IAESB International Accounting Education Standards Board

529 Fifth Avenue, 6th Floor, New York, NY 10017
T + 1 (212) 286-9344 F +1 (212) 286-9570
www.iaesb.org

Committee: International Accounting Education Standards Board (IAESB)

Meeting Location: IFAC Headquarters, New York, USA

Meeting Dates: July 11-12, 2018

Subject: Evaluation of IAASB, IESBA and PCAOB Standards for ICT-related Skills

Source Document	Source Document Name	Reference within Document	Extract	ICT Skills Identified	ICT Element
IAASB Standards and Related Documents					
ISA 200	Overall objectives of the independent auditor and the conduct of an audit in accordance with ISA	An audit of financial statements	7. The ISAs contain objectives, requirements and application and other explanatory material that are designed to support the auditor in obtaining reasonable assurance. The ISAs require that the auditor exercise professional judgment and maintain professional skepticism throughout the planning and performance of the audit…	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"	Behavioral Competence
ISA 200	Overall objectives of the independent auditor and the conduct of an audit in accordance with ISA	Definitions	(k) Professional judgment – The application of relevant training, knowledge and experience, within the context provided by auditing, accounting and ethical standards, in making informed decisions about the courses of action that are appropriate in the circumstances of the audit engagement. (l) Professional skepticism – An attitude that includes a questioning mind, being alert to conditions which may indicate possible misstatement due to error or fraud, and a critical assessment of audit evidence.	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"	Behavioral Competence

ISA 220	Quality Control for and Audit of Financial Statements	Assignment of Engagement Teams	A11. When considering the appropriate competence and capabilities expected of the engagement team as a whole, the engagement partner may take into consideration such matters as the team's: · Understanding of, and practical experience with, audit engagements of a similar nature and complexity through appropriate training and participation…. · …Technical expertise, including expertise with relevant information technology and specialized areas of accounting or auditing. · …Ability to apply professional judgment….	"Appropriately applies ICT related experience and knowledge"; "Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"; and "Makes Appropriate use of IT"	Behavioral Competence Digital Acumen
ISA 240	The Auditors' Responsibilities Relating to Fraud in Financial Statements	Responsibilities of the auditor	8. When obtaining reasonable assurance, the auditor is responsible for maintaining professional skepticism throughout the audit, considering the potential for management override of controls and recognizing the fact that audit procedures that are effective for detecting error may not be effective in detecting fraud. The requirements in this ISA are designed to assist the auditor in identifying and assessing the risks of material misstatement due to fraud and in designing procedures to detect such misstatement.	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"	Behavioral Competence

ISA 240	The Auditors' Responsibilities Relating to Fraud in Financial Statements	Professional Skepticism	12. In accordance with ISA 200, the auditor shall maintain professional skepticism throughout the audit, recognizing the possibility that a material misstatement due to fraud could exist, notwithstanding the auditor's past experience of the honesty and integrity of the entity's management and those charged with governance. (Ref: Para. A7–A8) 13. Unless the auditor has reason to believe the contrary, the auditor may accept records and documents as genuine. If conditions identified during the audit cause the auditor to believe that a document may not be authentic or that terms in a document have been modified but not disclosed to the auditor, the auditor shall investigate further. (Ref: Para. A9) A7. Maintaining professional skepticism requires an ongoing questioning of whether the information and audit evidence obtained suggests that a material misstatement due to fraud may exist. It includes considering the reliability of the information to be used as audit evidence and the controls over its preparation and maintenance where relevant. Due to the characteristics of fraud, the auditor's professional skepticism is particularly important when considering the risks of material misstatement due to fraud. A8. Although the auditor cannot be expected to disregard past experience of the honesty and integrity of the entity's management and those charged with governance, the auditor's professional skepticism is particularly important in considering the risks of material misstatement due to fraud because there may have been changes in circumstances. A9. An audit performed in accordance with ISAs rarely involves the authentication of documents, nor is the auditor trained as or expected to be an expert in such authentication. However, when the auditor identifies conditions that cause the auditor to believe that a document may not be authentic or that terms in a document have been modified but not disclosed to the auditor, possible procedures to investigate further may include: • Confirming directly with the third party. • Using the work of an expert to assess the document's authenticity.	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism" and "Able to assess usefulness of data transmitted in new channels"	Behavioral Competence Communication
ISA 240	The Auditors' Responsibilities Relating to Fraud in Financial Statements	Assignment and Supervision of Personnel	A34. The auditor may respond to identified risks of material misstatement due to fraud by, for example, assigning additional individuals with specialised skill and knowledge, such as forensic and IT experts, or by assigning more experience individuals to the engagement.	"Appropriately applies ICT related experience and knowledge"	Behavioral Competence

ISA 240	The Auditors' Responsibilities Relating to Fraud in Financial Statements	Audit Procedures Responsive to Assessed RoMM due to Fraud at the Assertion Level	A37. The auditor's responses to address the assessed risks of material misstatement due to fraud at the assertion level may include changing the nature, timing and extent of audit procedures in the following ways:• The nature of audit procedures to be performed may need to be changed to obtain audit evidence that is more reliable and relevant or to obtain additional corroborative information. This may affect both the type of audit procedures to be performed and their combination. For example:o Physical observation or inspection of certain assets may become more important or the auditor may choose to use computer-assisted audit techniques to gather more evidence about data contained in significant accounts or electronic transaction files….• …The extent of the procedures applied reflects the assessment of the risks of material misstatement due to fraud. For example, increasing sample sizes or performing analytical procedures at a more detailed level may be appropriate. Also, computer-assisted audit techniques may enable more extensive testing of electronic transactions and account files. Such techniques can be used to select sample transactions from key electronic files, to sort transactions with specific characteristics, or to test an entire population instead of a sample.	"Assessing Data Transmission and Security" and "Makes Use of Computer Assisted Techniques"	Digital AcumenData Interrogation, Syntesis and Analysis
ISA 240	The Auditors' Responsibilities Relating to Fraud in Financial Statements	Journal Entries and Other Adjustments	A42. Further, the auditor's consideration of the risks of material misstatement associated with inappropriate override of controls over journal entries is important since automated processes and controls may reduce the risk of inadvertent error but do not overcome the risk that individuals may inappropriately override such automated processes, for example, by changing the amounts being automatically passed to the general ledger or to the financial reporting system. Furthermore, where IT is used to transfer information automatically, there may be little or no visible evidence of such intervention in the information systems. A43. When identifying and selecting journal entries and other adjustments for testing and determining the appropriate method of examining the underlying support for the items selected, the following matters are of relevance:…. • Controls that have been implemented over journal entries and other adjustments – effective controls over the preparation and posting of journal entries and other adjustments may reduce the extent of substantive testing necessary, provided that the auditor has tested the operating effectiveness of the controls. • The entity's financial reporting process and the nature of evidence that can be obtained – for many entities routine processing of transactions involves a combination of manual and automated steps and procedures. Similarly, the processing of journal entries and other adjustments may involve both manual and automated procedures and controls. Where information technology is used in the financial reporting process, journal entries and other adjustments may exist only in electronic form	"Risk Assessment", "Understanding Processes and Controls" and "Assessing Data Transmission and Security"	Business Acumen Digital Acumen

ISA 240	The Auditors' Responsibilities Relating to Fraud in Financial Statements	Appendix 1: Examples of Fraud Risk Factors	Internal control components are deficient as a result of the following: • Inadequate monitoring of controls, including automated controls and controls over interim financial reporting (where external reporting is required). • High turnover rates or employment of staff in accounting, information technology, or the internal audit function that are not effective. • Accounting and information systems that are not effective, including situations involving significant deficiencies in internal control • Inadequate management understanding of information technology, which enables information technology employees to perpetrate a misappropriation.	"Able to evaluate and respond to process failures" and "Able to evaluate and respond to IT failures"	Business Acumen Digital Acumen
ISA 240	The Auditors' Responsibilities Relating to Fraud in Financial Statements	Appendix 2: Examples of Possible Audit Procedures	• Performing computer-assisted techniques, such as data mining to test for anomalies in a population. • Testing the integrity of computer-produced records and transactions. • Revenue Recognition - Performing substantive analytical procedures relating to revenue using disaggregated data, for example, comparing revenue reported by month and by product line or business segment during the current reporting period with comparable prior periods. Computer-assisted audit techniques may be useful in identifying unusual or unexpected revenue relationships or transactions. • Inventory - Using computer-assisted audit techniques to further test the compilation of the physical inventory counts – for example, sorting by tag number to test tag controls or by item serial number to test the possibility of item omission or duplication. • Misappropriation of assets - Performing a computerized match of the vendor list with a list of employees to identify matches of addresses or phone numbers. Performing a computerized search of payroll records to identify duplicate addresses, employee identification or taxing authority numbers or bank accounts.	"Assessing Data Transmission and Security" and "Makes Use of Computer Assisted Techniques"	Digital Acumen Data Interrogation, Syntesis and Analysis
ISA 240	The Auditors' Responsibilities Relating to Fraud in Financial Statements	Appendix 3: Examples of Circumstances that Indicate the Possibility of Fraud	Conflicting or missing evidence including • Unavailability of other than photocopied or electronically transmitted documents when documents in original form are expected to exist. • Unavailable or missing electronic evidence, inconsistent with the entity's record retention practices or policies. Problematic or unusual relationships between the auditor and management, including unwillingness to facilitate auditor access to key electronic files for testing through the use of computer-assisted audit techniques.	"Risk Assessment", "Assessing Data Transmission and Security" and "Makes Use of Computer Assisted Techniques"	Business Acumen Digital Acumen Data Interrogation, Syntesis and Analysis

ISA 250	Consideration of laws and regulations in an audit of financial statements	Audit procedures when non-compliance is identified or suspected	A13. If the auditor becomes aware of the existence of, or information about, the following matters, it may be an indication of non-compliance with laws and regulations:· Existence of an information system which fails, whether by design or by accident, to provide an adequate audit trail or sufficient evidence.	"Able to evaluate and respond to process failures" and "Able to evaluate and respond to IT failures"	Business AcumenDigital Acumen
ISA 265	Communicating Deficiencies in Internal Control to Those Charged with Governance and Management	Requirement	9. The auditor shall communicate in writing significant deficiencies in internal control identified during the audit to those charged with governance on a timely basis. (Ref: Para. A12–A18, A27) 10. The auditor shall also communicate to management at an appropriate level of responsibility on a timely basis: (Ref: Para. A19, A27) (a) In writing, significant deficiencies in internal control that the auditor has communicated or intends to communicate to those charged with governance, unless it would be inappropriate to communicate directly to management in the circumstances; and (Ref: Para. A14, A20–A21) (b) Other deficiencies in internal control identified during the audit that have not been communicated to management by other parties and that, in the auditor's professional judgment, are of sufficient importance to merit management's attention. (Ref: Para. A22–A26) 11. The auditor shall include in the written communication of significant deficiencies in internal control: (a) A description of the deficiencies and an explanation of their potential effects; and (Ref: Para. A28) (b) Sufficient information to enable those charged with governance and management to understand the context of the communication. In particular, the auditor shall explain that: (Ref: Para. A29–A30) (i) The purpose of the audit was for the auditor to express an opinion on the financial statements; (ii) The audit included consideration of internal control relevant to the preparation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of internal control; and (iii) The matters being reported are limited to those deficiencies that the auditor has identified during the audit and that the auditor has concluded are of sufficient importance to merit being reported to those charged with governance.	"Effectively Communicates with those Charged with Governance"	Communication

ISA 265	Communicating Deficiencies in Internal Control to Those Charged with Governance and Management	Determination of Whether Deficiencies in Internal Control Have Been Identified	A2. In discussing the facts and circumstances of the auditor's findings with management, the auditor may obtain other relevant information for further consideration, such as: • Management's understanding of the actual or suspected causes of the deficiencies. • Exceptions arising from the deficiencies that management may have noted, for example, misstatements that were not prevented by the relevant information technology (IT) controls. • A preliminary indication from management of its response to the findings.	"Able to evaluate and respond to process failures" and "Able to evaluate and respond to IT failures"	Business Acumen Digital Acumen
ISA 300	Planning an Audit of Financial Statements	Appendix - Considerations in Establishing the Overall Audit Strategy	This appendix provides examples of matters the auditor may consider in establishing the overall audit strategy. Many of these matters will also influence the auditor's detailed audit plan. The examples provided cover a broad range of matters applicable to many engagements. While some of the matters referred to below may be required by other ISAs, not all matters are relevant to every audit engagement and the list is not necessarily complete... • The effect of information technology on the audit procedures, including the availability of data and the expected use of computer-assisted audit techniques • Significant business developments affecting the entity, including changes in information technology and business processes, changes in key management, and acquisitions, mergers and divestments.	"Risk Assessment", "Understanding Processes and Controls" and "Makes Use of Computer Assisted Techniques"	Business Acumen Data Interrogation Synthesis and Analysis,

ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Components of Internal Control	18. The auditor shall obtain an understanding of the information system, including the related business processes, relevant to financial reporting, including the following areas: (Ref: Para. A90–A92 and A95-A96) (a) The classes of transactions in the entity's operations that are significant to the financial statements; (b) The procedures, within both information technology (IT) and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in the financial statements; (c) The related accounting records, supporting information and specific accounts in the financial statements that are used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the general ledger. The records may be in either manual or electronic form; (d) How the information system captures events and conditions, other than transactions, that are significant to the financial statements; (e) The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures; and (f) Controls surrounding journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments. (Ref: Para. A93–A94) This understanding of the information system relevant to financial reporting shall include relevant aspects of that system relating to information disclosed in the financial statements that is obtained from within or outside of the general and subsidiary ledgers.	"Understanding Processes and Controls"	Business Acumen
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Identifying and Assessing the Risks of Material Misstatement	30. In respect of some risks, the auditor may judge that it is not possible or practicable to obtain sufficient appropriate audit evidence only from substantive procedures. Such risks may relate to the inaccurate or incomplete recording of routine and significant classes of transactions or account balances, the characteristics of which often permit highly automated processing with little or no manual intervention. In such cases, the entity's controls over such risks are relevant to the audit and the auditor shall obtain an understanding of them. (Ref: Para. A149–A151)	"Understanding Processes and Controls", "Risk assessment"	Business Acumen
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Inquiries of Management, the Internal Audit Function and Others within the Entity	A7. The auditor may also obtain information, or a different perspective in identifying risks of material misstatement, through inquiries of other within the entity and other employees with different levels of authority. For example:...- Inquiries directed to information systems personnel may provide information about system changes, systems or control failures, or other information system-related risks.	"Risk assessment" and "Able to evaluate and respond to process failures"	Business Acumen

ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Objectives and strategies and related business risks	A40. Examples of matters that the auditor may consider when obtaining an understanding of the entity's objectives, strategies and related business risks that may result in a risk of material misstatement of the financial statements include:… · Use of IT (a potential related business risk might be, for example, that systems and processes are incompatible)….	"Understanding Processes and Controls", "Risk assessment"	Business Acumen
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Characteristics of Manual and Automated Elements of Internal Control Relevant to the Auditor's Risk Assessment	A61. The use of manual or automated elements in internal control also affects the manner in which transactions are initiated, recorded, processed, and reported: • Controls in a manual system may include such procedures as approvals and reviews of transactions, and reconciliations and follow-up of reconciling items. Alternatively, an entity may use automated procedures to initiate, record, process, and report transactions, in which case records in electronic format replace paper documents. • Controls in IT systems consist of a combination of automated controls (for example, controls embedded in computer programs) and manual controls. Further, manual controls may be independent of IT, may use information produced by IT, or may be limited to monitoring the effective functioning of IT and of automated controls, and to handling exceptions. When IT is used to initiate, record, process or report transactions, or other financial data for inclusion in financial statements, the systems and programs may include controls related to the corresponding assertions for material accounts or may be critical to the effective functioning of manual controls that depend on IT. An entity's mix of manual and automated elements in internal control varies with the nature and complexity of the entity's use of IT.	"Understanding Processes and Controls", "Risk assessment"	Business Acumen
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Characteristics of Manual and Automated Elements of Internal Control Relevant to the Auditor's Risk Assessment	A63. Generally, IT benefits an entity's 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.	"Makes Appropriate use of IT"	Digital Acumen

ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Characteristics of Manual and Automated Elements of Internal Control Relevant to the Auditor's Risk Assessment	A64. IT also poses specific risks to an entity's internal control, including, for example: • Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both. • 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 systems or programs. • Failure to make necessary changes to systems or programs. • Inappropriate manual intervention. • Potential loss of data or inability to access data as required.	"Understanding Processes and Controls", "Risk assessment"	Business Acumen
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Characteristics of Manual and Automated Elements of Internal Control Relevant to the Auditor's Risk Assessment	A67. The extent and nature of the risks to internal control vary depending on the nature and characteristics of the entity's information system. The entity responds to the risks arising from the use of IT or from use of manual elements in internal control by establishing effective controls in light of the characteristics of the entity's information system.	"Risk assessment"	Business Acumen
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Nature and extent of the understanding of relevant controls	A76. Obtaining an understanding of an entity's controls is not sufficient to test their operating effectiveness, unless there is some automation that provides for the consistent operation of the controls. For example, obtaining audit evidence about the implementation of a manual control at a point in time does not provide audit evidence about the operating effectiveness of the control at other times during the period under audit. However, because of the inherent consistency of IT processing (see paragraph A63), performing audit procedures to determine whether an automated control has been implemented may serve as a test of that control's operating effectiveness, depending on the auditor's assessment and testing of controls such as those over program changes. Tests of the operating effectiveness of controls are further described in ISA 330.	"Understanding Processes and Controls", "Risk assessment"	Business Acumen

ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Effect of the Control Environment	A83. The existence of a satisfactory control environment can be a positive factor when the auditor assesses the risks of material misstatement. However, although it may help reduce the risk of fraud, a satisfactory control environment is not an absolute deterrent to fraud. Conversely, deficiencies in the control environment may undermine the effectiveness of controls, in particular in relation to fraud. For example, management's failure to commit sufficient resources to address IT security risks may adversely affect internal control by allowing improper changes to be made to computer programs or to data, or unauthorized transactions to be processed. As explained in ISA 330, the control environment also influences the nature, timing, and extent of the auditor's further procedures.	"Understanding Processes and Controls", "Risk assessment" and "Assessing Data Transmission and Security"	Business AcumenDigital Acumen
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Components of Internal Control – the Information System	A90. The information system relevant to financial reporting objectives, which includes the accounting system, consists of the procedures and records designed and established to: • Initiate, record, process, and report entity transactions (as well as events and conditions) 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; • Transfer information from transaction processing systems to the general ledger; • Capture 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 accounts receivables; 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.	"Understanding Processes and Controls" and "Assessing Data Transmission and Security"	Business Acumen Digital Acumen
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Components of Internal Control – the Information System	A92. The understanding of the information system relevant to financial reporting required by paragraph 18 of this ISA (including the understanding of relevant aspects of that system relating to information disclosed in the financial statements that is obtained from within or outside of the general and subsidiary ledgers) is a matter of the auditor's professional judgment. For example, certain amounts or disclosures in the entity's financial statements (such as disclosures about credit risk, liquidity risk, and market risk) may be based on information obtained from the entity's risk management system. However, the auditor is not required to understand all aspects of the risk management system, and uses professional judgment in determining the necessary understanding.	"Understanding Processes and Controls" and "Assessing Data Transmission and Security"	Business Acumen Digital Acumen

ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Journal Entries	A93. An entity's information system typically includes the use of standard journal entries that are required on a recurring basis to record transactions. Examples might be journal entries to record sales, purchases, and cash disbursements in the general ledger, or to record accounting estimates that are periodically made by management, such as changes in the estimate of uncollectible accounts receivable. A94. An entity's financial reporting process also includes the use of non-standard journal entries to record non-recurring, unusual transactions or adjustments. Examples of such entries include consolidating adjustments and entries for a business combination or disposal or non-recurring estimates such as the impairment of an asset. In manual general ledger systems, non-standard journal entries may be identified through inspection of ledgers, journals, and supporting documentation. When automated procedures are used to maintain the general ledger and prepare financial statements, such entries may exist only in electronic form and may therefore be more easily identified through the use of computer-assisted audit techniques.	"Understanding Processes and Controls" and "Makes Use of Computer Assisted Techniques"	Business Acumen Data Interrogation Synthesis and Analysis,
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Considerations specific to smaller entities	A96. The information system, and related business processes relevant to financial reporting in small entities, including relevant aspects of that system relating to information disclosed in the financial statements that is obtained from within or outside of the general and subsidiary ledgers, is likely to be less sophisticated than in larger entities, but its role is just as significant. Small entities with active management involvement may not need extensive descriptions of accounting procedures, sophisticated accounting records, or written policies. Understanding the entity's information systems relevant to financial reporting may therefore be easier in an audit of smaller entities, and may be more dependent on inquiry than on review of documentation. The need to obtain an understanding, however, remains important.	"Understanding Processes and Controls", "Risk assessment"	Business Acumen

ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Risks Arising from IT	A107. The use of IT affects the way that control activities are implemented. From the auditor's perspective, controls over IT systems are effective when they maintain the integrity of information and the security of the data such systems process, and include effective general IT controls and application controls.A108. General IT controls are policies and procedures that relate to many applications and support the effective functioning of application controls. They apply to mainframe, miniframe, and end-user environments. General IT controls that maintain the integrity of information and security of data commonly include controls over the following:• Data center and network operations.• System software acquisition, change and maintenance.• Program change.• Access security.• Application system acquisition, development, and maintenance.They are generally implemented to deal with the risks referred to in paragraph A64 above.A109. Application controls are manual or automated procedures that typically operate at a business process level and apply to the processing of transactions by individual applications. Application controls can be preventive or detective in nature and are designed to ensure the integrity of the accounting records. Accordingly, application controls relate to procedures used to initiate, record, process and report transactions or other Undertsanifinancial data. These controls help ensure that transactions occurred, are authorized, and are completely and accurately recorded and processed. Examples include edit checks of input data, and numerical sequence checks with manual followup of exception reports or correction at the point of data entry.	"Risk assessment"	Business AcumenDigital Acumen
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Sources of Information	A121. Much of the information used in monitoring may be produced by the entity's information system. If management assumes that data used for monitoring are accurate without having a basis for that assumption, errors that may exist in the information could potentially lead management to incorrect conclusions from its monitoring activities.	"Understanding Processes and Controls"	Business Acumen
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Risks for Which Substantial Procedures Alone are not Enough	A149. Where such routine business transactions are subject to highly automated processing with little or no manual intervention, it may not be possible to perform only substantive procedures in relation to the risk. For example, the auditor may consider this to be the case in circumstances where a significant amount of an entity's information is initiated, recorded, processed, or reported only in electronic form such as in an integrated system. In such cases: • Audit evidence may be available only in electronic form, and its sufficiency and appropriateness usually depend on the effectiveness of controls over its accuracy and completeness.	"Understanding Existing Processes and designing appropriate response", "Able to respond to process	Business Acumen Digital Acumen

			• The potential for improper initiation or alteration of information to occur and not be detected may be greater if appropriate controls are not operating effectively.	failures", and "Able to respone to IT failures"	
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Appendix 1 – Internal Control Components	Entity Risk Assessent Process 4. 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 data 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: ... • New or revamped information systems. Significant and rapid changes in information systems can change the risk relating to internal control. • New technology. Incorporating new technologies into production processes or information systems may change the risk associated with 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 internal control.	"Risk assessment" and "Keeps current with new and emerging technologies"	Business Acumen

ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Appendix 1 – Internal Control Components	Information System, Including the Related Business Processes, Relevant to Financial Reporting, and Communication5. An information system consists of infrastructure (physical and hardware components), software, people, procedures, and data. Many information systems make extensive use of information technology (IT).6. The information system relevant to financial reporting objectives, which includes the financial reporting system, encompasses methods 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.7. The quality of system-generated information affects management's ability to make appropriate decisions in managing and controlling the entity's activities and to prepare reliable financial reports.8. Communication, which involves providing an understanding of individual roles and responsibilities pertaining to internal control over financial reporting, 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.	"Understanding Processes and Controls"	Business Acumen
ISA 315 (Revised)	Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and it's Environment	Appendix 1 – Internal Control Components	Control Activities 9. Generally, control activities that may be relevant to an audit may be categorized as policies and procedures that pertain to the following:... • Information processing. The two broad groupings of information systems control activities are application controls, which apply to the processing of individual applications, and general IT controls, which are policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. Examples of application controls include checking the arithmetical accuracy of records, maintaining and reviewing accounts and trial balances, automated controls such as edit checks of input data and numerical sequence checks, and manual follow-up of exception reports. Examples of general IT controls are program change controls, controls that restrict access to programs or data, controls over the implementation of new releases of packaged software applications, and controls over system software that restrict access to or monitor the use of system utilities that could change financial data or records without leaving an audit trail.	"Understanding Processes and Controls"	Business Acumen

ISA 330	The Auditors' Responses to Assessed Risks	Using audit evidence obtained in previous audits	13. In determining whether it is appropriate to use audit evidence about the operating effectiveness of controls obtained in previous audits, and, if so, the length of the time period that may elapse before retesting a control, the auditor shall consider the following: (a) The effectiveness of other elements of internal control, including the control environment, the entity's monitoring of controls, and the entity's risk assessment process; (b) The risks arising from the characteristics of the control, including whether it is manual or automated; (c) The effectiveness of general IT controls; (d) The effectiveness of the control and its application by the entity, including the nature and extent of deviations in the application of the control noted in previous audits, and whether there have been personnel changes that significantly affect the application of the control; (e) Whether the lack of a change in a particular control poses a risk due to changing circumstances; and (f) The risks of material misstatement and the extent of reliance on the control. (Ref: Para. A35)	"Understanding Existing Processes and designing appropriate response"	Business Acumen
ISA 330	The Auditors' Responses to Assessed Risks	Extent	A16. The use of computer-assisted audit techniques (CAATs) may enable more extensive testing of electronic transactions and account files, which may be useful when the auditor decides to modify the extent of testing, for example, in responding to the risks of material misstatement due to fraud. Such techniques can be used to select sample transactions from key electronic files, to sort transactions with specific characteristics, or to test an entire population instead of a sample.	"Makes Use of Computer Assisted Techniques"	Data Interrogation Synthesis and Analysis,
ISA 330	The Auditors' Responses to Assessed Risks	Extent of Tests of Controls	A27. The nature of the particular control influences the type of procedure required to obtain audit evidence about whether the control was operating effectively. For example, if operating effectiveness is evidenced by documentation, the auditor may decide to inspect it to obtain audit evidence about operating effectiveness. For other controls, however, documentation may not be available or relevant. For example, documentation of operation may not exist for some factors in the control environment, such as assignment of authority and responsibility, or for some types of control activities, such as control activities performed by a computer. In such circumstances, audit evidence about operating effectiveness may be obtained through inquiry in combination with other audit procedures such as observation or the use of CAATs.	"Makes Use of Computer Assisted Techniques"	Data Interrogation Synthesis and Analysis,

ISA 330	The Auditors' Responses to Assessed Risks	Extent of Tests of Controls	A29. Because of the inherent consistency of IT processing, it may not be necessary to increase the extent of testing of an automated control. An automated control can be expected to function consistently unless the program (including the tables, files, or other permanent data used by the program) is changed. Once the auditor determines that an automated control is functioning as intended (which could be done at the time the control is initially implemented or at some other date), the auditor may consider performing tests to determine that the control continues to function effectively. Such tests might include determining that:• Changes to the program are not made without being subject to the appropriate program change controls;• The authorized version of the program is used for processing transactions; and• Other relevant general controls are effective.Such tests also might include determining that changes to the programs have not been made, as may be the case when the entity uses packaged software applications without modifying or maintaining them. For example, the auditor may inspect the record of the administration of IT security to obtain audit evidence that unauthorized access has not occurred during the period.	"Understanding Existing Processes and designing appropriate response"	Business Acumen
ISA 330	The Auditors' Responses to Assessed Risks	Testing of indirect controls	A30. In some circumstances, it may be necessary to obtain audit evidence supporting the effective operation of indirect controls. For example, when the auditor decides to test the effectiveness of a user review of exception reports detailing sales in excess of authorized credit limits, the user review and related follow up is the control that is directly of relevance to the auditor. Controls over the accuracy of the information in the reports (for example, the general IT controls) are described as "indirect" controls. A31. Because of the inherent consistency of IT processing, audit evidence about the implementation of an automated application control, when considered in combination with audit evidence about the operating effectiveness of the entity's general controls (in particular, change controls), may also provide substantial audit evidence about its operating effectiveness.	"Understanding Existing Processes and designing appropriate response"	Business Acumen

ISA 402	Audit Considerations Relating to an Entity Using a Service Organisation	Scope of this ISA	3. Services provided by a service organization are relevant to the audit of a user entity's financial statements when those services, and the controls over them, are part of the user entity's information system, including related business processes, relevant to financial reporting. Although most controls at the service organization are likely to relate to financial reporting, there may be other controls that may also be relevant to the audit, such as controls over the safeguarding of assets. A service organization's services are part of a user entity's information system, including related business processes, relevant to financial reporting if these services affect any of the following:... (b) The procedures, within both information technology (IT) and manual systems, by which the user entity's transactions are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in the financial statements; (c) The related accounting records, either in electronic or manual form, supporting information and specific accounts in the user entity's financial statements that are used to initiate, record, process and report the user entity's transactions; this includes the correction of incorrect information and how information is transferred to the general ledger; (d) How the user entity's information system captures events and conditions, other than transactions, that are significant to the financial statements;	"Understanding Existing Processes and designing appropriate response"	Business Acumen
ISA 402	Audit Considerations Relating to an Entity Using a Service Organisation	Nature of the Services Provided by the Service Organisation	A3. A user entity may use a service organization such as one that processes transactions and maintains related accountability, or records transactions and processes related data. Service organizations that provide such services include, for example …. application service providers that provide packaged software applications and a technology environment that enables customers to process financial and operational transactions.	"Understanding Existing Processes and designing appropriate response"	Business Acumen
ISA 402	Audit Considerations Relating to an Entity Using a Service Organisation	Responding to the Assessed RoMM	A25. When the service organization maintains material elements of the accounting records of the user entity, direct access to those records may be necessary in order for the user auditor to obtain sufficient appropriate audit evidence relating to the operations of controls over those records or to substantiate transactions and balances recorded in them, or both. Such access may involve either physical inspection of records at the service organization's premises or interrogation of records maintained electronically from the user entity or another location, or both. Where direct access is achieved electronically, the user auditor may thereby obtain evidence as to the adequacy of controls operated by the service organization over the completeness and integrity of the user entity's data for which the service organization is responsible.	"Understanding Existing Processes and designing appropriate response"	Business Acumen
ISA 450	Evaluation of Misstatements	Definition of misstatement	A1. Misstatements may result from: (a) An inaccuracy in gathering or processing data from which the financial statements are prepared;…	"Understanding Existing	Business Acumen Digital Acumen

	Identified During the Audit			Processes and designing appropriate response" and "Assessing Data Transmission and Security"	
ISA 500	Audit Evidence	Audit Procedures for Obtaining Audit Evidence	A12. The nature and timing of the audit procedures to be used may be affected by the fact that some of the accounting data and other information may be available only in electronic form or only at certain points or periods in time. For example, source documents, such as purchase orders and invoices, may exist only in electronic form when an entity uses electronic commerce, or may be discarded after scanning when an entity uses image processing systems to facilitate storage and reference.A13. Certain electronic information may not be retrievable after a specified period of time, for example, if files are changed and if backup files do not exist. Accordingly, the auditor may find it necessary as a result of an entity's data retention policies to request retention of some information for the auditor's review or to perform audit procedures at a time when the information is available.A18. An external confirmation represents audit evidence obtained by the auditor as a direct written response to the auditor from a third party (the confirming party), in paper form, or by electronic or other medium….	"Understanding Existing Processes and designing appropriate response"	Business Acumen
ISA 500	Audit Evidence	Selecting items for testing to obtain audit evidence	A53. The auditor may decide that it will be most appropriate to examine the entire population of items that make up a class of transactions or account balance (or a stratum within that population). 100% examination is unlikely in the case of tests of controls; however, it is more common for tests of details. 100% examination may be appropriate when, for example: · …The repetitive nature of a calculation or other process performed automatically by an information system makes a 100% examination cost effective.	"Understanding Existing Processes and designing appropriate response" and "Makes Use of Computer Assisted Techniques"	Business Acumen Data Interrogation Synthesis and Analysis,
ISA 505	External Confirmations	Results of the External Confirmation Process	A12. Responses received electronically, for example by facsimile or electronic mail, involve risks as to reliability because proof of origin and authority of the respondent may be difficult to establish, and alterations may be difficult to detect. A process used by the auditor and the respondent that creates a secure environment for responses received electronically may mitigate these risks. If the auditor is satisfied that such a process is secure and properly controlled, the reliability of the related responses is enhanced. An electronic confirmation process might incorporate various techniques for validating the	"Understanding Existing Processes and designing appropriate response" and "Demonstrates	Business Acumen Behavioral Competence

			identity of a sender of information in electronic form, for example, through the use of encryption, electronic digital signatures, and procedures to verify web site authenticity.	objectivity, integrity, independence, professional competence, due care, professional skepticism	
ISA 520	Analytical Procedures	Substantive Analytical Procedures	5. When designing and performing substantive analytical procedures, either alone or in combination with tests of details, as substantive procedures in accordance with ISA 330, the auditor shall: (Ref: Para. A4–A5)… (b) Evaluate the reliability of data from which the auditor's expectation of recorded amounts or ratios is developed, taking account of source, comparability, and nature and relevance of information available, and controls over preparation; (Ref: Para. A12–A14) A5. The auditor may inquire of management as to the availability and reliability of information needed to apply substantive analytical procedures, and the results of any such analytical procedures performed by the entity. It may be effective to use analytical data prepared by management, provided the auditor is satisfied that such data is properly prepared. (See also reliability of Data A12-A14)	"Understanding Existing Processes and designing appropriate response" and "Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism	Business Acumen Behavioral Competence
ISA 600	Special considerations – audit of group financial statements	Appendix 2: Examples of matters about which the group engagement team obtains an understanding	The examples provided cover a broad range of matters; however, not all matters are relevant to every group audit engagement and the list of examples is not necessarily complete. Group-Wide Controls 1. Group-wide controls may include a combination of the following: • A central IT system controlled by the same general IT controls for all or part of the group. • Control activities within an IT system that is common for all or some components.	"Understanding Processes and Controls"	Business Acumen
ISA 700	Forming an Opinion and Reporting on Financial Statements	Signature of the Auditor	A65. In some cases, law or regulation may allow for the use of electronic signatures in the auditor's report.	"Able to assess usefulness of data transmitted in new channels"	Communication

ISA 701	Communicating Key Audit Matters in the Independent Auditor's Report	Considerations in Determining Those Matters that Required Significant Auditor Attention	A18. In addition to matters that relate to the specific required considerations in paragraph 9, there may be other matters communicated with those charged with governance that required signficiant auditor attention and that threfore may be determined to be key audit matters in accordance with paragraph 10. Such matters may include, for example, matters relevant to the audit that was performed that may not be required to be disclosed in the financial statements. For example, the implementation of a new IT system (or significnt changes to an existing IT system) during the period may be an area of significant auditor attention, in particular if such a change had a significant effect on the auditor's overall strategy or related to a signficiant risk (e.g., changes to a system affecting revenue recognition).	"Effectively Communicates with those Charged with Governance"	Communication
ISA 720	The Auditor's Responsibilities Relating to Other Information	Definitions	A4. An annual report may be made available to users in printed form, or electronically, including on the entity's website. A document (or combination of documents) may meet the definition of an annual report, irrespective of the manner in which it is made available to users.	"Able to assess usefulness of data transmitted in new channels"	Communication
ISAE 3000 (Revised)	Assurnace Engagements Other Than Audits or Reviews of Historical Financial Information	Assurance Skills and Techniques	A9. Assurance skills and techniques include: • Application of professional skepticism and professional judgment; • Planning and performing an assurance engagement, including obtaining and evaluating evidence; • Understanding information systems and the role and limitations of internal control;	"Understanding Processes and Controls" and "Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"	Business Acumen, Behavioural Competence
ISAE 3000 (Revised)	Assurnace Engagements Other Than Audits or Reviews of Historical Financial Information	Quantity and quality of available evidence	A53. The quantity or quality of available evidence is affected by: (b) Other circumstances, such as when evidence that could reasonably be expected to exist is not available because of, for example, the timing of the practitioner's appointment, an entity's document retention policy, inadequate information systems, or a restriction imposed by the responsible party.	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"	Behavioural Competence

ISAE 3400	The Examination of Prospective Financial Information	Knowledge of Business	13. The auditor should obtain a sufficient level of knowledge of the business to be able to evaluate whether all significant assumptions required for the preparation of the prospective financial information have been identified. The auditor would also need to become familiar with the entity's process for preparing prospective financial information, for example, by considering the following:• The internal controls over the system used to prepare prospective financial information and the expertise and experience of those persons preparing the prospective financial information.• The nature of the documentation prepared by the entity supporting management's assumptions.• The extent to which statistical, mathematical and computer-assisted techniques are used.• The methods used to develop and apply assumptions.• The accuracy of prospective financial information prepared in prior periods and the reasons for significant variances.	"Understanding Processes and Controls" and "Makes Use of Computer Assisted Techniques"	Business Acumen, Data Interrogation, Syntesis and Analysis
ISAE 3402	Assurance Reports on Controls at a Service Organisation	Assessing the Suitability of the Criteria	16. In assessing the suitability of the criteria to evaluate the service organization's description of its system, the service auditor shall determine if the criteria encompass, at a minimum: (a) Whether the description presents how the service organization's system was designed and implemented, including, as appropriate:... (viii) Other aspects of the service organization's control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the services provided.	"Understanding Processes and Controls" and "Risk Assessment"	Business acumen
ISAE 3402	Assurance Reports on Controls at a Service Organisation	Obtaining an Understanding of the Service Organisations System	20. The service auditor shall obtain an understanding of the service organization's system, including controls that are included in the scope of the engagement. (Ref: Para. A19–A20)	"Understanding Processes and Controls"	Business acumen
ISAE 3402	Assurance Reports on Controls at a Service Organisation	Obtaining evidence	24. When providing a type 2 report, the service auditor shall test those controls that the service auditor has determined are necessary to achieve the control objectives stated in the service organization's description of its system, and assess their operating effectiveness throughout the period. Evidence obtained in prior engagements about the satisfactory operation of controls in prior periods does not provide a basis for a reduction in testing, even if it is supplemented with evidence obtained during the current period.	"Understanding Processes and Controls"	Business Acumen
ISAE 3402	Assurance Reports on Controls at a Service Organisation	Acceptance and Continuance	Capabilities and Competence to Perform the Engagement (Ref: Para. 13(a)(i)) A7. Relevant capabilities and competence to perform the engagement include matters such as the following: • Knowledge of the relevant industry; • An understanding of information technology and systems; • Experience in evaluating risks as they relate to the suitable design of controls; and	"Understanding Processes and Controls"	Business Acumen

			• Experience in the design and execution of tests of controls and the evaluation of the results.		
ISAE 3402	Assurance Reports on Controls at a Service Organisation	Assessing the Suitability of the Criteria	A15. Paragraph 16(a) identifies a number of elements that are included in the service organization's description of its system as appropriate. These elements may not be appropriate if the system being described is not a system that processes transactions, for example, if the system relates to general controls over the hosting of an IT application but not the controls embedded in the application itself.	"Understanding Processes and Controls"	Business acumen
ISAE 3410	Assurance Engagements on Greenhouse Gas Statements	Obtaining an Understanding of the Entity's Internal Control	25L. For internal control relevant to emissions quantification and reporting, as the basis for identifying and assessing the risks of material misstatement, the practitioner shall obtain an understanding, through inquiries, about: (b) The information system, including the related business processes, and communication of emissions reporting roles and responsibilities and significant matters relating to emissions reporting	"Understanding Processes and Controls"	Business acumen
ISAE 3410	Assurance Engagements on Greenhouse Gas Statements	Obtaining an Understanding of the Entity's Internal Control	25R. The practitioner shall obtain an understanding of the following components of the entity's internal control relevant to emissions quantification and reporting as the basis for identifying and assessing risks of material misstatement: (b) The information system, including the related business processes, and communication of emissions reporting roles and responsibilities and significant matters relating to emissions reporting	"Understanding Processes and Controls"	Business acumen
ISAE 3410	Assurance Engagements on Greenhouse Gas Statements	Risks for Which Tests of Controls Are Necessary to Provide Sufficient Appropriate Evidence	A98. The quantification of emissions may include processes that are highly automated with little or no manual intervention, for example, where relevant information is recorded, processed, or reported only in electronic form such as in a continuous monitoring system, or when the processing of activity data is integrated with an information technology-based operational or financial reporting system. In such cases: • Evidence may be available only in electronic form, and its sufficiency and appropriateness dependent on the effectiveness of controls over its accuracy and completeness. • The potential for improper initiation or alteration of information to occur and not be detected may be greater if appropriate controls are not operating effectively.	"Understanding Processes and Controls"	Business acumen

ISRE 2400 (Revised)	Engagements to Review Historical Financial Statements	The Practitioner's Understanding	46. The practitioner's understanding shall include the following: (c) The entity's accounting systems and accounting records	"Understanding Processes and Controls"	Business Acumen
ISRE 2400 (Revised)	Engagements to Review Historical Financial Statements	Assignment of Engagement Teams	A31. When considering the appropriate competence and capabilities expected of the engagement team as a whole, the engagement partner may take into consideration such matters as the team's: • Technical expertise, including expertise with relevant information technology and specialized areas of accounting or assurance.	"Appropriately applies ICT related experience and knowledge"	Behavioural Competence
ISRE 2400 (Revised)	Engagements to Review Historical Financial Statements	The Practitioner's Understanding	A78. In obtaining an understanding of the entity and its environment, and of the applicable financial reporting framework, the practitioner may also consider:• The level of development and complexity of the entity's financial accounting and reporting systems and related controls through which the entity's accounting records and related information are maintained. • The entity's procedures for recording, classifying and summarizing transactions, accumulating information for inclusion in the financial statements and related disclosures.	"Understanding Processes and Controls"	Business Acumen
ISQC 1	Quality Control for Firms that Perform Audits and Reviews of Financial Statements and Other Assurance and Related Services Engagements	Human Resources, Assignment of Engagement Teams	A31. The firm's assignment of engagement teams and the determination of the level of supervision required, include for example, consideration of the engagement team's:.. · Technical knowledge and expertise, including knowledge of relevant information technology;	"Appropriately applies ICT related experience and knowledge"	Behavioral Competence
ISQC 1	Quality Control for Firms that Perform Audits and Reviews of Financial Statements and Other Assurance and Related Services Engagements	Engagement Performance	A32. The firm promotes consistency in the quality of engagement performance through its policies and procedures. This is often accomplished through written or electronic manuals, software tools or other forms of standardized documentation, and industry or subject matter-specific guidance materials.	"Appropriately applies ICT related experience and knowledge"	Behavioral Competence

ISQC 1	Quality Control for Firms that Perform Audits and Reviews of Financial Statements and Other Assurance and Related Services Engagements	Confidentiality, Safe Custody, Integrity, Accessibility and Retrievability of Engagement Documentation	A57. Whether engagement documentation is in paper, electronic or other media, the integrity, accessibility or retrievability of the underlying data may be compromised if the documentation could be altered, added to or deleted without the firm's knowledge, or if it could b e permanently lost or damaged. Accordingly, controls that the firm designs and implements to avoid unauthorized alteration or loss of engagement documentation may include those that: • Enable the determination of when and by whom engagement documentation was created, changed or reviewed; • Protect the integrity of the information at all stages of the engagement, especially when the information is shared within the engagement team or transmitted to other parties via the Internet; • Prevent unauthorized changes to the engagement documentation; and • Allow access to the engagement documentation by the engagement team and other authorized parties as necessary to properly discharge their responsibilities.	"Assessing Data Transmission and Security" and "Appropriately applies ICT related experience and knowledge"	Behavioral Competence Digital Acumen
ISQC 1	Quality Control for Firms that Perform Audits and Reviews of Financial Statements and Other Assurance and Related Services Engagements	Confidentiality, Safe Custody, Integrity, Accessibility and Retrievability of Engagement Documentation	A58. Controls that the firm designs and implements to maintain the confidentiality, safe custody, integrity, accessibility and retrievability of engagement documentation may include the following: • The use of a password among engagement team members to restrict access to electronic engagement documentation to authorized users. • Appropriate back-up routines for electronic engagement documentation at appropriate stages during the engagement. • Procedures for properly distributing engagement documentation to the team members at the start of the engagement, processing it during engagement, and collating it at the end of engagement. • Procedures for restricting access to, and enabling proper distribution and confidential storage of, hardcopy engagement documentation.	"Assessing Data Transmission and Security" and "Appropriately applies ICT related experience and knowledge"	Behavioral Competence Digital Acumen
ISQC 1	Quality Control for Firms that Perform Audits and Reviews of Financial Statements and Other Assurance and Related Services Engagements	Confidentiality, Safe Custody, Integrity, Accessibility and Retrievability of Engagement Documentation	A59. For practical reasons, original paper documentation may be electronically scanned for inclusion in engagement files. In such cases, the firm's procedures designed to maintain the integrity, accessibility, and retrievability of the documentation may include requiring the engagement teams to: • Generate scanned copies that reflect the entire content of the original paper documentation, including manual signatures, cross-references and annotations; • Integrate the scanned copies into the engagement files, including indexing and signing off on the scanned copies as necessary; and • Enable the scanned copies to be retrieved and printed as necessary. There may be legal, regulatory or other reasons for a firm to retain original paper documentation that has been scanned.	"Assessing Data Transmission and Security" and "Appropriately applies ICT related experience and knowledge"	Behavioral Competence Digital Acumen

IAPN 1000	The Examination of Prospective Financial Information	Reconciliations with Banks and Custodians	30. In entities with a high volume of financial instrument transactions, reconciliation and confirmation controls may be automated and, if so, adequate IT controls need to be in place to support them. In particular, controls are needed to ensure that data is completely and accurately picked up from external sources (such as banks and custodians) and from the entity's records and is not tampered with before or during reconciliation. Controls are also needed to ensure that the criteria on which entries are matched are sufficiently restrictive to prevent inaccurate clearance of reconciling items.	"Understanding Processes and Controls"	Business Acumen
IAPN 1000	The Examination of Prospective Financial Information	Models	47. Models may be used to value financial instruments when the price cannot be directly observed in the market. Models can be as simple as a commonly used bond pricing formula or involve complex, specifically developed software tools to value financial instruments with level 3 inputs. Many models are based on discounted cash flow calculations.	"Understanding Processes and Controls"	Business Acumen
IAPN 1000	The Examination of Prospective Financial Information	Models	49. Depending on the circumstances, matters that the entity may address when establishing or validating a model for a financial instrument include whether: ... - There are appropriate change control policies, procedures and security controls over the model.	"Understanding Processes and Controls" and "Assessing Data Transmission and Security"	Business Acumen Digital Acumenn
IAPN 1000	The Examination of Prospective Financial Information	Audit Considerations when Management Estimates Fair Values Using a Model	127. When markets become inactive or dislocated, or inputs are unobservable, management'svaluations may be more judgmental and less verifiable and, as result, may be less reliable. In such circumstances, the auditor may test the model by a combination of testing controls operated by the entity, evaluating the design and operation of the model, testing the assumptions and data used in the model, and comparing its output to a point estimate or range developed by the auditor or to other third-party valuation techniques.	"Understanding Processes and Controls"	Business Acumen
IAPN 1000	The Examination of Prospective Financial Information	Purposes and Risks of Using Financial Instruments	18. The principal types of risk applicable to financial instruments are listed below. This list is not meant to be exhaustive and different terminology may be used to describe these risks or classify the components of individual risks. Operational risk relates to the specific processing required for financial instruments. Operational risk may increase as the complexity of a financial instrument increases, and poor management of operational risk may increase other types of risk. Operational risk includes: (vi) The risk of loss resulting from inadequate or failed internal processes and systems, or from external events, including the risk of fraud from both internal and external sources;	"Understanding Processes and Controls"	Business Acumen

IAPN 1000	The Examination of Prospective Financial Information	Controls Relating to Financial Instruments	21. Often, it is the role of those charged with governance to set the tone regarding, and approve and oversee the extent of use of, financial instruments while it is management's role to manage and monitor the entity's exposures to those risks. Management and, where appropriate, those charged with governance are also responsible for designing and implementing a system of internal control to enable the preparation of financial statements in accordance with the applicable financial reporting framework. An entity's internal control over financial instruments is more likely to be effective when management and those charged with governance have: ... (c) Established information systems that provide those charged with governance with an understanding of the nature of the financial instrument activities and the associated risks, including adequate documentation of transactions;	"Understanding Processes and Controls" and "Establishes Appropriate Governance and Oversight"	Business Acumen Digital Acumenn
IAPN 1000	The Examination of Prospective Financial Information	Controls Relating to Financial Instruments	104. Procedures that may provide audit evidence to support the completeness, accuracy, and existence assertions include: - External confirmation25 of bank accounts, trades, and custodian statements. This can be done by direct confirmation with the counterparty (including the use of bank confirmations), where a reply is sent to the auditor directly. Alternatively this information may be obtained from the counterparty's systems through a data feed. Where this is done, controls to prevent tampering with the computer systems through which the information is transmitted may be considered by the auditor in evaluating the reliability of the evidence from the confirmation. If confirmations are not received, the auditor may be able to obtain evidence by reviewing contracts and testing relevant controls. External confirmations, however, often do not provide adequate audit evidence with respect to the valuation assertion though they may assist in identifying any side agreements.	"Understanding Processes and Controls" and "Assessing Data Transmission and Security"	Business Acumen Digital Acumenn
N/a	A Framework for Audit Quality: Key Elements that Create an Environment for Audit Quality	1 Input Factors; Values, Ethics and Attitudes – Engagement Level	3. The audit engagement partner is responsible for an audit engagement and therefore is directly responsible for the quality of the audit. In addition to taking responsibility for the quality of the audit, the audit engagement partner has a critical role in ensuring that the engagement team exhibits the values, ethics and attitudes necessary to support a quality audit. Key attributes are:... - The engagement team exhibits professional skepticism.	"Demonstrate intellectual curiosity, critical thinking, agility and life-long learning"	Behavioral Competence

N/a	A Framework for Audit Quality: Key Elements that Create an Environment for Audit Quality	2. Process Factors; Audit Process and Quality Control Procedures – Firm Level	14. The audit firm's policies and procedures will impact the audit process. Key attributes that contribute to audit quality are: - The audit methodology encourages individual team members to apply professional skepticism and exercise appropriate professional judgment.	"Demonstrate intellectual curiosity, critical thinking, agility and life-long learning"	Behavioral Competence
N/a	A Framework for Audit Quality: Key Elements that Create an Environment for Audit Quality	Appendix 2: 1.4 Knowledge, Skills Experience and Time – Engagement Level	42. While not all members of the team can be expected to have the same level of knowledge and experience, it is the responsibility of the audit engagement partner to ensure that the team collectively has the appropriate competences, and that external specialists, or experts, are engaged as required to meet the needs of engagement circumstances. For example, expertise may be needed in relation to such matters as:... - The entity's information systems, especially if the entity is considered to be information technology dependent.	"Understanding Processes and Controls" and "Demonstrate intellectual curiosity, critical thinking, agility and life-long learning"	Business Acumen Behavioral Competence
N/a	A Framework for Audit Quality: Key Elements that Create an Environment for Audit Quality	Appendix 2: 1.4 Knowledge, Skills Experience and Time – Engagement Level	49. Making reasonable judgments may involve partners and staff:... - Applying knowledge of business, financial accounting and reporting and information technology;	"Appropriately applies ICT related experience and knowledge"	Behavioral Competence
N/a	A Framework for Audit Quality: Key Elements that Create an Environment for Audit Quality	Appendix 2: 1.5 Knowledge, Skills Experience and Time – Firm Level	70. Professional accountancy organizations that are members of IFAC have requirements relating to CPD and the development programs used by the firms are designed to build the competence of audit professionals. Such programs often address a wide range of areas relevant to the firm's business as a whole, such as project management, information technology, and communication skills. It is important that firms dedicate sufficient time, resources and importance to training in audit and accounting matters including, where appropriate, specialized industry issues so as to provide the technical skills needed to support audit quality.	"Demonstrate intellectual curiosity, critical thinking, agility and life-long learning"	Behavioral Competence
IESBA Code of Ethics					

Handbook of the Code of Ethics for Professional Accountants	Part A - General Application of the code	Introduction and Fundamental Principles	100.5 A professional accountant shall comply with the following fundamental principles: (a) Integrity – to be straightforward and honest in all professional and business relationships. (b) Objectivity – to not allow bias, conflict of interest or undue influence of others to override professional or business judgments. (c) Professional Competence and Due Care – to maintain professional knowledge and skill at the level required to ensure that a client or employer receives competent professional services based on current developments in practice, legislation and techniques and act diligently and in accordance with applicable technical and professional standards. (d) Confidentiality – to respect the confidentiality of information acquired as a result of professional and business relationships and, therefore, not disclose any such information to third parties without proper and specific authority, unless there is a legal or professional right or duty to disclose, nor use the information for the personal advantage of the professional accountant or third parties. (e) Professional Behavior – to comply with relevant laws and regulations and avoid any action that discredits the profession.	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"	Behavioral competence
Handbook of the Code of Ethics for Professional Accountants		Professional Competence and Due Care	130.2 Competent professional service requires the exercise of sound judgment in applying professional knowleldge and skill in the performance of such service. Professional competence may be divided into two separate phases: (a) Attainment of professional competence; and (b) Maintenance of professional competence. 130.3 The maintenance of professinoal competence requires a continuing awareness and understanding of relevant technicalm professional and business developments. Continuing professional development enables a professional accountant to develop and maintain the capabilities to perform competently within the professional enviroment. ... 130.5 A prfessional accountant shall take reasonable steps to ensure that those working under the professional accountant's authority in a professional capacity have appropriate training and supervision.	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"	Behavioral competence

Handbook of the Code of Ethics for Professional Accountants	Part B – Professional Accountants in public Practice	Independence – Audit and Review Engagements	Independence comprises: (a) Independence of Mind The state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. (b) Independence in Appearance The avoidance of facts and circumstances that are so significant that a reasonable and informed third party would be likely to conclude, weighing all the specific facts and circumstances, that a firm's, or a member of the audit team's, integrity, objectivity or professional skepticism has been compromised.	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"	Behavioral competence
Handbook of the Code of Ethics for Professional Accountants	Part B – Professional Accountants in public Practice	Engagement Acceptance	210.7 A professional accountant in public practice shall evaluate the significance of threats and apply safeguards, when necessary, to eliminate them or reduce them to an acceptable level. Examples of such safeguards include: - Acquiring an appropriate understanding of the nature of the client's business, the complexity of its operations, the specific requirements of the engagement and ht purpose, nature and scope of the work to be performed; - Acquiring knowledge of relevant industries or subject matters; - Possessing or obtaining experience with relevant regulatry or reporting requirements; ...	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"	Behavioral Competence

Handbook of the Code of Ethics for Professional Accountants	Part B – Professional Accountants in public Practice	Provision of Non-Assurance Services to an Audit Client	290.197 The following IT systems services are deemed not to create a threat to independence as long as the firm's personnel do not assume a management responsibility: a. Design or implementation of IT systems that are unrelated to internal control over financial reporting; b. Design or implementation of IT systems that do not generate information forming a significant part of the accounting records or financial statements; c. Implementation of "off-the-shelf" accounting or financial information reporting software that was not developed by the firm if the customization required to meet the client's needs is not significant; and d. Evaluating and making recommendations with respect to a system designed, implemented or operated by another service provider or the client. Audit clients that are not public interest entities 290.198 Providing services to an audit client that is not a public interest entity involving the design or implementation of IT systems that (a) form a significant part of the internal control over financial reporting or (b) generate information that is significant to the client's accounting records or financial statements on which the firm will express an opinion creates a self-review threat.	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"	Behavioral Competence
PCAOB Standards					
PCAOB AS	AS 1105: Audit Evidence	Relevance and Reliability	.08 Reliability. The reliability of evidence depends on the nature and source of the evidence and the circumstances under which it is obtained. For example, in general: - Evidence obtained from a knowledgeable source that is independent of the company is more reliable than evidence obtained only from internal company sources. - The reliability of information generated internally by the company is increased when the company's controls over that information are effective. - Evidence obtained directly by the auditor is more reliable than evidence obtained indirectly. - Evidence provided by original documents is more reliable than evidence provided by photocopies or facsimiles, or documents that have been filmed, digitized, or otherwise converted into electronic form, the reliability of which depends on the controls over the conversion and maintenance of those documents.	"Assessing Data Transmission and Security" and "Keeps current with new and emerging technologies"	Digital Acumen Communication

PCAOB AS	AS 1201: Supervision of the Audit Engagement	Responsibility of the Engagement Partner for Supervision	.03 The engagement partner1 is responsible for the engagement and its performance. Accordingly, the engagement partner is responsible for proper supervision of the work of engagement team members and for compliance with PCAOB standards, including standards regarding using the work of specialists,2 other auditors,3 internal auditors,4 and others who are involved in testing controls.5 Paragraphs .05-.06 of this standard describe the nature and extent of supervisory activities necessary for proper supervision of engagement team members.	"Appropriately applies ICT related experience and knowledge"	Behavioral Competence
PCAOB AS	AS 1215: Audit Documentation	Audit Documentation Requirement	04 The auditor must prepare audit documentation in connection with each engagement conducted pursuant to the standards of the PCAOB. Audit documentation should be prepared in sufficient detail to provide a clear understanding of its purpose, source, and the conclusions reached. Also, the documentation should be appropriately organized to provide a clear link to the significant findings or issues.1 Examples of audit documentation include memoranda, confirmations, correspondence, schedules, audit programs, and letters of representation. Audit documentation may be in the form of paper, electronic files, or other media.	"Able to assess usefulness of data transmitted in new channels" and "Keeps current with new and emerging technologies"	Communication
PCAOB AS	AS 1215: Audit Documentation	Documentation of Specific Matters	.12 The auditor must document significant findings or issues, actions taken to address them (including additional evidence obtained), and the basis for the conclusions reached in connection with each engagement. Significant findings or issues are substantive matters that are important to the procedures performed, evidence obtained, or conclusions reached, and include, but are not limited to, the following: b. Results of auditing procedures that indicate a need for significant modification of planned auditing procedures, the existence of material misstatements (including omissions in the financial statements), the existence of significant deficiencies, or material weaknesses in internal control over financial reporting. Note: In an engagement conducted pursuant to Attestation Standard No. 1, Examination Engagements Regarding Compliance Reports of Brokers and Dealers, or Attestation Standard No. 2, Review Engagements Regarding Exemption Reports of Brokers and Dealers, significant findings or issues include, when applicable: (a) the assessment of, and the responses to, risks requiring special consideration by the auditor; (b) significant matters involving systems, processes, and controls to ensure the appropriateness of the subject matter and management's related assertions; and (c) the evaluation of identified instances of nonconformity with the evaluation criteria (e.g., errors, instances of non-compliance, or control deficiencies).	"Able to evaluate and respond to process failures"	Business Acumen

PCAOB AS	AS 2101: Audit Planning	Planning Activities	.07 The nature and extent of planning activities that are necessary depend on the size and complexity of the company, the auditor's previous experience with the company, and changes in circumstances that occur during the audit. When developing the audit strategy and audit plan, as discussed in paragraphs .08-.10, the auditor should evaluate whether the following matters are important to the company's financial statements and internal control over financial reporting and, if so, how they will affect the auditor's procedures: - Knowledge of the company's internal control over financial reporting obtained during other engagements performed by the auditor; - Matters affecting the industry in which the company operates, such as financial reporting practices, economic conditions, laws and regulations, and technological changes;... - The auditor's preliminary judgments about materiality, risk, and, in integrated audits, other factors relating to the determination of material weaknesses;... - Control deficiencies previously communicated to the audit committee or management;... - Knowledge about risks related to the company evaluated as part of the auditor's client acceptance and retention evaluation;	"Risk Assessment", "Understanding Existing Processes and designing appropriate response" and "Keeps current with new and emerging technologies"	Business Acumen Communication
PCAOB AS	AS 2101: Audit Planning	Multi-location Engagements	.12 Factors that are relevant to the assessment of the risks of material misstatement associated with a particular location or business unit and the determination of the necessary audit procedures include:... The degree of centralization of records or information processing;	"Understanding Processes and Controls"	Business Acumen
PCAOB AS	AS 2110: Identifying and Assessing Risks of Material Misstatement	Company Objectives, Strategies, and Related Business Risk	.15 The following are examples of situations in which business risks might result in material misstatement of the financial statements: ... - Use of information technology ("IT") (a potential related business risk might be, e.g., that systems and processes are incompatible.)	"Understanding Processes and Controls"	Business Acumen
PCAOB AS	AS 2110: Identifying and Assessing Risks of Material Misstatement	Obtaining an Understanding of Internal Control over Financial Reporting	.19 The nature, timing, and extent of procedures that are necessary to obtain an understanding of internal control depend on the size and complexity of the company; the auditor's existing knowledge of the company's internal control over financial reporting; the nature of the company's controls, including the company's use of IT; the nature and extent of changes in systems and operations; and the nature of the company's documentation of its internal control over financial reporting.	"Understanding Processes and Controls"	Business Acumen

PCAOB AS	AS 2110: Identifying and Assessing Risks of Material Misstatement	Information and Communication	.28 Information System Relevant to Financial Reporting. The auditor should obtain an understanding of the information system, including the related business processes, relevant to financial reporting, including:... The procedures, within both automated and manual systems, by which those transactions are initiated, authorized, processed, recorded, and reported;... How the information system captures events and conditions, other than transactions,16 that are significant to the financial statements; and... .29 The auditor also should obtain an understanding of how IT affects the company's flow of transactions. (See Appendix B.) Note: The identification of risks and controls within IT is not a separate evaluation. Instead, it is an integral part of the approach used to identify significant accounts and disclosures and their relevant assertions and, when applicable, to select the controls to test, as well as to assess risk and allocate audit effort.	"Understanding Processes and Controls"	Business Acumen
PCAOB AS	AS 2110: Identifying and Assessing Risks of Material Misstatement	Appendix B - Consideration of Manual and Automated Systems and Controls	.B1 While obtaining an understanding of the company's information system related to financial reporting, the auditor should obtain an understanding of how the company uses information technology ("IT") and how IT affects the financial statements. The auditor also should obtain an understanding of the extent of manual controls and automated controls used by the company, including the IT general controls that are important to the effective operations of the automated controls. That information should be taken into account in assessing the risks of material misstatement.	"Understanding Processes and Controls"	Business Acumen

PCAOB AS	AS 2110: Identifying and Assessing Risks of Material Misstatement	Appendix B - Consideration of Manual and Automated Systems and Controls	.B3 Alternatively, a company might use automated procedures to initiate, record, process, and report transactions, in which case records in electronic format would replace paper documents. When IT is used to initiate, record, process, and report transactions, the IT systems and programs may include controls related to the relevant assertions of significant accounts and disclosures or may be critical to the effective functioning of manual controls that depend on IT. .B4 The auditor should obtain an understanding of specific risks to a company's internal control over financial reporting resulting from IT. Examples of such risks include: - Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both; - Unauthorized access to data that might 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 might arise when 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 systems or programs; - Failure to make necessary changes to systems or programs; - Inappropriate manual intervention; and - Potential loss of data or inability to access data as required. .B5 In obtaining an understanding of the company's control activities, the auditor should obtain an understanding of how the company has responded to risks arising from IT.	"Understanding Processes and Controls" and "Risk Assessment"	Business Acumen

PCAOB AS	AS 2201: An Audit of Internal Control Over Financial Reporting That is Integrated with an Audit of Financial Statements	Planning the Audit	.09 The auditor should properly plan the audit of internal control over financial reporting and properly supervise the engagement team members. When planning an integrated audit, the auditor should evaluate whether the following matters are important to the company's financial statements and internal control over financial reporting and, if so, how they will affect the auditor's procedures - ... - Knowledge of the company's internal control over financial reporting obtained during other engagements performed by the auditor; - Matters affecting the industry in which the company operates, such as financial reporting practices, economic conditions, laws and regulations, and technological changes;... - The auditor's preliminary judgments about materiality, risk, and, in integrated audits, other factors relating to the determination of material weaknesses;... - Control deficiencies previously communicated to the audit committee or management;... - Knowledge about risks related to the company evaluated as part of the auditor's client acceptance and retention evaluation; and	"Risk Assessment", "Understanding Existing Processes and designing appropriate response" and "Keeps current with new and emerging technologies"	Business Acumen Communication
PCAOB AS	AS 2201: An Audit of Internal Control Over Financial Reporting That is Integrated with an Audit of Financial Statements	Identifying Entity-Level Controls	.27 As part of evaluating the period-end financial reporting process, the auditor should assess - - Inputs, procedures performed, and outputs of the processes the company uses to produce its annual and quarterly financial statements; - The extent of information technology ("IT") involvement in the period-end financial reporting process;... - The types of adjusting and consolidating entries; ...	"Understanding Processes and Controls"	Business Acumen

PCAOB AS	AS 2201: An Audit of Internal Control Over Financial Reporting That is Integrated with an Audit of Financial Statements	Understanding Likely Sources of Misstatements	.36 The auditor also should understand how IT affects the company's flow of transactions. The auditor should apply paragraph .29 and Appendix B of AS 2110, which discuss the effect of information technology on internal control over financial reporting and the risks to assess.Note: The identification of risks and controls within IT is not a separate evaluation. Instead, it is an integral part of the top-down approach used to identify significant accounts and disclosures and their relevant assertions, and the controls to test, as well as to assess risk and allocate audit effort as described by this standard..37 Performing Walkthroughs. Performing walkthroughs will frequently be the most effective way of achieving the objectives in paragraph .34. In performing a walkthrough, the auditor follows a transaction from origination through the company's processes, including information systems, until it is reflected in the company's financial records, using the same documents and information technology that company personnel use. Walkthrough procedures usually include a combination of inquiry, observation, inspection of relevant documentation, and re-performance of controls.	"Understanding Existing Processes and designing appropriate response"	Business Acumen
PCAOB AS	AS 2201: An Audit of Internal Control Over Financial Reporting That is Integrated with an Audit of Financial Statements	Relationship of Risk to the Evidence to be Obtained	.47 Factors that affect the risk associated with a control include - - The degree to which the control relies on the effectiveness of other controls (e.g., the control environment or information technology general controls); - Whether the control relies on performance by an individual or is automated (i.e., an automated control would generally be expected to be lower risk if relevant information technology general controls are effective); Note: A less complex company or business unit with simple business processes and centralized accounting operations might have relatively simple information systems that make greater use of off-the-shelf packaged software without modification. In the areas in which off-the-shelf software is used, the auditor's testing of information technology controls might focus on the application controls built into the pre-packaged software that management relies on to achieve its control objectives and the IT general controls that are important to the effective operation of those application controls.	"Understanding Processes and Controls" and "Risk Assessment"	Business Acumen

PCAOB AS	AS 2201: An Audit of Internal Control Over Financial Reporting That is Integrated with an Audit of Financial Statements	Benchmarking of Automated Controls	Benchmarking of Automated Controls .B28 Entirely automated application controls are generally not subject to breakdowns due to human failure. This feature allows the auditor to use a "benchmarking" strategy. .B29 If general controls over program changes, access to programs, and computer operations are effective and continue to be tested, and if the auditor verifies that the automated application control has not changed since the auditor established a baseline (i.e., last tested the application control), the auditor may conclude that the automated application control continues to be effective without repeating the prior year's specific tests of the operation of the automated application control. The nature and extent of the evidence that the auditor should obtain to verify that the control has not changed may vary depending on the circumstances, including depending on the strength of the company's program change controls. .B30 The consistent and effective functioning of the automated application controls may be dependent upon the related files, tables, data, and parameters. For example, an automated application for calculating interest income might be dependent on the continued integrity of a rate table used by the automated calculation. .B31 To determine whether to use a benchmarking strategy, the auditor should assess the following risk factors. As these factors indicate lower risk, the control being evaluated might be well-suited for benchmarking. As these factors indicate increased risk, the control being evaluated is less suited for benchmarking. These factors are -	"Understanding Processes and Controls" and "Makes Appropriate use of IT"	Business Acumen Digital Acumen

			- The extent to which the application control can be matched to a defined program within an application. - The extent to which the application is stable (i.e., there are few changes from period to period). - The availability and reliability of a report of the compilation dates of the programs placed in production. (This information may be used as evidence that controls within the program have not changed.) .B32 Benchmarking automated application controls can be especially effective for companies using purchased software when the possibility of program changes is remote - e.g., when the vendor does not allow access or modification to the source code. .B33 After a period of time, the length of which depends upon the circumstances, the baseline of the operation of an automated application control should be reestablished. To determine when to reestablish a baseline, the auditor should evaluate the following factors - The effectiveness of the IT control environment, including controls over application and system software acquisition and maintenance, access controls and computer operations. - The auditor's understanding of the nature of changes, if any, on the specific programs that contain the controls. - The nature and timing of other related tests. - The consequences of errors associated with the application control that was benchmarked. - Whether the control is sensitive to other business factors that may have changed. For example, an automated control may have been designed with the assumption that only positive amounts will exist in a file. Such a control would no longer be effective if negative amounts (credits) begin to be posted to the account.		
PCAOB AS	AS 2301: The Auditor's Responses to the Risks of Material Misstatement	Responses to Fraud Risks	.14 The following are examples of ways in which planned audit procedures may be modified to address assessed fraud risks: ... c. Changing the extent of the procedures applied to obtain more evidence, e.g., by increasing sample sizes or applying computer-assisted audit techniques to all of the items in an account.	"Makes Use of Computer Assisted Techniques"	Data Interrogation, Synthesis and Analysis

PCAOB AS	AS 2301: The Auditor's Responses to the Risks of Material Misstatement	Testing Controls in an Audit of Financial Statements	.17...Note: When a significant amount of information supporting one or more relevant assertions is electronically initiated, recorded, processed, or reported, it might be impossible to design effective substantive tests that, by themselves, would provide sufficient appropriate evidence regarding the assertions. For such assertions, significant audit evidence may be available only in electronic form. In such cases, the sufficiency and appropriateness of the audit evidence usually depend on the effectiveness of controls over their accuracy and completeness. Furthermore, the potential for improper initiation or alteration of information to occur and not be detected may be greater if information is initiated, recorded, processed, or reported only in electronic form and appropriate controls are not operating effectively.	"Understanding Existing Processes and designing appropriate response"	Business Acumen
PCAOB AS	AS 2301: The Auditor's Responses to the Risks of Material Misstatement	Extent of Tests of Controls	.27 Matters that could affect the necessary extent of testing of a control in relation to the degree of reliance on a control include the following:... - The nature of the control, including, in particular, whether it is a manual control or an automated control; and - For an automated control, the effectiveness of relevant information technology general controls.	"Understanding Existing Processes and designing appropriate response"	Business Acumen
PCAOB AS	AS 2301: The Auditor's Responses to the Risks of Material Misstatement	Timing of Tests of Controls	.31 Using Audit Evidence Obtained in Past Audits. For audits of financial statements, the auditor should obtain evidence during the current year audit about the design and operating effectiveness of controls upon which the auditor relies. When controls on which the auditor plans to rely have been tested in past audits and the auditor plans to use evidence about the effectiveness of those controls that was obtained in prior years, the auditor should take into account the following factors to determine the evidence needed during the current year audit to support the auditor's control risk assessments:... - The degree to which the control relies on the effectiveness of other controls (e.g., the control environment or information technology general controls);... - Whether the control relies on performance by an individual or is automated (i.e., an automated control would generally be expected to be lower risk if relevant information technology general controls are effective);16	"Understanding Existing Processes and designing appropriate response"	Business Acumen

PCAOB AS	AS 2401: Consideration of Fraud in a Financial Statement Audit	Additional Examples of Audit Procedures Performed to Respond to Assessed Fraud risks Relating to Fraudulent Financial Reporting	.54 The following are additional examples of audit procedures that might be performed in response to assessed fraud risks relating to fraudulent financial reporting: Revenue recognition. Because revenue recognition is dependent on the particular facts and circumstances, as well as accounting principles and practices that can vary by industry, the auditor ordinarily will develop auditing procedures based on the auditor's understanding of the entity and its environment, including the composition of revenues, specific attributes of the revenue transactions, and unique industry considerations. If there is an identified fraud risk that involves improper revenue recognition, the auditor also may want to consider: - Performing substantive analytical procedures relating to revenue using disaggregated data, for example, comparing revenue reported by month and by product line or business segment during the current reporting period with comparable prior periods. Computer-assisted audit techniques may be useful in identifying unusual or unexpected revenue relationships or transactions.	"Makes Use of Computer Assisted Techniques"	Data Interrogation, Synthesis and Analysis
PCAOB AS	AS 2401: Consideration of Fraud in a Financial Statement Audit	Additional Examples of Audit Procedures Performed to Respond to Assessed Fraud risks Relating to Fraudulent Financial Reporting	.54... Following the physical inventory count, the auditor may want to employ additional procedures directed at the quantities included in the priced out inventories to further test the reasonableness of the quantities counted—for example, comparison of quantities for the current period with prior periods by class or category of inventory, location or other criteria, or comparison of quantities counted with perpetual records. The auditor also may consider using computer-assisted audit techniques to further test the compilation of the physical inventory counts—for example, sorting by tag number to test tag controls or by item serial number to test the possibility of item omission or duplication.	"Makes Use of Computer Assisted Techniques"	Data Interrogation, Synthesis and Analysis

PCAOB AS	AS 2401: Consideration of Fraud in a Financial Statement Audit	Audit Procedures Performed to Specifically Address the Risk of Management Override of Controls	.61 The auditor should use professional judgment in determining the nature, timing, and extent of the testing of journal entries and other adjustments. For purposes of identifying and selecting specific entries and other adjustments for testing, and determining the appropriate method of examining the underlying support for the items selected, the auditor should consider: - The entity's financial reporting process and the nature of the evidence that can be examined. The auditor's procedures for testing journal entries and other adjustments will vary based on the nature of the financial reporting process. For many entities, routine processing of transactions involves a combination of manual and automated steps and procedures. Similarly, the processing of journal entries and other adjustments might involve both manual and automated procedures and controls. Regardless of the method, the auditor's procedures should include selecting from the general ledger journal entries to be tested and examining support for those items. In addition, the auditor should be aware that journal entries and other adjustments might exist in either electronic or paper form. When information technology (IT) is used in the financial reporting process, journal entries and other adjustments might exist only in electronic form. Electronic evidence often requires extraction of the desired data by an auditor with IT knowledge and skills or the use of an IT specialist. In an IT environment, it may be necessary for the auditor to employ computer-assisted audit techniques (for example, report writers, software or data extraction tools, or other systems-based techniques) to identify the journal entries and other adjustments to be tested.	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism" and "Makes Appropriate use of IT" and "Makes Use of Computer Assisted Techniques"	Behavioral Competence Digital Acumen Data Interrogation, Synthesis and Analysis
PCAOB AS	AS 2502: Auditing Fair Value Measurements and Disclosures	Understanding the Entity's Process for Determining Fair Value Measurements and Disclosures and the Relevant Controls, and Assessing Risk	.12 When obtaining an understanding of the entity's process for determining fair value measurements and disclosures, the auditor considers, for example: ... - Controls over the process used to determine fair value measurements, including, for example, controls over data and the segregation of duties between those committing the entity to the underlying transactions and those responsible for undertaking the valuations. ... - The role that information technology has in the process. ... - The integrity of change controls and security procedures for valuation models and relevant information systems, including approval processes.	"Understanding Processes and Controls"	Business Acumen

PCAOB AS	AS 2503: Auditing Derivative Instruments, Hedging Activities, and Investments in Securities	The Need for Special Skill or Knowledge to Plan and Perform Auditing Procedures	.05 The auditor may need special skill or knowledge to plan and perform auditing procedures for certain assertions about derivatives and securities. Examples of such auditing procedures and the special skill or knowledge required include— Obtaining an understanding of an entity's information system for derivatives and securities, including services provided by a service organization, which may require that the auditor have special skill or knowledge with respect to computer applications when significant information about derivatives and securities is transmitted, processed, maintained, or accessed electronically.	"Understanding Existing Processes and designing appropriate response"	Business Acumen
PCAOB AS	AS 2503: Auditing Derivative Instruments, Hedging Activities, and Investments in Securities	Obtaining an Understanding of Internal Control to Plan the Audit	.10 Controls should be related to management's objectives for financial reporting, operations, and compliance. For example, to achieve its objectives, management of an entity with extensive derivatives transactions may implement controls that call for— ... - The accurate transmittal of derivatives positions to the risk measurement systems.	"Understanding Existing Processes and designing appropriate response"	Business Acumen
PCAOB AS	AS 2503: Auditing Derivative Instruments, Hedging Activities, and Investments in Securities	Obtaining an Understanding of Internal Control to Plan the Audit	.11 The extent of the understanding of internal control over derivatives and securities obtained by the auditor depends on how much information the auditor needs to identify the types of potential misstatements, consider factors that affect the risk of material misstatement, design tests of controls when applicable, and design substantive tests. The understanding obtained may include controls over derivatives and securities transactions from their initiation to their inclusion in the financial statements. It may encompass controls placed in operation by the entity and by service organizations whose services are part of the entity's information system. AS 2110.28 through .32 and AS 2110.B1 through .B6 discuss the information system, including related business processes, relevant to financial reporting. Following the guidance in AS 2601, Consideration of an Entity's Use of a Service Organization, a service organization's services are part of an entity's information system for derivatives and securities if they affect any of the following:... - The accounting processing involved from the initiation of those transactions to their inclusion in the financial statements, including electronic means (such as computers and electronic data interchange) used to transmit, process, maintain, and access information	"Understanding Existing Processes and designing appropriate response"	Business Acumen
PCAOB AS	AS 2503: Auditing Derivative Instruments, Hedging Activities, and Investments in Securities	Obtaining an Understanding of Internal Control to Plan the Audit	.12 Examples of a service organization's services that would be part of an entity's information system include— ... - A pricing service providing fair values of derivatives and securities through paper documents or electronic downloads that the entity uses to value its derivatives and securities for financial statement reporting.	"Able to assess usefulness of data transmitted in new channels"	Communication

PCAOB AS	AS 2503: Auditing Derivative Instruments, Hedging Activities, and Investments in Securities	Obtaining an Understanding of Internal Control to Plan the Audit	.14 An auditor who needs information about the nature of a service organization's services that are part of an entity's information system for derivatives and securities transactions, or its controls over those services, to plan the audit may be able to gather the information from a variety of sources, such as the following: -User manuals -System overviews -Technical manuals ... - Reports by auditors, internal auditors, or regulatory authorities on the information system and other controls placed in operation by a service organization	"Understanding Existing Processes and designing appropriate response"	Business Acumen
PCAOB AS	AS 2601: Consideration of an Entity's Use of a Service Organization	Introduction and Applicability	Service organizations that provide such services include, for example, bank trust departments that invest and service assets for employee benefit plans or for others, mortgage bankers that service mortgages for others, and application service providers that provide packaged software applications and a technology environment that enables customers to process financial and operational transactions. The guidance in this section may also be relevant to situations in which an organization develops, provides, and maintains the software used by client organizations. The provisions of this section are not intended to apply to situations in which the services provided are limited to executing client organization transactions that are specifically authorized by the client, such as the processing of checking account transactions by a bank or the execution of securities transactions by a broker. This section also is not intended to apply to the audit of transactions arising from financial interests in partnerships, corporations, and joint ventures, such as working interests in oil and gas ventures, when proprietary interests are accounted for and reported to interest holders.	"Understanding Existing Processes and designing appropriate response"	Business Acumen

PCAOB AS	AS 2601: Consideration of an Entity's Use of a Service Organization	Reports on Controls Placed in Operation	.26 After obtaining a description of the relevant controls, the service auditor should determine whether the description provides sufficient information for user auditors to obtain an understanding of those aspects of the service organization's controls that may be relevant to a user organization's internal control. The description should contain a discussion of the features of the service organization's controls that would have an effect on a user organization's internal control. Such features are relevant when they directly affect the service provided to the user organization. They may include controls within the control environment, risk assessment, control activities, information and communication, and monitoring components of internal control. The control environment may include hiring practices and key areas of authority and responsibility. Risk assessment may include the identification of risks associated with processing specific transactions. Control activities may include policies and procedures over the modification of computer programs and are ordinarily designed to meet specific control objectives. The specific control objectives of the service organization should be set forth in the service organization's description of controls. Information and communication may include ways in which user transactions are initiated and processed. Monitoring may include the involvement of internal auditors.	"Understanding Processes and Controls"	Business Acumen
PCAOB AS	AS 2601: Consideration of an Entity's Use of a Service Organization	Responsibilities of Service Organizations and Service Auditors With Respect to Subsequent Events	.57 Changes in a service organization's controls that could affect user organizations' information systems may occur subsequent to the period covered by the service auditor's report but before the date of the service auditor's report. These occurrences are referred to as subsequent events. A service auditor should consider information about two types of subsequent events that come to his or her attention. .58 The first type consists of events that provide additional information about conditions that existed during the period covered by the service auditor's report. This information should be used by the service auditor in determining whether controls at the service organization that could affect user organizations' information systems were placed in operation, suitably designed, and, if applicable, operating effectively during the period covered by the engagement. .59 The second type consists of those events that provide information about conditions that arose subsequent to the period covered by the service auditor's report that are of such a nature and significance that their disclosure is necessary to prevent users from being misled. This type of information ordinarily will not affect the service auditor's report if the information is adequately disclosed by management in a section of the report containing "Other Information Provided by the Service Organization." If this information is not disclosed by the service organization, the service auditor should disclose it in a section of the report containing "Other Information Provided by the Service Auditor" and/or in the service auditor's report.	"Understanding Existing Processes and designing appropriate response"	Business Acumen

PCAOB AS	AS 2605: Consideration of the Internal Audit Function	Understanding of Internal Control	.13 The auditor obtains a sufficient understanding of the design of controls relevant to the audit of financial statements to plan the audit and to determine whether they have been placed in operation. Since a primary objective of many internal audit functions is to review, assess, and monitor controls, the procedures performed by the internal auditors in this area may provide useful information to the auditor. For example, internal auditors may develop a flowchart of a new computerized sales and receivables system. The auditor may review the flowchart to obtain information about the design of the related controls. In addition, the auditor may consider the results of procedures performed by the internal auditors on related controls to obtain information about whether the controls have been placed in operation.	"Understanding Processes and Controls"	Business Acumen
PCAOB AS	AS 2810: Evaluating Audit Results	Appendix C - Matters That Might Affect the Assessment of Fraud Risks	.C1 If the following matters are identified during the audit, the auditor should take into account these matters in the evaluation of the assessment of fraud risks, as discussed in paragraph .28 of this standard: ...a. Discrepancies in the accounting records, including: (4) Evidence of employees' access to systems and records that is inconsistent with the access that is necessary to perform their authorized duties. ...b. Conflicting or missing evidence, including: (8) Unavailable or missing electronic evidence that is inconsistent with the company's record retention practices or policies. (9) Inability to produce evidence of key systems development and program change testing and implementation activities for current year system changes and deployments. ...c. Problematic or unusual relationships between the auditor and management, including: (1) Denial of access to records, facilities, certain employees, customers, vendors, or others from whom audit evidence might be sought, including:2 Unwillingness to facilitate auditor access to key electronic files for testing through the use of computer-assisted audit techniques. Denial of access to key information technology operations staff and facilities, including security, operations, and systems development.	"Demonstrates objectivity, integrity, independence, professional competence, due care, professional skepticism"	Behavioral Competence
PCAOB AS	AS 4105: Reviews of Interim Financial Information	Appendix A - Analytical Procedures the Accountant May Consider Performing When Conducting a Review of Interim Financial Information	A2. Analytical procedures may include such statistical techniques as trend analysis or regression analysis and may be performed manually or with the use of computer-assisted techniques.	"Makes Use of Computer Assisted Techniques"	Data Interrogation, Synthesis and Analysis

PCAOB AS	AS 6115: Reporting on Whether a Previously Reported Material Weakness Continues to Exist.	Applying the Standards of the PCAOB	.19 The auditor must adhere to the standards of the PCAOB in performing an engagement to report on whether a previously reported material weakness continues to exist. Adherence to the standards involves: a. Planning the engagement, b. Obtaining an understanding of internal control over financial reporting, c. Testing and evaluating whether a material weakness continues to exist, including using the work of others, and d. Forming an opinion on whether a previously reported material weakness continues to exist.	"Understanding Processes and Controls"	Business Acumen
PCAOB QC	QC Section 40 - The Personnel Management Element of a Firm's System of Quality Control-Competencies Required by a Practitioner-in-Charge of an Attest Engagement	Competencies Expected in Performing Accounting, Auditing, and Attestation Engagements	.08In practice, the kinds of competency requirements that a firm should establish for the practitioner-in-charge of an engagement are necessarily broad and varied in both their nature and number. However, the firm's quality control policies and procedures should ordinarily address the following competencies for the practitioner-in-charge of an engagement. Firms policies and procedures should also address other competencies as necessary in the circumstances....- Technical Proficiency—Practitioners-in-charge of an engagement should possess an understanding of the applicable accounting, auditing, and attest professional standards including those standards directly related to the industry in which a client operates and the kinds of transactions in which a client engages....- Understanding the Organization's Information Technology Systems—Practitioners-in-charge of an audit engagement should have an understanding of how the organization is dependent on or enabled by information technologies; and the manner in which information systems are used to record and maintain financial information.	"Appropriately applies ICT related experience and knowledge"	Behavioral Competence
PCAOB QC	QC Section 20 - System of Quality Control for a CPA Firm's Accounting and Auditing Practice	Personnel Management	.13 Personnel Management encompasses hiring, assigning personnel to engagements, professional development, and advancement activities. Accordingly, policies and procedures should be established to provide the firm with reasonable assurance that— Those hired possess the appropriate characteristics to enable them to perform competently. Work is assigned to personnel having the degree of technical training and proficiency required in the circumstances. Personnel participate in general and industry-specific continuing professional education and other professional development activities that enable them to fulfill responsibilities assigned, and satisfy applicable continuing professional education requirements of the AICPA and regulatory agencies. fn 8	"Appropriately applies ICT related experience and knowledge"	Behavioral Competence

			Personnel selected for advancement have the qualifications necessary for fulfillment of the responsibilities they will be called on to assume.		