Key principles	
IT AUDIT INSPECTION WORK PROGRAM	
	The IT audit inspection program supports the inspection of **the IT audit work performed by the auditor as part of an audit of financial statements**. This IT audit work is usually done by IT specialists from the audit firm.

Key conclusions	
On completion of procedures in this area, assess in conclusion whether	
1	the inspection team is satisfied that the auditor adequately identified and assessed the RoMM arising from the relevant IT environment as well as the relevant risks arising from the use of IT
2	the auditor obtained sufficient and appropriate audit responses to the RoMM arising from the relevant IT environment as well as the relevant risks arising from IT.

Definitions[1]	
Access controls	Procedures designed to restrict access to on-line terminal devices, programs and data. Access controls consist of “user authentication” and “user authorization”. “User authentication” typically attempts to identify a user through unique logon identifications, passwords, access cards or biometric data. “User authorization” consists of access rules to determine the computer resources each user may access. Specifically, such procedures are designed to prevent or detect: (i) Unauthorized access to on-line terminal devices, programs and data; (ii) Entry of unauthorized transactions; (iii) Unauthorized changes to data files; (iv) The use of computer programs by unauthorized personnel; and (v) The use of computer programs that have not been authorized.
Application controls in information technology / IT Application Controls (ITAC)	Manual or automated procedures that typically operate at a business process level. Application controls can be preventative 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 financial data.
Automated Tools & Techniques	Using automated tools and techniques, the auditor may perform risk assessment procedures on large volumes of data (from the general ledger, sub-ledgers or other operational data) including for analysis, recalculations, reperformance or reconciliations. The auditor may use automated tools and techniques to understand flows of transactions and processing as part of the auditor’s procedures to understand the information system. An outcome of these procedures may be that the auditor obtains information about the entity’s organizational structure or those with whom the entity conducts business (e.g., vendors, customers, related parties). Automated tools or techniques may also be used to observe or inspect, in particular assets, for example through the use of remote observation tools (e.g., a drone).
General IT Controls (GITC)	Controls over the entity’s IT processes that support the continued proper operation of the IT environment, including the continued effective functioning of information processing controls and the integrity of information (i.e. the completeness, accuracy and validity of information) in the entity’s information system. General IT Controls are controls over the entity’s IT processes. (Appendix 6 of ISA 315 provides with examples of GITC)

[1] Definitions of Access controls, Application controls in information technology, Computer-assisted audit techniques, Information system relevant to financial reporting and Service organization are extracted from the glossary of terms as documented in the “International Auditing and Assurance Standards Board’s Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements – 2020 Edition Volume I”. Definitions of General IT Controls, Information Processing controls, IT environment, Risks arising from the use of IT and System of internal control are extracted from ISA 315 (revised 2019).

Information processing controls	Controls relating to the processing of information in IT applications or manual information processes in the entity's information system that directly address risks to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information).
Information system relevant to financial reporting	A component of internal control that includes the financial reporting system, and consists of procedures and records 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.
IT environment	The IT applications and supporting IT infrastructure, as well as the IT processes and personnel involved in those processes, that an entity uses to support business operations and achieve business strategies: (i) An IT application is a program or a set of programs that is used in the initiation, processing, recording and reporting of transactions or information. IT applications include data warehouses or report writers. (ii) The IT infrastructure comprises the network, operating systems, and databases and their related hardware and software. (iii) The IT processes are the entity's processes to manage access to the IT environment, manage program changes or changes to the IT environment and manage IT operations.
Risks arising from the use of IT	Susceptibility of information processing controls to ineffective design or operation, or risks to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information) in the entity's information system, due to ineffective design or operation of controls in the entity's IT processes.
Service organization	A third-party organization (or segment of a third-party organization) that provides services to user entities that are part of those entities' information systems relevant to financial reporting.
System of internal control	The system designed, implemented and maintained by those charged with governance, management and other personnel, to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. The system of internal control consists of five interrelated components: (i) Control environment, (ii) The entity's risk assessment process, (iii) The entity's process to monitor the system of internal control, (iv) The information system and communication, (v) Control activities.
List of Acronyms	
ATT	Automated Tools & Techniques
BCP	Business Continuity Plan
DRP	Disaster Recovery Plan
GITC	General IT Controls
IPE	Information Provided / Produced by the Entity
IT	Information Technology
ITAC	IT Application Controls
JET	Journal Entries Testing
RoMM	Risks of Material Misstatement
SDLC	Software Development Life Cycle

Step	Test objective	Reference	Inspection procedures
Risk Assessment Procedures			
1	Evaluate whether the auditor adequately identified and assessed the RoMM arising from the use of IT	ISA 315.19 & A56-A67, A140-A143 ISA 315 Appendix 5 ISA 600.17 ISA 402.14 ISA 402.16 ISA 402. 17 ISA 315.21-26 & A108, A166-A174 ISA 315.19 & A56-A67 ISA 300.8 & A8 ISA 220.14 ISA 200.14 ISA 315.19 & A56-A67 ISA 315.26 & A150 & A158 ISA 620.9 ISA 620.A14-A20 ISA 315.19 ISA 315 Appendix 2 ISA 701.9 & A18	1. Evaluate whether the auditor obtained an <u>understanding of the entity and its environment and in particular the extent to which the business model integrates the use of IT</u>. 2. Evaluate whether the auditor obtained an understanding of the relevant IT components of the Entity's System of Internal Control, when performing risk assessment procedures. 3. Evaluate whether the auditor adequately determined the <u>need for specialized skills or knowledge in IT</u> to assess the risks arising from IT and to design and perform the audit procedures to address these risks. 4. Review whether the auditor adequately identified and assessed the <u>risks arising from the use of IT</u>, including determining whether the identified risks are considered significant, specifically with regards the information systems relevant to financial reporting. 5. Assess whether the auditor identified potential <u>unusual events at IT level</u> (e.g. Implementation of a new critical IT system, major IT incidents, changes in IT organization or governance, …), evaluate whether the auditor adequately assessed the linked risks.
2	Evaluate whether the auditor designed and implemented appropriate responses to the RoMM arising from the use of IT	ISA 315.26 & A150 & A166-A172 ISA 315.30 ISA 330.5 & A1 ISA 330.7 & A16 ISA 330.8 & A24 ISA 315.26 & A173-174 ISA 701.9 & A18	1. Evaluate whether the auditor designed appropriate procedures to address the <u>specificities of the audited entity in relation to IT</u> and in particular the RoMM arising from IT. 2. When the auditor identified potential <u>unusual events at IT level</u> (e.g. Implementation of a new critical IT system…), evaluate whether the auditor adequately performed procedures to address the linked risks. If it was considered as a Key Audit Matter, review whether it has been adequately addressed in the audit report as well as in the additional report to the audit committee and that the disclosures are adequate.

Step	Test objective	Reference	Inspection procedures
Evaluation of the General IT Controls (GITC)			
2a	Ensure that the tests covered all the critical IT systems, including those located and/or managed by service organizations -	ISA 315.21 ISA 315.26 & A150 & A166-174 ISA 330.10 & A29 ISA 315.21 ISA 315.26 & A150 & A166-174 ISA 330.10 & A29 ISA 315.21 ISA 315.26 & A150 & A166-174 ISA 330.10 & A29 ISA 402.14 ISA 402.16 ISA 402. 17 ISA 330. 12 & A33	1. Review the IT specialists work performed **on the change management process** to ensure that a. the critical IT systems, and all related layers (applications, databases, operating systems and network infrastructure) were part of the scope, b. GITC related to **change management** have been adequately tested (1. design & implementation, 2. operating effectiveness), and c. the conclusion about the design, implementation and operating effectiveness of the GITCs is in line with the results of the tests. 2. Review the IT specialists work performed **on access and security controls** to ensure that a. the critical IT systems, and all related layers (applications, databases, operating systems and network infrastructure) were part of the scope, b. GITC related to **access and security controls** have been adequately tested (1. design & implementation, 2. operating effectiveness), and c. the conclusion about the design, implementation and operating effectiveness of the GITCs is in line with the results of the tests. 3. **If relevant, depending on the business model and/or the type of applications controls identified by the financial audit (e.g.: automated transfer of operational data to the accounting system)**, review the IT specialists work performed **on IT operations** to ensure that a. the critical IT systems, and all related layers (applications, databases, operating systems and network infrastructure) were part of the scope, b. GITC related to **IT operations** have been adequately tested (1. design & implementation, 2. operating effectiveness), and c. the conclusion about the design, implementation and operating effectiveness of the GITCs is in line with the results of the tests. 4. For systems located and/or managed in/by service organizations, review the work performed by IT specialists on the controls performed by third parties (if any). In particular, a. Consider the type of the third parties report to understand whether the operating effectiveness is covered and not only the design & implementation of the controls, b. Evaluate the report and consider whether the scope of the audit procedures performed by the service organization auditor addresses the identified risks (“no gap”), and consider whether the entity is covered, c. Consider the period covered by the third parties’ reports and identify if a bridge letter has been issued by the service organization, d. Evaluate the deficiencies reported and compensating controls and assess their potential impact on the financial statements, e. Verify that the audit team covered the “Complementary User Entity Controls”, i.e. the controls that are expected by the service organization to be performed completely and accurately in a timely manner by the user entity.
Evaluation of IT Application Controls (ITAC)			
2b	Ensure that the auditor evaluated relevant information processing controls / IT Application Controls and with an appropriate approach	ISA 315.21 ISA 315.26 & A166-181 & Appendix 5 ISA 330.10 & A29-A31	1. Review the list of information processing controls, automated controls and/or controls dependent on IT selected by the auditor, the approach retained to assess these controls, and review if appropriate work (e.g. test of design and implementation of control, operating effectiveness) has been conducted to support the conclusion on these controls. 2. Assess whether the systems that embed relevant ITACs have been covered by the evaluation of the GITCs and that the conclusion on the GITCs has been considered with regards ITACs.
Evaluation of relevant Information Provided by the Entity (IPE)			
2c	Evaluate whether the auditor assessed the reliability of system generated information e.g. of the relevant reports	ISA315.26 & A169 ISA 500.7 ISA 500.9 & A50-A51 ISA 330.10 & A29-A31	1. Review the list of system generated information e.g. of reports used by the auditor, the approach retained to assess the reliability of these reports (completeness and accuracy) and ensure appropriate work has been conducted to support the conclusion on the reliability of these reports.

Step	Test objective	Reference	Inspection procedures
	(produced by the IT systems)		2. Assess whether the systems generating IPEs have been covered by the evaluation of the GITCs and that the conclusion on the GITCs has been considered with regards IPE.
Support for Journal Entries Testing (JET)			
2d	Ensure that the IT audit work on Journal Entries adequately supports the audit approach to address the fraud risk	ISA 500.7 ISA 500.9 & A50-A51 ISA 240.33 & A42-A45	1. When a data analysis approach based on ATT or data analytics has been applied for Journal Entries Testing, assess the procedures applied by the audit team to validate the completeness and accuracy of electronic data for the testing of Journal Entries. 2. Review the tests of Journal Entries to ensure they are relevant and sufficient considering the Entity's environment and risk factors.
Utilization of Automated tools and techniques (ATT)			
2e	Ensure that the work with ATT and/or automated tools and techniques is based on reliable data, properly done and supported by sufficient documentation	ISA 330.7 & A16 ISA 500.7 ISA 500.9 & A50-A51 ISA 230.8 ISA 315.14 & A27 – A31	1. Evaluate if the procedures to validate data provide with enough comfort regarding completeness and accuracy of the data used for ATT and/or automated tools and techniques. 2. Review whether the documentation of the work performed with ATT to assess is sufficient to understand how the tests were performed and assess proper utilization of the ATT with regards the auditor's objectives. 3. With regards the risk assessment procedures, evaluate if the tools supporting analytical procedures, in particular when automated, were properly used.
Overall evaluation			
3	Review how the auditor used the results from the IT specialists	ISA 265.9 ISA 315.38 ISA 620.12-13	**Expected inspection procedures:** 1. Evaluate whether the auditor adequately determined that the IT audit work performed by the IT specialists is appropriate and documented for his purpose. 2. Assess whether any significant findings raised, in particular with regards GITCs and ITACs, have been properly investigated and addressed by the auditor, and communicated to the audited entity.

Additional resources	
ISACA	COBIT framework, Cybersecurity Nexus, IT knowledge (https://www.isaca.org/)
ISO	ISO 2700x series (https://www.iso.org/)
ITIL	Information Technology Infrastructure Library (ITIL)
NIST	Artificial Intelligence, Information Technology, Cybersecurity (https://www.nist.gov/)
BSI	BSI (Federal Office for Information Security, Germany) (https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html)
GDPR	GDPR (General Data Protection Regulation (EU) 2016/679) (https://en.wikipedia.org/wiki/General_Data_Protection_Regulation)