Appendix 5

(Ref: Para. 25(a), 26(b)–(c), A94, A166–A172)

Considerations for Understanding Information Technology (IT)

This 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 Entity's System of Internal Control

1. 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 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 the preparation of the financial report in accordance with the applicable financial reporting framework is processed, stored and communicated, and therefore affects the manner in which the entity's system of internal control is designed and implemented. Each component of the entity's system of internal control may use some extent of IT.

   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. 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, 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. 25(a))

3. The entity's information system 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. 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. However, such characteristics are directional and may differ depending on the nature of the specific IT applications in use by an entity.

	Examples of typical characteristics of:		
	Non-complex commercial software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems)
Matters related to extent of automation and use of data:			
• The extent of automated procedures for processing, and the complexity of those procedures, including, whether there is highly automated, paperless processing.	N/A	N/A	Extensive and often complex automated procedures
• The extent of the entity's reliance on system-generated reports in the processing of information.	Simple automated report logic	Simple relevant automated report logic	Complex automated report logic; Report-writer software
• How data is input (i.e., manual input, customer or vendor input, or file load).	Manual data inputs	Small number of data inputs or simple interfaces	Large number of data inputs or complex interfaces
• How IT facilitates communication between applications, databases or other aspects of the IT environment, internally and externally, as appropriate, through system interfaces.	No automated interfaces (manual inputs only)	Small number of data inputs or simple interfaces	Large number of data inputs or complex interfaces
• The volume and complexity of data in digital form being processed by the	Low volume of data or simple data that is able to be verified	Low volume of data or simple data	Large volume of data or complex data; Data

	Examples of typical characteristics of:		
information system, including whether accounting records or other information are stored in digital form and the location of stored data.	manually; Data available locally		warehouses;[76] Use of internal or external IT service providers (e.g., third-party storage or hosting of data)
Matters related to the IT applications and IT infrastructure:			
• The type of application (e.g., a commercial application with little or no customization, or a highly-customised or highly-integrated application that may have been purchased and customised, or developed in-house).	Purchased application with little or no customization	Purchased application or simple legacy or low-end ERP applications with little or no customization	Custom developed applications or more complex ERPs with significant customization
• The complexity of the nature of the IT applications and the underlying IT infrastructure.	Small, simple laptop or client server-based solution	Mature and stable mainframe, small or simple client server, software as a service cloud	Complex mainframe, large or complex client server, web-facing, infrastructure as a service cloud
• Whether there is third-party hosting or outsourcing of IT.	If outsourced, competent, mature, proven provider (e.g., cloud provider)	If outsourced, competent, mature, proven provider (e.g., cloud provider)	Competent, mature proven provider for certain applications and new or start-up provider for others
• Whether the entity is using emerging technologies that affect its financial reporting.	No use of emerging technologies	Limited use of emerging technologies in some applications	Mixed use of emerging technologies across platforms
Matters related to IT processes:			
• The personnel involved in maintaining the IT environment (the	Few personnel with limited IT knowledge to process vendor	Limited personnel with IT skills / dedicated to IT	Dedicated IT departments with skilled personnel,

[76] A data warehouse is generally described as 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.

	Examples of typical characteristics of:		
number and skill level of the IT support resources that manage security and changes to the IT environment).	upgrades and manage access		including programming skills
• The complexity of processes to manage access rights.	Single individual with administrative access manages access rights	Few individuals with administrative access manage access rights	Complex processes managed by IT department for access rights
• 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 risks, particularly when there are web-based transactions or transactions involving external interfaces.	Simple on-premise access with no external web-facing elements	Some web-based applications with primarily simple, role-based security	Multiple platforms with web-based access and complex security models
• Whether program changes have been made to the manner in which information is processed, and the extent of such changes during the period.	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
• The extent of change within the IT environment (e.g., new aspects of the IT environment or significant changes in the IT applications or the underlying IT infrastructure).	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
• Whether there was a major data conversion during the period and, if so, the nature and significance of the changes made, and how the conversion was undertaken.	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

Emerging Technologies

5. Entities may use emerging technologies (e.g., blockchain, robotics or artificial intelligence) because such technologies may present specific opportunities to increase operational efficiencies or enhance financial reporting. When emerging technologies are used in the entity's information system relevant to the preparation of the financial report, the auditor may include such technologies in the identification of IT applications and other aspects of the IT environment that are subject to risks arising from the use of IT. While emerging technologies may be seen to be more sophisticated or more complex compared to existing technologies, the auditor's responsibilities in relation to IT applications and identified general IT controls in accordance with paragraph 26(b)–(c) remain unchanged.

Scalability

6. Obtaining an understanding of the entity's IT environment may be more easily accomplished for a 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 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;
   - 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; and
   - The extent to which data related to the preparation of the financial report can be directly accessed (i.e., direct access to the database without using the IT application) and the volume of data that is processed. The greater the volume of data, the more likely the entity may need controls that address maintaining the integrity of the data, which may include general IT controls over unauthorised access and changes to the data.

7. Complex IT environments may include highly-customised 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 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 also be relevant to the preparation of the financial report. 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 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

8. Through understanding the nature and complexity of the entity's IT environment, including the nature and extent of information processing controls, the auditor may determine which IT applications the entity is relying upon to accurately process and maintain the integrity of financial information. The identification of IT applications on which the entity relies may affect the auditor's decision to test the automated controls within such IT applications, assuming that such automated controls address identified risks of material misstatement. Conversely, if the entity is not relying on an IT application, the automated controls within such IT application are unlikely to be appropriate or sufficiently precise for purposes of operating effectiveness tests. Automated controls that may be identified in accordance with paragraph 26(b) may include, for example, automated calculations or input, processing and output controls, such as a three-way match of a purchase order, vendor shipping document, and vendor invoice. When automated controls are identified by the auditor and the auditor determines through the understanding of the IT environment that the entity is relying on the IT application that includes those automated controls, it may be more likely for the auditor to identify the IT application as one that is subject to risks arising from the use of IT.

9. In considering whether the IT applications for which the auditor has identified automated controls are 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 or configuration changes and the extent to which the IT processes over such changes are formalised may also be relevant considerations. The auditor is also likely to consider the risk of inappropriate access or changes to data.

10. 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. For such reports, 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 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 unauthorised program changes to, or data changes in, the report.

11. 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 subject to risks arising from the use of IT.

12. 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 subject to risks arising from the use of IT.

13. 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 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 subject to risks arising from the use of IT.

End-User Computing

14. Although 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 or simple databases), such tools are not typically identified as IT applications in the context of paragraph 26(b). Designing and implementing controls around access and change to end-user computing tools may be challenging, and such controls are rarely equivalent to, or as effective as, general IT controls. Rather, the auditor may consider a combination of information processing controls, taking into account the purpose and complexity of the end-user computing involved, such as:

- Information processing controls over the initiation and processing of the source data, including relevant automated or interface controls to the point from which the data is extracted (i.e., the data warehouse);
- Controls to check that the logic is functioning as intended, for example, controls which 'prove' the extraction of data, such as reconciling the report to the data from which it was derived, comparing the individual data from the report to the source and vice versa, and controls which check the formulas or macros; or
- Use of validation software tools, which systematically check formulas or macros, such as spreadsheet integrity tools.

Scalability

15. 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 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 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 subject to risks arising from the use of IT.

Example characteristics of an IT application that is likely not subject to risks arising from IT	Example characteristics of an IT application that is likely subject to risks arising from IT
• Stand-alone applications. • The volume of data (transactions) is not significant. • The application's functionality is not complex. • Each transaction is supported by original hard copy documentation.	• Applications are interfaced. • The volume of data (transactions) is significant. • The application's functionality is complex as: ○ The application automatically initiates transactions; and

	o There are a variety of complex calculations underlying automated entries.
IT application is likely not subject to risks arising from IT because: • The volume of data is not significant and therefore management is not relying upon general IT controls to process or maintain the data. • Management does not rely on automated controls or other automated functionality. The auditor has not identified automated controls in accordance with paragraph 26(a). • Although management uses system-generated reports in their controls, it does not rely on these reports. Instead, it reconciles the reports back to the hard copy documentation and verifies the calculations in the reports. • The auditor will directly test information produced by the entity used as audit evidence.	IT application is likely subject to risks arising from IT because: • Management relies on an application system to process or maintain data as the volume of data is significant. • Management relies upon the application system to perform certain automated controls that the auditor has also identified.

Other Aspects of the IT Environment that Are Subject to Risks Arising from the Use of IT

16. When the auditor identifies IT applications that are subject to risks arising from the use of IT, other aspects of the IT environment are also typically subject to risks arising from the use of IT. The IT infrastructure includes the databases, operating system, and 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. The operating system is responsible for managing communications between hardware, IT applications, and other software used in the network. As such, IT applications and databases may be directly accessed through the operating system. 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.

17. 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 is typically also identified. Similarly, because an IT application's ability to operate is often dependent on the operating system and IT applications and databases may be directly accessed from the operating system, the operating system is typically subject to risks arising from the use of IT. The network may be identified when it is a central point of access to the identified IT applications and related databases or when an IT application interacts with vendors or external parties through the internet, or when web-facing IT applications are identified by the auditor.

Identifying Risks Arising from the Use of IT and General IT Controls

18. Examples of risks arising from the use of IT include risks related to inappropriate reliance on IT applications that are inaccurately processing data, processing inaccurate data, or both, such as

- Unauthorised access to data that may result in destruction of data or improper changes to data, including the recording of unauthorised 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.
- Unauthorised changes to data in master files.
- Unauthorised 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.

19. The auditor's consideration of unauthorised access may include risks related to unauthorised access by internal or external parties (often referred to as cybersecurity risks). Such risks may not necessarily affect financial reporting, as an entity's IT environment may also include IT applications and related data that address operational or compliance needs. It is important to note that cyber incidents usually first occur through the perimeter and internal network layers, which tend to be further removed from the IT application, database and operating systems that affect the preparation of the financial report. Accordingly, if information about a security breach has been identified, the auditor ordinarily considers the extent to which such a breach had the potential to affect financial reporting. If financial reporting may be affected, the auditor may decide to understand, and test the related controls to determine the possible impact or scope of potential misstatements in the financial report or may determine that the entity has provided adequate disclosures in relation to such security breach.

20. In addition, laws and regulations that may have a direct or indirect effect on the entity's financial report may include data protection legislation. Considering an entity's compliance with such laws or regulations, in accordance with ASA 250,[77] may involve understanding the entity's IT processes and general IT controls that the entity has implemented to address the relevant laws or regulations.

21. 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 and the applicable risks arising from the use of IT in determining the general IT controls to identify. 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.

22. In general, a greater number of general IT controls related to IT applications and databases are likely to be identified than for other aspects of the IT environment. This is because these aspects are the most closely concerned with the information processing and storage of information in the entity's information system. In identifying general IT controls, the auditor

[77] See ASA 250.

may consider controls over actions of both end users and of the entity's IT personnel or IT service providers.

23. **Appendix 6** 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.