ISA 315 (Revised)¹ – Appendices to the Standard

This paper sets out:

- Proposed revisions in mark-up to the appendices as presented in Exposure Draft ISA 315 (Revised) (ED–315)²:
  - Appendix 1: Considerations for understanding the entity and its business model.
  - Appendix 2: Inherent risk factors (previously "events and conditions that may indicate susceptibility to risks of material misstatement").
  - Appendix 3: Understanding the entity’s system of internal control

- Proposed new appendices:
  - Appendix 4: Internal audit
  - Appendix 5: Information technology

- Appendix 6 - Appendix 4 as presented in ED–315 (Considerations for understanding general IT controls) has been re-numbered as Appendix 6.

Changes shown as marked within this document include:

- Paragraphs moved from the application material (the relevant application material paragraph number has been indicated). If there have been no changes to the words within the paragraph then the mark-up has been ‘hard-coded’ – i.e., appears in black (underlined or strike-through as relevant). The only exception is Appendix 5.

- Changes to address comments from ED-315 or because some of the content may now be repetitive because of the moves from the application material. These changes are shown as true mark-ups (i.e. in color).

Although some changes have been shown to the existing and new Appendices, and paragraphs from the Application Material variously combined into the existing or new Appendices, it is the intention of the Task Force to revisit the Appendices before targeted finalization of ISA 315 (Revised) in September 2019.

---

¹ ISA 315 (Revised), Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment

² Proposed ISA 315 (Revised), Identifying and Assessing the Risks of Material Misstatement

Prepared by: Bev Bahlmann and Phil Minnaar (May 2019)
Considerations for Understanding the Entity and its Business Model

The appendix provides further explains the objectives and scope of the entity’s business model and provides examples of matters that the auditor may consider in understanding the activities of the entity that may be included in the entity and its business model. The auditor’s understanding of the entity’s business model, and how it is affected by its business strategy and business objectives, may assist the auditor in identifying business risks that are relevant to the audit. In addition, this may assist the auditor in identifying risks of material misstatement.

Objectives and Scope of an Entity’s Business Model

1. **[Moved from para. A53 of ED–315]** An entity’s business model describes how an entity considers, for example its organizational structure, operations or scope of activities, business lines (including competitors and customers thereof), processes, growth opportunities, globalization, regulatory requirements and technologies. The entity’s business model describes how the entity creates, preserves and captures financial or broader value, such as public benefits, for its stakeholders.

2. **[Moved from para. A54 of ED–315]** Strategies are the approaches by which management plans to achieve the entity’s objectives, including how the entity plans to address the risks and opportunities that it faces. An entity’s strategies are changed over time by management, to respond to changes in its objectives and in the internal and external circumstances in which it operates.

3. **[Moved from para. A55 of ED–315]** A description of a business model typically includes:
   - The scope of the entity’s activities, and why it does them.
   - The entity's structure and scale of its operations.
   - The markets or geographical or demographic spheres, and parts of the value chain, in which it operates, how it engages with those markets or spheres (main products, customer segments and distribution methods), and the basis on which it competes.
   - The entity’s business or operating processes (e.g., investment, financing and operating processes) employed in performing its activities, focusing on those parts of the business processes that are important in creating, preserving or capturing value.
   - The resources (e.g., financial, human, intellectual, environmental and technological) and other inputs and relationships (e.g., customers, competitors, suppliers and employees) that are necessary or important to its success.
   - How the entity’s business model integrates the use of IT in its interactions with customers, suppliers, lenders and other stakeholders through IT interfaces and other technologies.
4. **Moved from para. A60 of ED–315** A business risk may have an immediate consequence for the risk of material misstatement for classes of transactions, account balances, and disclosures at the assertion level or the financial statement level. For example, the business risk arising from a significant fall in real estate market values may increase the risk of material misstatement associated with the valuation assertion for a lender of medium-term real estate backed loans. However, the same risk, particularly in combination with a severe economic downturn that concurrently increases the underlying risk of lifetime credit losses on its loans, may also have a longer-term consequence. The resulting net exposure to credit losses may cast significant doubt on the entity’s ability to continue as a going concern. If so, this could have implications for management’s and the auditor’s conclusion as to the appropriateness of the entity’s use of the going concern basis of accounting and determination as to whether a material uncertainty exists. Whether a business risk may result in a risk of material misstatement is, therefore, considered in light of the entity’s circumstances. Examples of events and conditions that may indicate risks of material misstatement are indicated in Appendix 2.

**Activities of the Entity**

45. Examples of matters that the auditor may consider when obtaining an understanding of the activities of the entity (included in the entity’s business model) include:

(a) Business operations such as:

- Nature of revenue sources, products or services, and markets, including involvement in electronic commerce such as Internet sales and marketing activities.
- Conduct of operations (for example, stages and methods of production, or activities exposed to environmental risks).
- Alliances, joint ventures, and outsourcing activities.
- Geographic dispersion and industry segmentation.
- Location of production facilities, warehouses, and offices, and location and quantities of inventories.
- Key customers and important suppliers of goods and services, employment arrangements (including the existence of union contracts, pension and other post-employment benefits, stock option or incentive bonus arrangements, and government regulation related to employment matters).
- Research and development activities and expenditures.
- Transactions with related parties.

(b) Investments and investment activities such as:

- Planned or recently executed acquisitions or divestitures.
- Investments and dispositions of securities and loans.
- Capital investment activities.
(c) Financing and financing activities such as:

- Investments in non-consolidated entities, including partnerships, joint ventures and special-purpose entities.
- Major subsidiaries and associated entities, including consolidated and non-consolidated structures.
- Debt structure and related terms, including off-balance-sheet financing arrangements and leasing arrangements.
- Beneficial owners (local, foreign, business reputation and experience) and related parties.
- Use of derivative financial instruments.

**Nature of Special-Purpose Entities**

26. A special-purpose entity (sometimes referred to as a special-purpose vehicle) is an entity that is generally established for a narrow and well-defined purpose, such as to effect a lease or a securitization of financial assets, or to carry out research and development activities. It may take the form of a corporation, trust, partnership or unincorporated entity. The entity on behalf of which the special-purpose entity has been created may often transfer assets to the latter (for example, as part of a derecognition transaction involving financial assets), obtain the right to use the latter’s assets, or perform services for the latter, while other parties may provide the funding to the latter. As ISA 550 indicates, in some circumstances, a special-purpose entity may be a related party of the entity.³

37. Financial reporting frameworks often specify detailed conditions that are deemed to amount to control, or circumstances under which the special-purpose entity should be considered for consolidation. The interpretation of the requirements of such frameworks often demands a detailed knowledge of the relevant agreements involving the special-purpose entity.

---

³ ISA 550, paragraph A7
Appendix 2

(Ref: Para. 16(f), A5, A48–A60, A83, A209)

Understanding the Inherent Risk Factors  Events and Conditions That May Indicate Susceptibility to Risks of Material Misstatement

The appendix provides further explanation about the inherent risk factors as well as matters that the auditor may consider in understanding and applying the inherent risk factors in identifying and assessing the risks of material misstatement at the assertion level.

The Inherent Risk Factors

1. The inherent risk factors are 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. In obtaining the understanding of the entity and its environment and the applicable financial reporting framework in accordance with paragraph 23(a) and (b), the auditor considers whether and, if so, how events and conditions are subject to by, or affected by, the inherent risk factors.

2. [Moved from para. A5 of ED–315] Inherent risk factors relating to the preparation of information required by the applicable financial reporting framework (referred to in this paragraph as “required information”) include:
   - **Complexity**—arises either from the nature of the information or in the way that the required information is prepared, including when such preparation processes are more inherently difficult to apply. For example, complexity may arise:
     - In calculating supplier rebate provisions because it may be necessary to take into account different commercial terms with many different suppliers, or many interrelated commercial terms that are all relevant in calculating the rebates due; or
     - When there are many potential data sources, with different characteristics used in making an accounting estimate, the processing of that data involves many inter-related steps, and the data is therefore inherently more difficult to identify, capture, access, understand or process.
   - **Subjectivity**—arises from inherent limitations in the ability to prepare required information in an objective manner, due to limitations in the availability of knowledge or information, such that management may need to make an election or subjective judgment about the appropriate approach to take and about the resulting information to include in the financial statements. Because of different approaches to preparing the required information, different outcomes could result from appropriately applying the requirements of the applicable financial reporting framework. As limitations in knowledge or data increase, the subjectivity in the judgments that could be made by reasonably knowledgeable and independent individuals, and the diversity in possible outcomes of those judgments will also increase.
• **Change**—results from events or conditions that, over time, affect the entity’s business or the economic, accounting, regulatory, industry or other aspects of the environment in which it operates, when the effects of those events or conditions are reflected in the required information. Such events or conditions may occur during, or between, financial reporting periods. For example, change may result from developments in the requirements of the applicable financial reporting framework, or in the entity and its business model, or in the environment in which the entity operates. Such change may affect management’s assumptions and judgments, including as they relate to management’s selection of accounting policies or how accounting estimates are made or related disclosures are determined.

• **Uncertainty**—arises when the required information cannot be prepared based only on sufficiently precise and comprehensive data that is verifiable through direct observation. In these circumstances, an approach may need to be taken that applies the best available knowledge to prepare the information using sufficiently precise and comprehensive observable data, to the extent available, and reasonable assumptions supported by the best available data, when it is not. Constraints on the availability of knowledge or data, which are not within the control of management (subject to cost constraints where applicable) are sources of uncertainty and their effect on the preparation of the required information cannot be eliminated. For example, estimation uncertainty arises when the required monetary amount cannot be determined with precision and the outcome of the estimate is not known before the date the financial statements are finalized.

• **Susceptibility to misstatement due to management bias or misappropriation of assets**—results from conditions that create susceptibility to intentional or unintentional failure by management to maintain neutrality in preparing the information. Management bias is often associated with certain conditions that have the potential to give rise to management not maintaining neutrality in exercising judgment (indicators of potential management bias), which could lead to a material misstatement of the information that would be fraudulent if intentional. Such indicators include inherent incentives or pressures (for example, as a result of motivation to achieve a desired result, such as a desired profit target or capital ratio), and opportunity, not to maintain neutrality. Factors relevant to the susceptibility to misstatement due to fraud management bias that could result in susceptibility to fraud in the form of fraudulent financial reporting or misappropriation of assets for assertions about classes of transactions, account balances and disclosures, are described in paragraphs A1 to A5 of ISA 240.

3. **[Moved from A86 of ED – 315]** When complexity is an inherent risk factor, there may be an inherent need for more complex processes in preparing the information, and such processes may be inherently more difficult to apply. As a result, applying them may require specialized skills or knowledge, and may require the use of a management’s expert. For example, when there are many potential data sources, with different characteristics, and the processing of that data involves many interrelated steps, the data may be inherently more difficult to identify, capture, access, understand or process.

4. **[Moved from A87 of ED – 315]** When management judgment is more subjective, the susceptibility to misstatement due to management bias, whether unintentional or intentional, may also increase. For example, significant management judgment may be involved in making accounting estimates that
Examples of Events or Conditions that May Indicate the Existence of Risks of Material Misstatement

6. The following are examples of events and conditions that may indicate the existence of risks of material misstatement in the financial statements, either at the financial statement level or the assertion level. The examples provided by inherent risk factor cover a broad range of events and conditions; however, not all events and conditions are relevant to every audit engagement and the list of examples is not necessarily complete. The events and conditions have been categorized by the inherent risk factor that may have the greatest effect in the circumstances. Importantly, due to the interrelationships among the inherent risk factors, the example events and conditions also are likely to be subject to, or affected by, other inherent risk factors to varying degrees.

Inherent Risk Factors at the Assertion Level

Complexity:
<table>
<thead>
<tr>
<th>Relevant Inherent Risk Factor:</th>
<th>Examples of Events and Conditions That May Indicate the Existence of Risks of Material Misstatement at the Assertion Level:</th>
</tr>
</thead>
</table>
| **Complexity**                | Regulatory:  
|                               | • Operations that are subject to a high degree of complex regulation.  
|                               | Business model:  
|                               | • The existence of complex alliances and joint ventures.  
|                               | Applicable financial reporting framework:  
|                               | • Accounting measurements that involve complex processes.  
|                               | Transactions:  
|                               | • Use of off-balance sheet finance, special-purpose entities, and other complex financing arrangements.  
| **Subjectivity**              | Applicable financial reporting framework:  
|                               | • A wide range of possible measurement criteria of an accounting estimate. For example, management’s recognition of depreciation or construction income and expenses.  
|                               | • Management’s selection of a valuation technique or model for a non-current asset, such as investment properties.  
| **Change**                    | Economic conditions:  
|                               | • Operations in regions that are economically unstable, for example, countries with significant currency devaluation or highly inflationary economies.  
|                               | Markets:  
|                               | • Operations exposed to volatile markets, for example, futures trading.  
|                               | Customer loss:  
|                               | • Going concern and liquidity issues including loss of significant customers.  
|                               | Industry model:  
|                               | • Changes in the industry in which the entity operates.  
|                               | Business model:  
|                               | • Changes in the supply chain.  
|                               | • Developing or offering new products or services, or moving into new lines of business.  
|                               | Geography:  
|                               | • Expanding into new locations.  

<table>
<thead>
<tr>
<th>Entity structure:</th>
<th>Reporting:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Changes in the entity such as large acquisitions or reorganizations or other</td>
<td>- Opportunities for management and employees to engage in fraudulent financial reporting,</td>
</tr>
<tr>
<td>unusual events.</td>
<td>including omission, or obscuring, of significant information in disclosures.</td>
</tr>
<tr>
<td>- Entities or business segments likely to be sold.</td>
<td></td>
</tr>
<tr>
<td>Human resources competence:</td>
<td>Transactions:</td>
</tr>
<tr>
<td>- Changes in key personnel including departure of key executives.</td>
<td>- Significant transactions with related parties.</td>
</tr>
<tr>
<td>IT:</td>
<td>- Significant amount of non-routine or non-systematic transactions including</td>
</tr>
<tr>
<td></td>
<td>intercompany transactions and large revenue transactions at period end.</td>
</tr>
<tr>
<td></td>
<td>- Transactions that are recorded based on management’s intent, for example,</td>
</tr>
<tr>
<td></td>
<td>debt refinancing, assets to be sold and classification of marketable securities.</td>
</tr>
<tr>
<td>Applicable financial reporting framework:</td>
<td></td>
</tr>
<tr>
<td>- Application of new accounting pronouncements.</td>
<td></td>
</tr>
<tr>
<td>Reporting:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Establishments in the operations or financial results by regulatory or government bodies.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Susceptibility to misstatement due to management bias and the misappropriation of assets.**
Change:

Uncertainty:

Susceptibility to misstatement due to management bias or fraud:

Other Inherent Risk Factors

• Constraints on the availability of capital and credit. [Moved to table: ‘change’]
• Inconsistencies between the entity’s IT strategy and its business strategies. [Deleted]
• Investigations into the entity’s operations or financial results by regulatory or government bodies. [Moved to table: ‘change’]

Other events or conditions that may indicate risks of material misstatement at the financial statement level:

• Lack of personnel with appropriate accounting and financial reporting skills.
• Control deficiencies, especially those not addressed by management.
• Past misstatements, history of errors or a significant amount of adjustments at period end.
Appendix 3

U n d e r s t a n d i n g t h e E n t i t y ’ s S y s t e m o f I n t e r n a l C o n t r o l

1. [Moved from para. A11 of ED–315] The entity’s system of internal control may be reflected in policy and procedures manuals, systems and forms, and the information embedded therein, and is effected by people. The system of internal control is implemented by management, those charged with governance, and other personnel based on the structure of the entity. The system of internal control can be applied, based on the decisions of management, those charged with governance and other personnel and in the context of legal or regulatory requirements, to the operating model of the entity, the legal entity structure, or a combination of these.

12. This appendix further explains the components of, as well as the limitations of, the entity’s system of internal control as set out in paragraphs 16(lf), 27–38, A51, A9\textsuperscript{3a}2, and A105–A165, as they relate to a financial statement audit.

Components of the System of Internal Control

Control Environment

3. [Moved from para. A105 of ED–315] The control environment includes the governance and management functions and the attitudes, awareness, and actions of those charged with governance and management concerning the entity’s system of internal control and its importance in the entity. The control environment sets the tone of an organization, influencing the control consciousness of its people.

4. [Moved from para. A112 (part) of ED–315] An entity’s control consciousness is influenced by those charged with governance, because one of their roles is to counterbalance pressures on management in relation to financial reporting that may arise from market demands or remuneration schemes. The effectiveness of the design of the control environment in relation to participation by those charged with governance is therefore influenced by such matters as:

- Their independence from management and their ability to evaluate the actions of management.
- Whether they understand the entity’s business transactions.
- The extent to which they evaluate whether the financial statements are prepared in accordance with the applicable financial reporting framework, including whether the financial statements include adequate disclosures.

25. The control environment encompasses the following elements:

(a) How the entity demonstrates a commitment to integrity and ethical values. The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical behavior are the product of the entity’s
ethical and behavioral standards or codes of conduct, how they are communicated (e.g., through policy statements), and how they are reinforced in practice (e.g., through management actions to eliminate or mitigate incentives or temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts). The communication of entity policies on integrity and ethical values may include the communication of behavioral standards to personnel through policy statements and codes of conduct and by example.

(b) How those charged with governance demonstrate independence from management and exercise oversight of the entity’s system of internal control. An entity’s control consciousness is influenced significantly by those charged with governance. Considerations include whether there are sufficient individuals who are independent from management and objective in their evaluations and decision-making; how those charged with governance identify and accept oversight responsibilities and whether those charged with governance retain oversight responsibility for management’s design, implementation and conduct of the entity’s system of internal control. The importance of the responsibilities of those charged with governance is recognized in codes of practice and other laws and regulations or guidance produced for the benefit of those charged with governance. Other responsibilities of those charged with governance include oversight of the design and effective operation of whistle blower procedures.

(c) How the entity has established, with oversight from those charged with governance, structures, reporting lines, and appropriate authorities and responsibilities in pursuit of its objectives. This includes considerations about:

- Key areas of authority and responsibility and appropriate lines of reporting;
- Policies relating to appropriate business practices, knowledge and experience of key personnel, and resource provided for carrying out duties; and
- Policies and communications directed at ensuring that all personnel understand the entity’s objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

The appropriateness of an entity’s organizational and governance structure depends, in part, on its size and the nature of its activities.

(d) How the entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with its objectives. This includes how the entity ensures the individuals have the knowledge and skills necessary to accomplish the tasks that define the individual’s job, such as:

- Standards for recruiting the most qualified individuals – with an emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior.
- Training policies that communicate prospective roles and responsibilities, including practices such as training schools and seminars that illustrate expected levels of performance and behavior; and
• Periodic performance appraisals driving promotions that demonstrate the entity’s commitment to the advancement of qualified personnel to higher levels of responsibility.

(e) How the entity holds individuals accountable for their internal control responsibilities in pursuit of its objectives. This may be accomplished through, for example:

• Mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities and implement corrective actions as necessary;
• Establishing performance measures, incentives and rewards for those responsible for internal control, including how the measures are evaluated and maintain their relevance;
• How pressures associated with the achievement of internal control objectives impact the individual’s responsibilities and performance measures; and
• How the individuals are disciplined as necessary.

The appropriateness of the above matters will be different for every entity depending on its size, the complexity of its structure and the nature of its activities.

Entity’s Risk Assessment Process

6. [Moved from para. A115 from ED–315] The entity’s risk assessment process is an iterative process for identifying and analyzing risks to achieving the entity’s objectives, and forms the basis for how management or those charged with governance determine the risks to be managed.

37. For financial reporting purposes, the entity’s risk assessment process includes how management identifies business risks relevant to the preparation of financial statements in accordance with the entity’s applicable financial reporting framework, estimates their significance, assesses the likelihood of their occurrence, and decides upon actions to respond to and manage them and the results thereof. For example, the entity’s risk assessment process may address how the entity considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements.

48. Risks relevant to reliable financial reporting include external and internal events, transactions or circumstances that may occur and adversely affect an entity’s ability to initiate, record, process, and report financial information consistent with the assertions of management in the financial statements. Management may initiate plans, programs, or actions to address specific risks or it may decide to accept a risk because of cost or other considerations. Risks can arise or change due to circumstances such as the following:

• Changes in operating environment. Changes in the regulatory, economic or operating environment can result in changes in competitive pressures and significantly different risks.
• New personnel. New personnel may have a different focus on or understanding of the system of internal control.
• New or revamped information system. Significant and rapid changes in the information system can change the risk relating to the entity’s system of internal control.
• **Rapid growth.** Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls.

• **New technology.** Incorporating new technologies into production processes or the information system may change the risk associated with the entity’s system of internal control.

• **New business models, products, or activities.** Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with the entity’s system of internal control.

• **Corporate restructurings.** Restructurings may be accompanied by staff reductions and changes in supervision and segregation of duties that may change the risk associated with the entity’s system internal control.

• **Expanded foreign operations.** The expansion or acquisition of foreign operations carries new and often unique risks that may affect internal control, for example, additional or changed risks from foreign currency transactions.

• **New accounting pronouncements.** Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.

• **Use of IT.** Risks relating to:
  
  o Maintaining the integrity of data and information processing (including cyber security risks);
  
  o Risks to the entity business strategy that arise if the entity’s IT strategy does not effectively supporting the entity’s business strategy; or
  
  o Changes or interruptions in the entity’s IT environment or turnover of IT personnel or when the entity does not make necessary updates to the IT environment or such updates are not timely.

**The Entity’s Process to Monitor the System of Internal Control**

9. [Moved from para. A122 of ED–315] The entity’s process to monitor the system of internal control is a continuous process to evaluate the effectiveness of the system of internal control and to take necessary remedial actions on a timely basis. The entity’s process to monitor the system of internal controls may consist of ongoing activities, separate evaluations (conducted periodically), or some combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of an entity and include regular management and supervisory activities. The entity’s process will likely vary in scope and frequency depending on the assessment of the risks by the entity.

510. [Deletions - duplicative of the new para. 9] An important management responsibility is to establish and maintain the entity’s system of internal control on an ongoing basis. Management’s process to monitor the system of internal control includes considering whether controls are operating as intended and that they are modified as appropriate 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. Monitoring is done also to ensure that controls continue to operate effectively over time. For example, if the timeliness and accuracy of bank reconciliations are not monitored, personnel are likely to stop preparing them.

11. **Moved from para. A128 of ED–315** Controls within the entity’s process to monitor the system of internal control, including those that monitor underlying automated controls, may be automated or manual, or a combination of both. For example, an entity may use automated monitoring controls over access to certain technology with automated reports of unusual activity to management, who manually investigate identified anomalies.

612. When distinguishing between a monitoring activity and a control in the control activities component, the underlying details of the activity are considered, especially where the activity involves some level of supervisory review. As also explained in the application material, supervisory reviews are not automatically classified as monitoring activities and it may be a matter of judgment whether a review is classified as a control in the control activities component or a monitoring activity. For example, the intent of a monthly completeness control in the control activities component would be to detect and correct errors, where a monitoring activity would ask why errors are occurring and assign management the responsibility of fixing the process to prevent future errors. In simple terms, a control in the control activities component responds to a specific risk, whereas a monitoring activity assesses whether controls within each of the five components of the system of internal control are operating as intended.

713. Monitoring activities may include using information from communications from external parties that may indicate problems or highlight areas in need of improvement. Customers implicitly corroborate billing data by paying their invoices or complaining about their charges. In addition, regulators may communicate with the entity concerning matters that affect the functioning of the system of internal control, for example, communications concerning examinations by bank regulatory agencies. Also, management may consider in performing monitoring activities any communications relating to the system of internal control from external auditors.

Use of internal audit

8. **Moved to new Appendix 4**

The objectives and scope of an internal audit function, the nature of its responsibilities and its status within the organization, including the function's authority and accountability, vary widely and depend on the size and structure of the entity and the requirements of management and, where applicable, those charged with governance. These matters may be set out in an internal audit charter or terms of reference.

9. **Moved to new Appendix 4**

The responsibilities of an internal audit function may include performing procedures and evaluating the results to provide assurance to management and those charged with governance regarding the design and effectiveness of risk management, the system of internal control and governance processes. If so, the internal audit function may play an important role in the entity’s process to monitor the system of internal control. However, the responsibilities of the internal audit function may
be focused on evaluating the economy, efficiency and effectiveness of operations and, if so, the work of the function may not directly relate to the entity’s financial reporting.

The Information System and Communication

4014. [Moved from para. A136 of ED–315] The information system relevant to financial reporting consists of the policies or procedures, and records, designed and established to:

- Initiate, record, process, and report entity transactions (as well as to capture, process and disclose information about events and conditions other than transactions) and to maintain accountability for the related assets, liabilities, and equity;
- Resolve incorrect processing of transactions, for example, automated suspense files and procedures followed to clear suspense items out on a timely basis;
- Process and account for system overrides or bypasses to controls;
- Incorporate information from transaction processing in the general ledger (e.g., transferring of accumulated transactions from a subsidiary ledger);
- Capture and process information relevant to financial reporting for events and conditions other than transactions, such as the depreciation and amortization of assets and changes in the recoverability of assets; and
- Ensure information required to be disclosed by the applicable financial reporting framework is accumulated, recorded, processed, summarized and appropriately reported in the financial statements.

10. [Deleted – duplicative of new para. 14] The information system relevant to financial reporting encompasses policies, procedures and records that:

- Identify and record all valid transactions.
- Describe on a timely basis the transactions in sufficient detail to permit proper classification of transactions for financial reporting.
- Measure the value of transactions in a manner that permits recording their proper monetary value in the financial statements.
- Determine the time period in which transactions occurred to permit recording of transactions in the proper accounting period.
- Present properly the transactions and related disclosures in the financial statements.
- Capture, process and disclose information about events and conditions other than transactions.

15. [Moved from part of A137 of ED–315] An entity’s business processes include the activities designed to:

- Develop, purchase, produce, sell and distribute an entity’s products and services;
- Ensure compliance with laws and regulations; and
- Record information, including accounting and financial reporting information.
Business processes result in the transactions that are recorded, processed and reported by the information system.

416. The quality of the information affects management’s ability to make appropriate decisions in managing and controlling the entity’s activities and to prepare reliable financial reports.

4217. Communication, which involves providing an understanding of individual roles and responsibilities pertaining to the entity’s system of internal control, may take such forms as policy manuals, accounting and financial reporting manuals, and memoranda. Communication also can be made electronically, orally, and through the actions of management.

18. [Moved from para. A158 of ED–315] Communication by the entity of the financial reporting roles and responsibilities and of significant matters relating to financial reporting involves providing an understanding of individual roles and responsibilities pertaining to the system of internal control relevant to financial reporting. It may include such matters as the extent to which personnel understand how their activities in the information system relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity.

Control Activities

4319. Controls in the control activities component consist of application controls and general IT controls, both of which may be manual or automated in nature. [Moved from para. A163 of ED–315] The greater the extent of automated controls, or controls involving automated aspects, that management uses and relies on in relation to its financial reporting, the more important it may become for the entity to implement general IT controls that address the continued functioning of the automated aspects of application information processing controls. Control activities and may pertain to the following:

- **Authorization and approvals.** An authorization affirms that a transaction is valid (i.e. it represents an actual economic event or is within an entity’s policy). An authorization typically takes the form of an approval by a higher level of management or of verification and a determination if the transaction is valid. For example, a supervisor approves an expense report after reviewing whether the expenses seem reasonable and within policy. An example of an automated approval is where an invoice unit cost is automatically compared with the related purchase order unit cost within a pre-established tolerance level. Invoices within the tolerance level are automatically approved for payment. Those invoices outside the tolerance level are flagged for additional investigation.

- **Reconciliations** – Reconciliations compare two or more data elements and, if differences are identified, action is taken to bring the data into agreement. Reconciliations generally address the completeness or accuracy of processing transactions.

- **Verifications** – Verifications compare two or more items with each other or compare an item with a policy, and perform a follow-up action when the two items do not match or the item is not consistent with policy. Verifications generally address the completeness, accuracy, of validity of processing transactions.

- **Physical or logical controls,** including those that address security of assets against unauthorized access, acquisition, use or disposal. Controls that encompass:
The physical security of assets, including adequate safeguards such as secured facilities over access to assets and records.

The authorization for access to computer programs and data files (i.e., logical access).

The periodic counting and comparison with amounts shown on control records (for example, comparing the results of cash, security and inventory counts with accounting records).

The extent to which physical controls intended to prevent theft of assets are relevant to the reliability of financial statement preparation depends on circumstances such as when assets are highly susceptible to misappropriation.

- **Segregation of duties.** Assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets. Segregation of duties is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud in the normal course of the person's duties.

For example, a manager authorizing credit sales is not responsible for maintaining accounts receivable records or handling cash receipts. If one person is able to perform all these activities he or she could, for example, create a fictitious sale that could go undetected. Similarly, salespersons should not have the ability to modify product price files or commission rates.

Sometimes segregation is not practical, cost effective, or feasible. For example, smaller and less complex entities may lack sufficient resources to achieve ideal segregation, and the cost of hiring additional staff may be prohibitive. In these situations, management institutes alternative controls. In the example above, if the salesperson can modify product price files, a detective control activity can be put in place to have personnel unrelated to the sales function periodically review whether and under what circumstances the salesperson changed prices.

---

**Benefits of IT**

45. [Moved to (IT) Appendix 5] Generally, IT benefits an entity's system of internal control by enabling an entity to:

- Consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data;

- Enhance the timeliness, availability, and accuracy of information;

- Facilitate the additional analysis of information;

- Enhance the ability to monitor the performance of the entity's activities and its policies and procedures;
• Reduce the risk that controls will be circumvented; and

• Enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems.

Limitations of Internal Control

1621. Internal control, no matter how effective, can provide an entity with only reasonable assurance about achieving the entity’s financial reporting objectives. The likelihood of their achievement is affected by the inherent limitations of internal control. These include the realities that human judgment in decision-making can be faulty and that breakdowns in internal control can occur because of human error. For example, there may be an error in the design of, or in the change to, a control. Equally, the operation of a control may not be effective, such as where information produced for the purposes of the system of internal control (for example, an exception report) is not effectively used because the individual responsible for reviewing the information does not understand its purpose or fails to take appropriate action.

4722. Additionally, controls can be circumvented by the collusion of two or more people or inappropriate management override of internal control. For example, management may enter into side agreements with customers that alter the terms and conditions of the entity’s standard sales contracts, which may result in improper revenue recognition. Also, edit checks in an IT application that are designed to identify and report transactions that exceed specified credit limits may be overridden or disabled.

1823. Further, in designing and implementing controls, management may make judgments on the nature and extent of the controls it chooses to implement, and the nature and extent of the risks it chooses to assume.
Appendix 4 is a NEW Appendix on internal audit activities of the client.

Given that the consideration of internal audit activities is only relevant for entities with an internal audit department (or similar), the Task Force has proposed to move selected material in the application material to an appendix. The Task Force is also of the view that this would be helpful in reducing the length of the application material for entities where internal audit is not relevant.

Guidance included in the proposed appendix is existing application material in ED–315 that was moved to this appendix as noted below (presented in mark-up).

Considerations for Understanding Internal Audit

This appendix provides further matters relating to internal audit.

Objectives and Scope of the Internal Audit Function

1. **Moved from Appendix 3 of ED–315: Para. 8** The objectives and scope of an internal audit function, the nature of its responsibilities and its status within the organization, including the function’s authority and accountability, vary widely and depend on the size and structure of the entity and the requirements of management and, where applicable, those charged with governance. These matters may be set out in an internal audit charter or terms of reference.

2. **Moved from Appendix 3 of ED–315: Para. 9** The responsibilities of an internal audit function may include performing procedures and evaluating the results to provide assurance to management and those charged with governance regarding the design and effectiveness of risk management, the system of internal control and governance processes. If so, the internal audit function may play an important role in the entity’s process to monitor the system of internal control. However, the responsibilities of the internal audit function may be focused on evaluating the economy, efficiency and effectiveness of operations and, if so, the work of the function may not directly relate to the entity’s financial reporting.

Inquiries of the Internal Audit Function

3. **Moved from A25 of ED–315** If an entity has an internal audit function, inquiries of the appropriate individuals within the function may provide information that is useful to the auditor in obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the entity’s system of internal control, and in identifying and assessing risks of material misstatement at the financial statement and assertion levels. In performing its work, the internal audit function is likely to have obtained insight into the entity’s operations and business risks, and may have findings based on its work, such as identified control deficiencies or risks, that may provide valuable input into the auditor’s understanding of the entity and its environment, the applicable financial reporting framework and the system of internal control, the auditor’s risk assessments or other aspects of the audit. The auditor’s inquiries are therefore made whether or not the auditor expects to use the work of the
internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed. Inquiries of particular relevance may be about matters the internal audit function has raised with those charged with governance and the outcomes of the function’s own risk assessment process.

4. [Moved from A26 of ED–315] If, based on responses to the auditor’s inquiries, it appears that there are findings that may be relevant to the entity’s financial reporting and the audit, the auditor may consider it appropriate to read related reports of the internal audit function. Examples of reports of the internal audit function that may be relevant include the function’s strategy and planning documents and reports that have been prepared for management or those charged with governance describing the findings of the internal audit function’s examinations.

5. [Moved from A27 of ED–315] In addition, in accordance with ISA 240, if the internal audit function provides information to the auditor regarding any actual, suspected or alleged fraud, the auditor takes this into account in the auditor’s identification of risk of material misstatement due to fraud.

6. [Moved from A28 of ED–315] Appropriate individuals within the internal audit function with whom inquiries are made are those who, in the auditor’s judgment, have the appropriate knowledge, experience and authority, such as the chief internal audit executive or, depending on the circumstances, other personnel within the function. The auditor may also consider it appropriate to have periodic meetings with these individuals.

Consideration of the Internal Audit Function in Understanding the Control Environment

7. [Moved from para A109 of ED–315] The auditor may also consider how management has responded to the findings and recommendations of the internal audit function regarding identified control deficiencies relevant to the audit, including whether and how such responses have been implemented, and whether they have been subsequently evaluated by the internal audit function.

Understanding the Role that the Internal Audit Function Plays in the Entity’s Process to Monitor the System of Internal Control

8. [Moved from A132 of ED–315] If the nature of the internal audit function’s responsibilities and assurance activities are related to the entity’s financial reporting, the auditor may also be able to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed directly by the auditor in obtaining audit evidence. Auditors may be more likely to be able to use the work of an entity’s internal audit function when it appears, for example, based on experience in previous audits or the auditor’s risk assessment procedures, that the entity has an internal audit function that is adequately and appropriately resourced relative to the size of the entity and the nature of its operations, and has a direct reporting relationship to those charged with governance.

9. [Moved from A133 of ED–315] If, based on the auditor’s preliminary understanding of the internal audit function, the auditor expects to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed, ISA 610 (Revised 2013) applies.

---

4 The relevant requirements are contained in ISA 610 (Revised 2013).
5 ISA 240, paragraph 19
10. [Moved from A134 of ED–315] As is further discussed in ISA 610 (Revised 2013), the activities of an internal audit function are distinct from other monitoring controls that may be relevant to financial reporting, such as reviews of management accounting information that are designed to contribute to how the entity prevents or detects misstatements.

11. [Moved from A135 of ED–315] Establishing communications with the appropriate individuals within an entity’s internal audit function early in the engagement, and maintaining such communications throughout the engagement, can facilitate effective sharing of information. It creates an environment in which the auditor can be informed of significant matters that may come to the attention of the internal audit function when such matters may affect the work of the auditor. ISA 200 discusses the importance of the auditor planning and performing the audit with professional skepticism, including being alert to information that brings into question the reliability of documents and responses to inquiries to be used as audit evidence. Accordingly, communication with the internal audit function throughout the engagement may provide opportunities for internal auditors to bring such information to the auditor’s attention. The auditor is then able to take such information into account in the auditor’s identification and assessment of risks of material misstatement.
Appendix 5
(Ref: Para. 23(a), A97, A179a)

Appendix 5 is a new Appendix on Information Technology (IT) and was developed to provide further guidance in response to specific concerns raised by respondents, for example:

- Clarifying why the understanding of IT is required.
- Risks arising from IT – what is the nature of the such risks and in which circumstances are the auditor required to identify or evaluate GITCs?
- IT applications relevant to the audit – when are IT applications relevant to the audit, or alternatively, when are IT applications not relevant to the audit?

NOTE RE MARK-UP: Guidance included in the proposed appendix is either new material (mark-up), or existing application material included in ED–315 that were moved to this appendix (also presented in mark-up). This is different to the rest of this agenda item.

Considerations for Understanding Information Technology (IT)

The appendix provides further matters that the auditor may consider in understanding the entity’s use of IT in its system of internal control.

Understanding the Entity’s Use of Information Technology in the Components of the System of Internal Control

1. [Moved from para. A197 of ED–315] An entity’s system of internal control contains manual elements and automated elements (i.e., manual and automated controls and other resources used in the entity’s system of internal control). An entity’s mix of manual and automated elements in the entity’s system of internal control varies with the nature and complexity of the entity’s use of IT. An entity’s use of IT affects the manner in which the information relevant to financial reporting is processed, stored and communicated, and therefore affects the manner in which the system of internal control relevant to financial reporting is designed and implemented. Each component of the system of internal control may involve some extent of automation IT.

[Moved from Appendix 3 of ED–315: para 15]

Generally, IT benefits an entity’s system of internal control by enabling an entity to:

- Consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data;
- Enhance the timeliness, availability, and accuracy of information;
- Facilitate the additional analysis of information;
- Enhance the ability to monitor the performance of the entity’s activities and its policies and procedures;
• Reduce the risk that controls will be circumvented; and
• Enhance the ability to achieve effective segregation of duties by implementing security controls in IT applications, databases, and operating systems.

2. **[Moved from para. A98 of ED–315]** The characteristics of manual or automated elements are relevant to the auditor’s identification and assessment of the risks of material misstatement, and further audit procedures based thereon. Automated controls may be more reliable than manual controls because they cannot be as easily bypassed, ignored, or overridden, and they are also less prone to simple errors and mistakes. Automated controls may be more effective than manual controls in the following circumstances:

• High volume of recurring transactions, or in situations where errors that can be anticipated or predicted can be prevented, or detected and corrected, by control parameters that are automated through automation

• Controls where the specific ways to perform the control can be adequately designed and automated.

**Understanding the Entity’s Use of Information Technology in the Information System (Ref: Para. 35A)**

3. **[Moved from para. A138 of ED–315]** The entity’s information system relevant to financial reporting may include the use of manual and automated elements, which also affect the manner in which transactions are initiated, recorded, processed, and reported. In particular, procedures to initiate, record, process, and report transactions may be enforced through the IT applications used by the entity, and how the entity has configured those applications. In addition, records in the form of digital information may replace or supplement records in the form of paper documents.

4. **[Moved from para, A148 of ED–315, table also incorporates points made in A147]** Obtaining the auditor’s understanding of the IT environment in accordance with paragraph 35(d), and the auditor’s identification of IT applications and other aspects of the IT environment relevant to the audit in accordance with paragraph 40, may involve an iterative process or may be performed concurrently. Matters that may be relevant to the auditor’s understanding of the IT environment, or the determination of the aspects that are relevant to the audit, include matters such as: In obtaining an understanding of the IT environment relevant to the flows of transactions and information processing in the information system, the auditor gathers information about the nature and characteristics of the IT applications used, as well as the supporting IT infrastructure and IT. The following table includes examples of matters that the auditor may consider in obtaining the understanding of the IT environment and includes examples of typical characteristics of IT environments based on the complexity of IT applications used in the entity’s information system:

<table>
<thead>
<tr>
<th>Examples of typical characteristics of:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-complex commercial software</td>
</tr>
<tr>
<td>Mid-size and moderately complex</td>
</tr>
<tr>
<td>Large or complex IT applications (e.g., ERP systems)</td>
</tr>
</tbody>
</table>

---

Agenda Item 2-D
Page 24 of 35
### Matters related to extent of automation and use of data:

<table>
<thead>
<tr>
<th><strong>Commercial Software or IT Applications</strong></th>
<th><strong>Matters related to extent of automation and use of data:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>• The extent of automated procedures for processing, and the complexity of those procedures, including, whether there is highly automated, paperless processing</td>
</tr>
<tr>
<td>N/A</td>
<td>Simple automated report logic</td>
</tr>
<tr>
<td>N/A</td>
<td>Simple relevant automated report logic</td>
</tr>
<tr>
<td>Extensive and often complex automated procedures</td>
<td>Complex automated report logic: Report-writer software</td>
</tr>
<tr>
<td>Simple automated report logic</td>
<td>• The extent of the entity's reliance on system-generated reports in the processing of information.</td>
</tr>
<tr>
<td>Simple relevant automated report logic</td>
<td>Manual data inputs</td>
</tr>
<tr>
<td>Complex automated report logic: Report-writer software</td>
<td>Small number of data inputs or simple interfaces</td>
</tr>
<tr>
<td>Large number of data inputs or complex interfaces</td>
<td>Large number of data inputs or complex interfaces</td>
</tr>
<tr>
<td>Manual data inputs</td>
<td>No automated interfaces (manual inputs only)</td>
</tr>
<tr>
<td>Small number of data inputs or simple interfaces</td>
<td>Large number of data inputs or complex interfaces</td>
</tr>
<tr>
<td>Large number of data inputs or complex interfaces</td>
<td>Low volume of data or simple data</td>
</tr>
<tr>
<td>Low volume of data or simple data</td>
<td>Large volume of data or complex data; Data warehouses; Use of internal or external IT service providers (e.g., third-party storage or hosting of data)</td>
</tr>
<tr>
<td>Low volume of data or simple data</td>
<td>Low volume of data or simple data</td>
</tr>
</tbody>
</table>

---

6. A data warehouse is a central repository of integrated data from one or more disparate sources (such as multiple databases) from which reports may be generated or that may be used by the entity for other data analysis activities. A report-writer is an IT application that is used to extract data from one or more sources (such as a data warehouse, a database or an IT application) and present the data in a specified format. [Moved from A7 of ED–315]
<table>
<thead>
<tr>
<th>Matters related to the IT applications and IT infrastructure:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• The type of application (e.g., a commercial application with little or no customization, or a highly-customized or highly-integrated application that may have been purchased and customized, or developed in-house).</td>
<td></td>
</tr>
<tr>
<td>Purchased application with little or no customization</td>
<td>Purchased application or simple legacy or low-end ERP applications with little or no customization</td>
</tr>
<tr>
<td>• The complexity of the nature of the IT applications and the underlying IT infrastructure.</td>
<td></td>
</tr>
<tr>
<td>Small, simple laptop or client server-based solution</td>
<td>Mature and stable mainframe, small or simple client server, software as a service cloud</td>
</tr>
<tr>
<td>• Whether there is third-party hosting or outsourcing of IT.</td>
<td></td>
</tr>
<tr>
<td>If outsourced, competent, mature, proven provider (e.g., cloud provider)</td>
<td>If outsourced, competent, mature, proven provider (e.g., cloud provider)</td>
</tr>
<tr>
<td>• Whether the entity is using emerging technologies that affect its financial reporting.</td>
<td></td>
</tr>
<tr>
<td>No use of emerging technologies</td>
<td>Limited use of emerging technologies in some applications</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Matters related to IT processes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The personnel involved in maintaining the IT environment (the number and skill level of the IT support resources that manage security and changes to the IT environment)</td>
</tr>
<tr>
<td>Few personnel with limited IT knowledge to process vendor upgrades and manage access</td>
</tr>
<tr>
<td>• The complexity of processes to manage access rights</td>
</tr>
<tr>
<td>Single individual with administrative access manages access rights</td>
</tr>
</tbody>
</table>
• The complexity of the security over the IT environment, including vulnerability of the IT applications, databases, and other aspects of the IT environment to cyber security risks, particularly when there are web-based transactions or transactions involving external interfaces.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Simple on-premise access with no external web-facing elements;</th>
<th>Some web-based applications with primarily simple, role-based security</th>
<th>Multiple platforms with web-based access and complex security models</th>
</tr>
</thead>
</table>

| Requirement                                      | Commercial software with no source code installed             | Some commercial applications with no source code and other mature applications with a small number or simple changes; traditional systems development lifecycle | New or large number or complex changes, several development cycles each year |

| Requirement                                      | Changes limited to version upgrades of commercial software     | Changes consist of commercial software upgrades, ERP version upgrades, or legacy enhancements | New or large number or complex changes, several development cycles each year, heavy ERP customization |

| Requirement                                      | Software upgrades provided by vendor. No data conversion features for upgrade. | Minor version upgrades for commercial software applications with limited data being converted | Major version upgrade, new release, platform change |

**Scalability**

4.5.1 [Moved from para, A149 of ED–315] Obtaining an understanding of the entity’s IT environment may be more easily accomplished for a smaller and less complex entity that uses commercial software and when the entity does not have access to the source code to make any program changes. Such entities may not have dedicated IT resources but may have a person assigned in an administrator role for the purpose of granting employee access or installing vendor-provided updates to the IT applications. Specific matters that the auditor may consider in understanding the nature of a
commercial accounting software package, which may be the single IT application used by a smaller and less complex entity in its information system, may include:

- The extent to which the software is well established and has a reputation for reliability;
- The extent to which it is possible for the entity to modify the source code of the software, to include additional modules (i.e., add-ons) to the base software, or to make direct changes to data; and
- The nature and extent of modifications that have been made to the software. Although an entity may not be able to modify the source code of the software, many software packages allow for configuration (e.g., setting or amending reporting parameters). These do not usually involve modifications to source code; however, the auditor may consider the extent to which the entity is able to configure the software when considering the completeness and accuracy of information produced by the software that is used as audit evidence.

5.6. [Moved from para. A150 of ED–315] Complex IT environments may include highly-customized or highly-integrated IT applications and may therefore require more effort to understand. Financial reporting processes or IT applications may be integrated with other IT applications. Such integration may involve IT applications that are used in the entity’s business operations and that provide information to the financial reporting IT applications relevant to the flows of transactions and information processing in the entity’s information system. In such circumstances, certain IT applications used in the entity’s business operations may support or also be relevant to the preparation of the financial statements. Complex IT environments also may require dedicated IT departments that have structured IT processes supported by personnel that have software development and IT environment maintenance skills. In other cases, an entity may use third-party internal or external service providers to manage certain aspects of, or IT processes within, its IT environment (e.g., third-party hosting).

Identifying IT Applications that are Subject to Risks Arising from the use of IT

6.7. [Moved from para. A183 of ED–315] Automated controls that may be determined identified to be relevant to the audit in accordance with paragraph 4039 may include, for example, automated calculations or input, processing and output controls, such as a three-way match of a purchase order, shipping document, and vendor invoice. System-generated reports that the auditor may intend to use as audit evidence may include, for example, a trade receivable aging report or an inventory valuation report. Audit evidence may also come in the form of system-generated output that is used in a calculation performed in an end-user computing tool (e.g., spreadsheet software).

7.8. [Moved from part of A184 of ED–315] In considering whether the IT applications in which automated controls exist and reports are generated are relevant to the audit subject to risks arising from the use of IT, the auditor is likely to consider whether, and the extent to which, the entity may have access to source code that enables management to make program changes to such controls or the IT applications. The extent to which the entity makes program changes and the extent to which the IT processes over such changes are formalized may also be relevant considerations.

8.9. [Moved from part of A184 of ED–315] For system-generated reports to be used as audit evidence, the auditor may obtain audit evidence about the completeness and accuracy of the reports by
substantively testing the inputs and outputs of the report. In other cases, the auditor may plan to test
the operating effectiveness of the controls over the preparation and maintenance of the report, in
which case the IT application from which it is produced is likely to be relevant to the audit subject to
risks arising from the use of IT. In addition to testing the completeness and accuracy of the report,
the auditor may plan to test the operating effectiveness of general IT controls that address risks
related to inappropriate or unauthorized program changes to the report.

10. [Moved from part of para. A185 of ED–315] Some IT applications may include report-writing
functionality within them while some entities may also utilize separate report-writing applications (i.e.,
report-writers). In such cases, the auditor may need to determine the sources of system-generated
reports (i.e., the application that prepares the report and the data sources used by the report) to
determine the IT applications relevant to the audit subject to risks arising from the use of IT.

9.11. [Moved from part of para. A185 of ED–315] The data sources used by IT applications may be
databases that, for example, can only be accessed through the IT application or by IT personnel with
database administration privileges. In other cases, the data source may be a data warehouse that
may itself be considered to be an IT application relevant to the audit subject to risks arising from the
use of IT.

10.12. [Moved from para A187 of ED–315] The auditor may have identified a risk for which substantive procedures alone are not sufficient
because of the entity's use of highly-automated and paperless processing of transactions, which may
involve multiple integrated IT applications. In such circumstances, the controls identified by the
auditor relevant to the audit are likely to include automated controls. Further, the entity may be relying
on general IT controls to maintain the integrity of the transactions processed and other information
used in processing. In such cases, the IT applications involved in the processing and the storage of
the information are likely relevant to the audit subject to risks arising from the use of IT.

Scalability

44.13. [Moved from para. A186 of ED–315] The entity's ability to maintain the integrity of information
stored and processed in the information system may vary based on the complexity and volume of the
related transactions and other information. The greater the complexity and volume of data that
supports a significant class of transactions, account balance or disclosure, the less likely it may
become for the entity to maintain integrity of that information through application information
processing controls alone (e.g., input and output controls or review controls). It also becomes less
likely that the auditor will be able to obtain audit evidence about the completeness and accuracy of
such information through substantive testing alone when such information is used as audit evidence.
In some circumstances, when volume and complexity of transactions are lower, management may
have an application information processing control that is sufficient to verify the accuracy and
completeness of the data (e.g., individual sales orders processed and billed may be reconciled to the
hard copy originally entered into the IT application). When the entity relies on general IT controls to
maintain the integrity of certain information used by IT applications, the auditor may determine that
the IT applications that maintain that information are relevant to the audit subject to risks arising from the use of IT.

<table>
<thead>
<tr>
<th>Example characteristics of an IT application that is likely not subject to risks arising from IT</th>
<th>Example characteristics of an IT application that is likely subject to risks arising from IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Standalone applications</td>
<td>• Applications are interfaced.</td>
</tr>
<tr>
<td>• The volume of data (transactions) is not significant.</td>
<td>• The volume of data (transactions) is significant.</td>
</tr>
<tr>
<td>• The application’s functionality is not complex.</td>
<td>• The application’s functionality is complex as</td>
</tr>
<tr>
<td>• Each transaction is supported by original hard copy documentation.</td>
<td>– The application automatically initiates transactions</td>
</tr>
<tr>
<td></td>
<td>– There are multi-factor transactions, and</td>
</tr>
<tr>
<td></td>
<td>– There are a variety of complex calculations underlying automated entries.</td>
</tr>
</tbody>
</table>

IT application is likely not subject to risks arising from IT because:

<table>
<thead>
<tr>
<th></th>
<th>IT application is likely subject to risks arising from IT because:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The volume of data is not significant and therefore management is not relying upon general IT controls to process or maintain the data.</td>
<td>• Management relies on an application system to process or maintain data as the volume of data is significant.</td>
</tr>
<tr>
<td>• Management does not rely on automated controls or other automated functionality. The auditor has not identified automated controls [in accordance with paragraph X]</td>
<td>• Management relies upon the application system to perform certain automated controls that the auditor has also identified.</td>
</tr>
<tr>
<td>• Although management uses system-generated reports in their controls, they do not rely on these reports. Instead, they reconcile the reports back to the hard copy documentation and verify the calculations in the reports.</td>
<td>• We will directly test information produced by the entity used as audit evidence.</td>
</tr>
</tbody>
</table>

Other Aspects of the IT Environment that May Be Subject to Risks Arising from the Use of IT
14. **[Moved from para. A8 of ED–315]** The IT infrastructure includes the network, operating system and databases. A network is used in the IT infrastructure to transmit data and to share information, resources and services through a common communications link. The network also typically establishes a layer of logical security (enabled through the operating system) for access to the underlying resources. The operating system is responsible for managing communications between hardware, IT applications, and other software used in the network. Databases store the data used by IT applications and may consist of many interrelated data tables. Data in databases may also be accessed directly through database management systems by IT or other personnel with database administration privileges.

15. **[Moved from para. A188 of ED–315]**

When IT applications are identified by the auditor to be subject to risks arising from IT, the database(s) that stores the data processed by an identified IT application relevant to the audit is typically relevant to the audit also identified. Similarly, because an IT application’s ability to operate is often dependent on the operating system, the operating system is typically relevant to the audit subject to risks arising from the use of IT. The network may be relevant to the audit identified when it is a central point of access to the identified IT applications and related databases or, for example, when an IT application interacts with vendors or external parties through the internet.

**Identifying Risks arising from the Use of IT and General IT Controls**

16. **[Moved from para A145 of ED–315]** Examples of risks arising from the use of IT include risks related to:

- Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions, or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database.
- The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.
- Unauthorized changes to data in master files.
- Unauthorized changes to IT applications or other aspects of the IT environment.
- Failure to make necessary changes to IT applications or other aspects of the IT environment.
- Inappropriate manual intervention.
- Potential loss of data or inability to access data as required.

17. The auditor’s consideration of unauthorized access may include risks related to unauthorized access by external parties (often referred to as cyber risks). For an identified IT application or other aspect of the IT environment, the auditor’s consideration of such risks may include, for example, consideration of the entity’s IT processes and general IT controls that address privileged account access, data security, or customer/vendor access management. In addition, laws and regulations that may have a direct or indirect effect on the entity’s financial statements may include data protection legislation. Considering an entity’s compliance with such laws or regulations, in
accordance with ISA 250 (Revised), ⁷ may involve understanding the entity’s IT processes and general IT controls that the entity has implemented to address the relevant laws or regulations.

17.18. [Moved from para. A190 of ED–315]

General IT controls are implemented to address risks arising from the use of IT. Accordingly, the auditor uses the understanding obtained about the identified IT applications and other aspects of the IT environment that are relevant to the audit and the related risks arising from the use of IT in determining the general IT controls to identify relevant to the audit. In doing so, the auditor may take an approach of understanding the general IT controls that the entity has established over its IT processes for management of access, program change and IT operations for each IT application or other aspect of the IT environment that is relevant to the audit. In some cases, an entity may use common IT processes across its IT environment or across certain IT applications, in which case common risks arising from the use of IT and common general IT controls may be identified.

18.19. [Moved from para. A192 of ED–315]

In general, a greater number of general IT controls related to IT applications and databases are likely to be relevant to the audit identified than for other aspects of the IT environment. This is because these aspects are the most closely concerned with the processing and storage of information and most subject to automated controls used in the entity’s information system. In identifying general IT controls, the auditor may consider controls over actions of both end users and of the entity’s IT personnel or IT service providers.

19.20. [Moved from para. A193 of ED–315]

Appendix 46 provides further explanation of the nature of the general IT controls typically implemented for different aspects of the IT environment. In addition, examples of general IT controls for different IT processes are provided.
As noted, Appendix 4 as presented in ED–315 has been re-numbered as Appendix 6. The Task Force plans to expand and enhance this Appendix to provide further explanation of the nature of the general IT controls typically implemented for different aspects of the IT environment. These enhancements will be focused on illustrating scalability of the risks arising from the use of IT and general IT controls for IT environments of varying complexity. Further consideration will be given to enhancements related to outsourcing and cyber risks, as well. The revised Appendix 6 will be provided to the Board in September 2019.

Considerations for Understanding General IT Controls

The appendix provides further matters that the auditor may consider in understanding general IT controls.

1. The nature of the general IT controls (GITCs) typically implemented for each of the aspects of the IT environment
   
   (a) Applications
   
   General IT controls at the IT application layer will correlate to the nature and extent of application functionality and the access paths allowed in the technology. For example, more controls will be relevant for highly-integrated IT applications with complex security options than a legacy IT application supporting a small number of account balances with access methods only through transactions.

   (b) Database
   
   General IT controls at the database layer typically address risks arising from the use of IT related to unauthorized updates to financial reporting information in the database through direct database access or execution of a script or program.

   (c) Operating system
   
   General IT controls at the operating system layer typically address risks arising from the use of IT related to administrative access, which can facilitate the override of other controls. This includes actions such as compromising other user’s credentials, adding new, unauthorized users, loading malware or executing scripts or other unauthorized programs.

   (d) Network
   
   General IT controls at the network layer typically address risks arising from the use of IT related to network segmentation, remote access, and authentication. Network controls may be relevant when an entity has web-facing applications used in financial reporting. Network controls are also may be relevant when the entity has significant business partner relationships or third party outsourcing, which may increase data transmissions and the need for remote access.
2. Examples of general IT controls that may exist by IT process include:

(a) Process to manage access:

- **Authentication**
  Controls that ensure a user accessing the IT application or other aspect of the IT environment is using their own log-in credentials (i.e., the user is not using another user’s credentials).

- **Authorization**
  Controls that allow users to access the information necessary for their job responsibilities and nothing further, which facilitates appropriate segregation of duties.

- **Provisioning**
  Controls to authorize new users and modifications to existing users’ access privileges.

- **Deprovisioning**
  Controls to remove user access upon termination or transfer.

- **Privileged access**
  Controls over administrative or powerful users’ access.

- **User access reviews**
  Controls to recertify or evaluate user access for ongoing authorization over time.

- **Security configuration controls**
  Each technology generally has key configuration settings that help restrict access to the environment.

- **Physical access**
  Controls over physical access to the data center and hardware, as such access may be used to override other controls.

(b) Process to manage program or other changes to the IT environment

- **Change management process**
  Controls over the process to design, program, test and migrate changes to a production (i.e., end user) environment.

- **Segregation of duties over change migration**
  Controls that segregate access to make and migrate changes to a production environment.

- **Systems development or acquisition or implementation**
  Controls over initial IT application development or implementation (or in relation to other aspects of the IT environment).
o **Data conversion**
Controls over the conversion of data during development, implementation or upgrades to the IT environment.

(c) Process to manage IT Operations

o **Job scheduling**
Controls over access to schedule and initiate jobs or programs that may affect financial reporting.

o **Job monitoring**
Controls to monitor financial reporting jobs or programs for successful execution.

o **Backup and recovery**
Controls to ensure backups of financial reporting data occur as planned and that such data is available and able to be accessed for timely recovery in the event of an outage or attack.

o **Intrusion detection**
Controls to monitor for vulnerabilities and or intrusions in the IT environment.