contents

Objectives and Requirements

The objective of the auditor is to plan the audit so it is performed in an effective manner.

The requirements of the Standard is to involve **all key engagement team members** including the **Engagement Partner** in planning the audit.

The auditor shall undertake the following **Preliminary Engagement Activities** at the beginning of any current audit engagement:

- Perform procedures regarding continuance of client relationship as required by SA 220 "Quality Control for an Audit of Financial Statements"
- Evaluate compliance with ethical requirements, including independence, as required by SA 220
- Establish an understanding of the terms of engagement, as required by SA 210

Planning Activities – The auditor is required to establish an overall audit strategy that sets the scope, timing and direction of the audit and guides the development of the audit plan

In establishing the overall audit strategy, the auditor must:

- Identify the characteristics defining scope of the engagement
- Determine reporting objectives to plan the audit timing and necessary communications
- Consider factors deemed significant in directing the engagement team's efforts
- Reflect on results from preliminary engagement activities and assess the relevance of knowledge gained from other engagements by the partner for the entity
- Determine the NTE (Nature, Timing and Extent) of the resources required for audit.

The auditor is required to develop an audit plan, which should encompass:

- A description of the NTE of planned risk assessment procedures, as guided by SA 315
- A description of the NTE of planned further audit procedures at the assertion level, as determined under SA 330
- Inclusion of other planned audit procedures necessary for compliance with the relevant Standards on Auditing

The Role of Timing and Planning

Adequate planning benefits the audit in several ways:

- Helping the auditor to devote appropriate attention to important areas of the audit
- Helping the auditor identify and resolve potential problems on a timely basis.
- Helping the auditor properly organize and manage the audit engagement so that it is performed in an effective and efficient manner.
- Assisting in the selection of engagement team members with appropriate levels of capabilities and competence to respond to anticipated risks, and the proper assignment of work to them.
- Facilitating the direction and supervision of engagement team members and the review of their work.
- Assisting, where applicable, in coordination of work done by auditors of components and experts.

The nature and extent of planning activities will vary according to the size and complexity of the entity, the key engagement team members' previous experience with the entity, and changes in circumstances that occur during the audit engagement.

Planning is a continual and iterative process and considers matters, such as:

- The analytical procedures to be applied as Risk Assessment Procedures;
- Obtaining a general understanding of the legal and regulatory framework applicable to the entity and how the entity is complying with it;
- The determination of materiality;
- The involvement of experts;
- The performance of other Risk Assessment Procedures.

Other considerations of Planning Activities

- The auditor shall update and change the overall audit strategy and the audit plan as deemed necessary during the course of the audit
- The auditor shall plan the NTE of direction and supervision of the engagement team members and the review of their work.

The Overall Audit Strategy vs. The Audit Plan

In establishing the overall audit strategy, the auditor is able to determine matters such as:

- The resources to deploy for specific audit areas
- The amount of resources to allocate to specific audit areas
- When these resources are to be deployed, such as whether at an interim audit stage or at key cut-off dates
- How such resources are to be managed, directed and supervised and whether to complete engagement quality control reviews.

Once the overall audit strategy has been established, **an audit plan** can be developed **to address** the various **matters identified** in the **overall audit strategy.**

The establishment of the overall audit strategy and the detailed audit plan are **not necessarily discrete or sequential processes** but are **closely inter-related** since changes in one may result in consequential changes to the other.

The Audit Plan:

- The audit plan is more detailed than the overall audit strategy that includes the NTE of audit procedures to be performed. Planning for these audit procedures takes place over the course of the audit.
- Additionally, the auditor may begin the execution of further audit procedures for some classes of transactions, account balances and disclosures before planning all remaining further audit procedures.

Initial Audit Engagements

Auditor's Responsibility:

- Perform procedures required by SA 220 regarding the acceptance of client relationship and specific audit engagement;
- Communicate with the predecessor auditor, where there has been a change of auditors, to comply with ethical requirements.

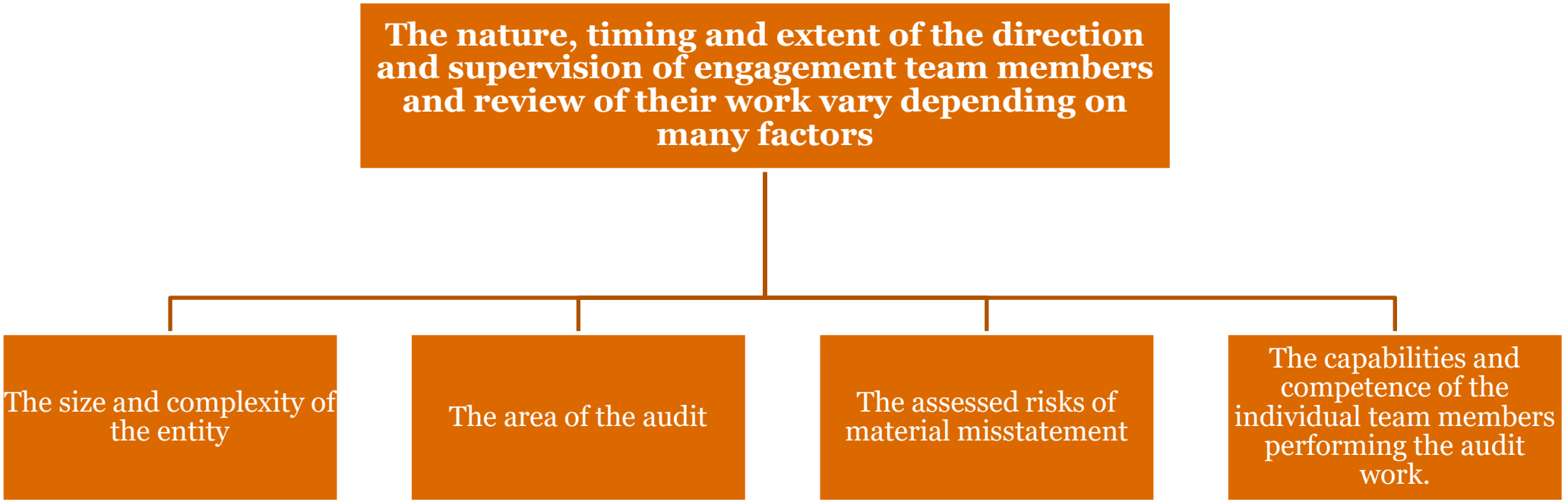
Additional considerations in establishing overall audit strategy and audit plan:

- Unless prohibited by law or regulation, arrangements to be made with the predecessor auditor.
- Any major issues discussed with management in connection with the initial selection as auditor, the communication of these matters to those charged with governance and how these matters affect the overall audit strategy and audit plan.
- The audit procedures necessary to obtain sufficient appropriate audit evidence regarding opening balances, as suggested by SA 510.
- Other procedures required by the firm's system of quality control for initial audit engagements.

Matters that may be considered in Establishing the Overall Audit Strategy

Characteristics of the Engagement	Reporting Objectives, Timing of the Audit, and Nature of Communications
• The financial reporting framework on which the financial information to be audited has been prepared • Industry-specific reporting requirements such as reports mandated by industry regulators • The expected audit coverage, including the number and locations of the components to be included. • The extent to which the components are being audited by other auditors • The nature of the business segments to be audited	• The entity's timetable for reporting, such as at interim and final stages. • The organization of meetings with management and those charged with governance to discuss the nature, timing and extent of the audit work. • The discussion with management regarding the expected communications on the status of audit work throughout the engagement.
• The reporting currency to be used, including any need for currency translation for the financial information audited. • The need for a statutory audit of standalone financial statements in addition to an audit for consolidation purposes. • The availability of the work of internal auditors and the extent of the auditor's potential reliance on such work. • The entity's use of service organizations and how the auditor may obtain evidence concerning the design or operation of controls performed by them.	• The discussion with management and those charged with governance regarding the expected type and timing of reports to be issued and other communications, both written and oral, including the auditor's report, management letters and communications to those charged with governance. • Communication with auditors of components regarding the expected types and timing of reports to be issued and other communications in connection with the audit of components. • Whether there are any other expected communications with third parties.

Direction, Supervision and Review



Matters that may be considered in Establishing the Overall Audit Strategy

Significant Factors, Preliminary Engagement Activities, and Knowledge gained from other engagements	Nature, Timing and Extent of Resources
• The determination of materiality in accordance with SA 3201 • Preliminary identification of areas where there may be a higher risk of material misstatement. • The impact of the assessed risk of material misstatement at the overall financial statement level on direction, supervision and review. • The manner in which the auditor emphasizes to engagement team members the need to maintain a questioning mind and to exercise professional skepticism in gathering and evaluating audit evidence.	• The selection of the engagement team (including, where necessary, the engagement quality control reviewer) and the assignment of audit work to the team members, including the assignment of appropriately experienced team members to areas where there may be higher risks of material misstatement. • Engagement budgeting, including considering the appropriate amount of time to set aside for areas where there may be higher risks of material misstatement.
• The discussion of matters that may affect the audit with firm personnel responsible for performing other services to the entity. • Volume of transactions, which may determine whether it is more efficient for the auditor to rely on internal control. • Importance attached to internal control throughout the entity to the successful operation of the business. • Significant industry developments such as changes in industry regulations and new reporting requirements.	

Documentation

The Overall Audit Strategy:

The documentation of the overall audit strategy is a record of the key decisions considered necessary to properly plan the audit and to communicate significant matters to the engagement team.

The Audit Plan:

The documentation of the audit plan is a record of the planned nature, timing and extent of risk assessment procedures and further audit procedures at the assertion level in response to the assessed risks. It also serves as a record of the proper planning of the audit procedures that can be reviewed and approved prior to their performance.

The Overall Audit Strategy:

A record of the significant changes to the overall audit strategy and the audit plan, and resulting changes to the planned nature, timing and extent of audit procedures, explains why the significant changes were made, and the overall strategy and audit plan finally adopted for the audit. It also reflects the appropriate response to the significant changes occurring during the audit.

SA 315 (Revised)
Identifying and assessing the risks of material misstatements through understanding the entity & its environment

Agenda

- Overview of SA 315
- Components of Internal Controls
- Why SA 315 is Revised?
- What outcome is the revised standard seeking to achieve?
- Key significant changes in SA 315 (Revised)
- Entity's use of Information Technology (IT) In current times
- Documentation improvement

Overview of SA 315

- **Scope-** This Standard on Auditing (SA) deals with the auditor's responsibility to identify and assess the risks of material misstatement in the financial statements, through understanding the entity and its environment, including the entity's internal control.
- **Objective-** 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, through understanding the entity and its environment, including the entity's internal control, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement. This will help the auditor to reduce the risk of material misstatement to an acceptably low level.
- **Definitions of Key terms-**
  - **Assertions:** Representations by management, explicit or otherwise, that are embodied in the financial statements, as used by the auditor to consider the different types of potential misstatements that may occur.
  - **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.
  - **Internal control:** The process 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, safeguarding of assets, and compliance with applicable laws and regulations. The term "controls" refers to any aspects of one or more of the components of internal control.
  - **Significant risk:** An identified and assessed risk of material misstatement that, in the auditor's judgment, requires special audit consideration.

Components of Internal Control

- **Control Environment**
- **Risk assessment process**
- **Information system relevant to FR**
- **Control Activities**
- **Monitoring of Controls**

Components of Internal Control

- **Control Environment-** The auditor shall evaluate whether:

  (a) Management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior; and

  (b) The strengths in the control environment elements collectively provide an appropriate foundation for the other components of internal control, and whether those other components are not undermined by deficiencies in the control environment

- **Risk Assessment Process-** The auditor shall obtain an understanding of whether the entity has a process for:

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

  (b) Estimating the significance of the risks;

  (c) Assessing the likelihood of their occurrence; and

  (d) Deciding about actions to address those risks.

Components of Internal Control

- **Information system relevant to Financial Reporting-** The auditor shall obtain an understanding of the information system, including the related business processes, relevant to financial reporting, including the following areas:

(a) The classes of transactions in the entity's operations that are significant to the financial statements;

(b) The procedures, within both information technology (IT) and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in the financial statements;

(c) The related accounting records, supporting information and specific accounts in the financial statements that are used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the general ledger. The records may be in either manual or electronic form;

(d) How the information system captures events and conditions, other than transactions, that are significant to the financial statements;

(e) The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures;

(f) Controls surrounding journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments.

Components of Internal Control

- **Control Activities relevant to Audit-** The auditor shall obtain an understanding of control activities relevant to the audit, being those the auditor judges it necessary to understand in order to assess the risks of material misstatement at the assertion level and design further audit procedures responsive to assessed risks. An audit requires an understanding of only those control activities related to significant class of transactions, account balance, and disclosure in the financial statements and the assertions which the auditor finds relevant in his risk assessment process.

- **Monitoring of Controls-** The auditor shall obtain an understanding of the major activities that the entity uses to monitor internal control over financial reporting, including those related to those control activities relevant to the audit, and how the entity initiates remedial actions to deficiencies in its controls

Why is SA 315 revised

- Identifying and assessing the risks of material misstatement is foundational to the audit. SA 315 (Revised), Identifying and Assessing the Risks of Material Misstatement, has been revised to require a more robust risk identification and assessment, thereby promoting better responses to the identified risks.

- 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.

- The audit risk model has not changed. However, enhancements and clarifications help auditors in applying the audit risk model when identifying and assessing the risks of material misstatement.

Key significant changes in SA 315 (Revised)

Detailed Guidance materials on Entity's use of Information Technology (IT) In current times

Strengthened documentation requirements relating to the exercise of professional skepticism

The introduction of five new inherent risk factors to aid in risk assessment; subjectivity, complexity, uncertainty, change and susceptibility to misstatement due to management bias or fraud.

A new spectrum of risk, at the higher end of which lie significant risks.

Requiring "sufficient, appropriate" evidence to be obtained from risk assessment procedures as the basis for the risk assessment.

More on controls relevant to the audit and on the design and implementation work required for these controls.

Removal of considerations specific to smaller entities as a separate category of paragraph and inclusion of that material within the main body of the text and the addition of new material.

Requiring inherent and control risk to be assessed separately (the extant standard permits a combined assessment);

Distinguishing between direct and indirect control components; and

A new stand-back requiring reconsideration, when material classes of transactions, account balance and disclosure are not assessed as significant.

What outcome is the revised standard seeking to achieve?

Promote consistency in application of procedures for risk identification and assessment.

Make the standard more scalable through revised principles-based requirements.

Reduce the complexity and make the standard more usable by auditors of all entities, whatever the nature or complexity.

Encourage a more robust risk assessment thereby more focused responses to those identified risks.

Support auditors using the standard by incorporating guidance material that recognizes the evolving environment, including in relation to information technology

Entity's use of Information Technology 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 recognizes 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 to have robust risk assessment methodology

Guidance for entity using IT in current time

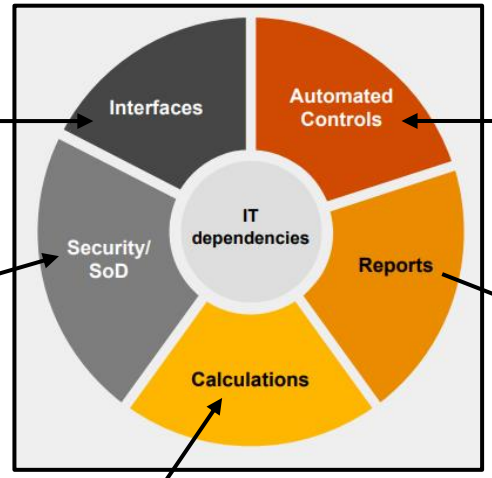
- Implication of the IT Dependency
- Identify and assess the design and implementation of ITGCs related controls
- ITGCs (Controls) that address the risk of arising from use of IT
- Formulation of Conclusion on the Complexity of IT Environment"
- Other IT Risk assessment

Identifying IT Dependencies

Interfaces are programmed logic that transfer data from one IT system to another.

Security, including segregation of duties, is enabled by the IT system to restrict access to information and to identify any lack of separation of roles and responsibilities that could allow an employee to perpetrate and conceal errors or fraud, or allow process errors to go undetected.

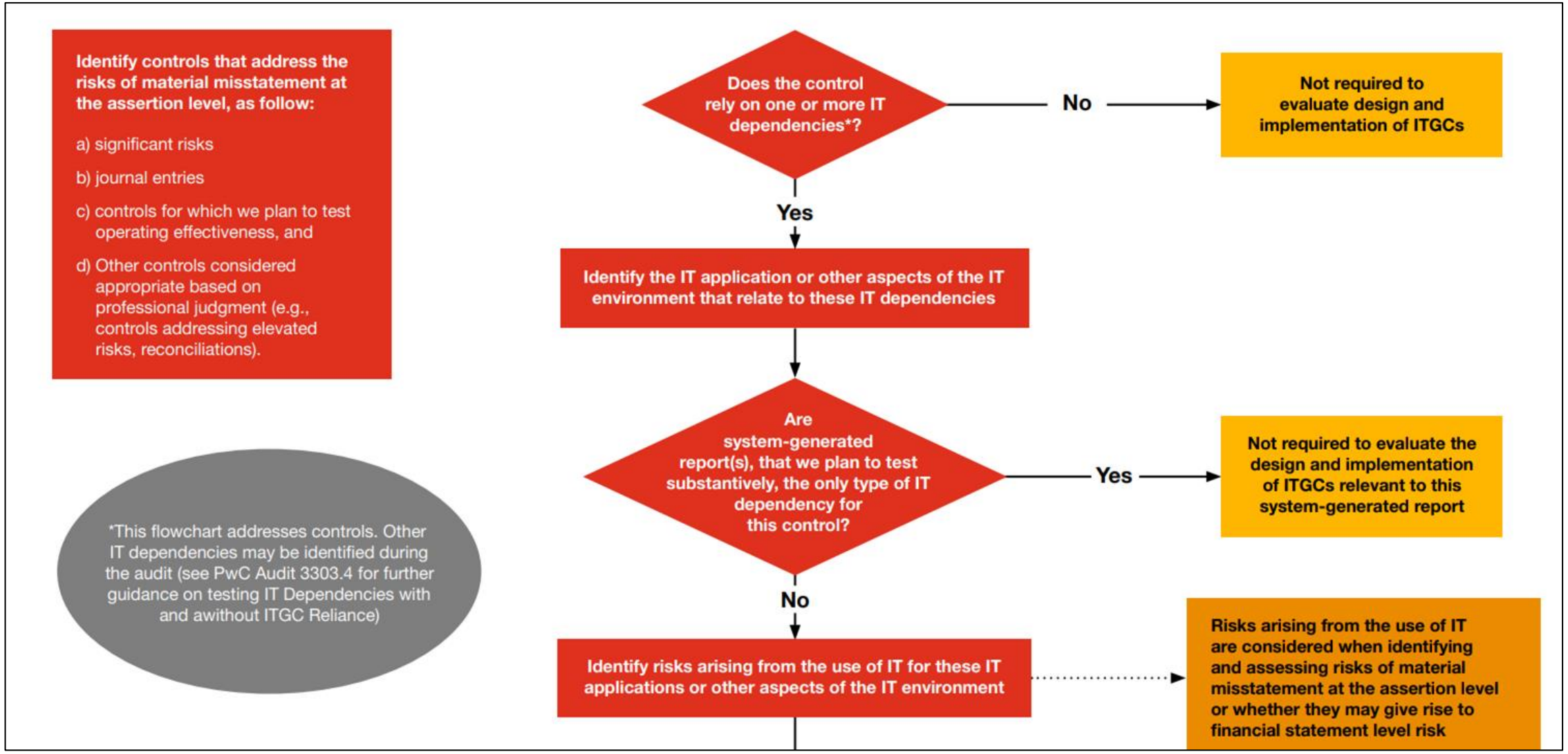
Calculations are accounting procedures that are performed by an IT system instead of a person.



Automated controls are designed into the IT environment to enforce business rules. For example, many IT applications include format checks

System generated reports are information generated by IT systems and are often used in the execution of manual and automated controls, including business performance reviews, or as supporting documents for substantive audit tests.

Identify when to assess design and implementation of ITCGs related to controls



ITGCs that address the risk arising from the use of IT

In identifying ITGCs that address IT risks we consider the following 4 domains:

Access to programs and data

The domain objective is to ensure that only authorized access is granted to the IT applications and other aspects of the IT environment upon authentication of a user's identity. Controls over access include the processes used by the entity to add, delete, and change users and their related access rights according to the control objectives established in the design of the control.

The domain objective is to ensure that changes to the IT application and other aspects of the IT environment are requested, authorized, performed, tested, and implemented to achieve management's IT control objectives.

Program change

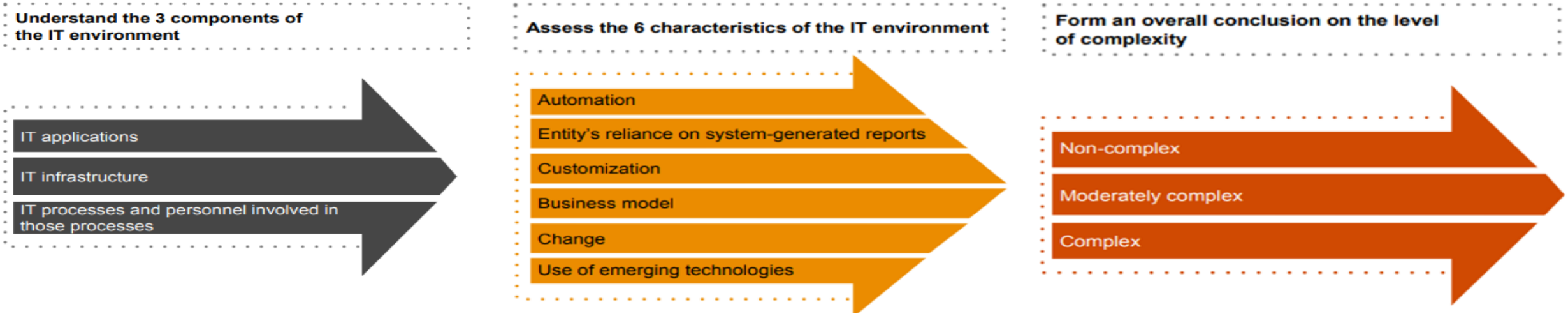
Program development

The domain objective is to ensure that IT applications and other aspects of the IT environment are developed, configured, and implemented to achieve management's control objectives. This includes development or acquisition or implementation controls and data conversion controls.

The domain objective is to ensure that information in the IT applications and other aspects of the IT environment is processed completely and accurately in accordance with management's control objectives, and that processing problems are identified and resolved completely and accurately to maintain the integrity of financial data.

Computer operations

Formulation of conclusion on the "Complexity of IT Environment"



Overall Assessment

Characteristics/ Criteria	Non Complex	Complex
Automation	An entity using low levels of automation with very simple calculations and simple data inputs that can be verified manually	Entities with highly automated complex calculations with a large number of data inputs and more than one operating system
Entity's reliance on system generated reports	An entity relying on standard reports with simple data inputs that can be verified manually or manual data input	An entity with in-house ability to create custom reports, with large numbers of data inputs and transactions or data pulled from more than one system or application
Use of emerging technologies	An entity not using emerging technology	An entity, using an Artificial Intelligence, Robotics Process Automation (RPA), Blockchain or other new and emerging software
Customisation	An entity using standard commercial software with no, or minor modification, employs a limited number of interfaces between systems, databases or applications and has consistent IT controls and staff to manage changes	An entity using a complex ERP with significant customization (e.g., SAP customized to address an entity-specific needs), has a large number of customised interfaces between systems, databases or applications)
Business model	Non- complex business entity, Low level of reliance on technology, Manual business operations with limited reliance on technology, Limited volume of documentation only available in electronic form, purchased or vendor supported firewalls, Mature software and hardware, low cybersecurity risks	Complex or sophisticated business, Business operations heavily rely on technology, Complex operations that requires automation, Significant participation in electronic commerce, Significant volume of documentation only in electronic form, High level of complexity and configuration for firewalls, Higher cybersecurity risks
Change	Low extent and frequency of changes within the IT environment	High extent and frequency of changes within the IT environment

Other IT Risk Assessment

Understand whether the entity's risk assessment process considers Entity Level Controls (ELCs) and other IT risk which are specific to the entity.

- Understand how the entity's risk assessment process considers cybersecurity.
- Understand the entity's established roles and responsibilities over cybersecurity, such as Chief Information Security Officer (CISO), CIO, or Cybersecurity Risk Officer.
- Understand the entity's process for safeguarding material digital/electronic assets that are included on its balance sheet and subject to cybersecurity risk and management's process for identifying these assets and prioritizing their protection.
- Understand the entity's controls and procedures to monitor and detect security breaches or incidents.

Documentation- Strengthened documentation requirements relating to the exercise of professional skepticism

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.

Below mentioned are the documentation which generally needs to be checked:

-Identify IT risks and understand and evaluate related ITGCs

-Understand and assess complexity of the entity's IT environment

Questions?

Thank You