Key principles

INFORMATION & CYBERSECURITY INSPECTION WORK PROGRAM

The Information security & Cybersecurity inspection work program supports the inspection of **the measures implemented by the audit firm (“the firm”) to protect the information and in particular the audit documentation, which includes**

- **the documentation produced by the auditor, and**
- **the client documentation which has been collected during the audit engagements.**

The measures in place should ensure the confidentiality, availability and reliability of the information as well as the safe custody, integrity, accessibility or retrievability of the underlying data and the related technology.

Scope

All IT functions and systems that are required for quality management and statutory audits, including IT infrastructure (e.g. Data Centers, networks, IT platforms), systems (e.g. operational systems, database management systems) and applications (e.g. for independence analysis, audit documentation, data analytics) as well as an appropriate Internal Control System including policies, guidelines, processes, preventive measures and controls.

Key conclusions

On completion of procedures in this area, assess in conclusion whether

1	the audit firm has set up an IT organization, has implemented IT processes as well as an IT environment that supports the Internal Controls System for its audit work
2	the audit firm established a robust information security framework for both the firm and the clients’ information
3	the audit firm implemented controls to prevent and detect IT and Cybersecurity incidents and promptly react when such an incident occurs
4	the audit firm is regularly assessing its information security framework and takes corrective actions on a timely basis
5	the audit firm implemented up-to-date solutions to ensure the continuity of its activities

Definitions[1]

COBIT	A complete, internationally accepted framework for governing and managing enterprise information and technology (IT) that supports enterprise executives and management in their definition and achievement of business goals and related IT goals.
Cybersecurity	The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems.
Incident management	The process of identifying unplanned event or service interruption occurring on the system and responding in a timely manner with the objective to restore the service to its operational state.

[1] Definitions are based on the ISACA Glossary and have been updated when needed.

Information security	Ensures that within the enterprise, information is protected against disclosure to unauthorised users (confidentiality), improper modification (integrity), and non-access when required (availability).
Information security governance	The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly. It also includes the periodic assessment and evaluation of the cybersecurity program for effectiveness.
Information Technology	The hardware, software, communication and other facilities used to input, store, process, transmit and output data in whatever form.
ISO/IEC 27001	It is intended to provide the foundation for third-party audit and is harmonized with other management standards, such as ISO/IEC 9001 and 14001.
ITIL (IT Infrastructure Library)	The UK Office of Government Commerce (OGC) IT Infrastructure Library. A set of guides on the management and provision of operational IT services.
IT system monitoring	The process of reviewing a system activity (including batch processing) to identify anomalies that warrant follow-up or further investigation.
Penetration testing	Comparing the system's performance to other equivalent systems, using well-defined benchmarks.
Security incident	A series of unexpected events that involves an attack or series of attacks (compromise and/or breach of security) at one or more sites. A security incident normally includes an estimation of its level of impact. A limited number of impact levels are defined and, for each, the specific actions required and the people who need to be notified are identified.
Security awareness programs	A clearly and formally defined plan, structured approach, and set of related activities and procedures with the objective of realizing and maintaining a security-aware culture. **Scope Notes:** This definition clearly states that it is about realizing and maintaining a security aware culture, meaning attaining and sustaining security awareness at all times. This implies that a security awareness program is not a one-time effort, but a continuous process.
Vulnerability management	The process of identifying vulnerabilities (i.e., issues, weaknesses) relating to an entity's security environment and implementing timely corrective action to address the vulnerability.

List of Acronyms

BCP	Business Continuity Plan
BIA	Business Impact Analysis
CRM	Customer Relationship Management (system)
DORA[2]	Digital Operational Resilience Act
DPO	Data Protection Officer
DRP	Disaster Recovery Plan
GDPR	General Data Protection Regulation
ISO	Information Security Officer
IT	Information Technology
SDLC	Software Development Life Cycle
SLA	Service Level Agreement

[2] The final version of DORA is not available as of November 2021. In case the statutory auditors and audit firms would be excluded from the scope of DORA, the requirements of DORA which are referenced to in this work program should be read as "recommended practices" (and not as regulatory requirements).

Step	Test objective	Reference	Inspection procedures
1	Obtain an up to date understanding of the firm's IT environment, including underlying IT platforms, relevant network infrastructure, operating systems and databases as well as relevant IT processes, with a focus on the firm's system of quality management and on the performance of statutory audits	ISQC1 46 **ISQM1 32 (f)** **ISQM1 33 (a)** DORA Art. 5-13	1. Understand and evaluate the firm's IT environment including underlying IT platforms, relevant network infrastructure, operating systems and databases as well as relevant IT processes and essential data flows.
2	Obtain an up to date understanding of the firm's **governance model** regarding information and Cybersecurity	**ISQM1 32 (f)** *DORA Art. 4-5*	1. Understand and evaluate the firm's organization including roles and responsibilities for IT and information security.
		ISQC1 46, 47 **ISQM1 33**	2. Understand and evaluate the firm's policies and procedures for information and cyber security.
		DORA Art. 5	3. Understand and evaluate the risk assessment approach for IT and information security risks.
		DORA Art.21-23 **ISQM1 35**	4. Understand and evaluate the firm's internal and external monitoring activities in relation to information and cyber security.
			5. Evaluate the key changes made by the firm since the previous inspection visit, as well as current initiatives.
		GDPR	6. Evaluate the implementation of GDPR and how the firm ensures compliance to the regulations.
3	Obtain an up to date understanding of the firm's control environment as well as procedures, policies and processes regarding information and Cybersecurity	ISQC1 46 **ISQM1 32 (f)** **ISQM1 33 (a)** *DORA Art. 8*	1. Understand and evaluate the measures and controls concerning information and cyber security.
			2. Understand and evaluate the firm's plans for training and awareness on information security and Cybersecurity.
		DORA Art. 4, 7, 10, 11, 25	3. Understand and evaluate the firm's utilization, control and monitoring of IT Outsourcing and/or IT services delivered by third-parties.

Step	Test objective	Reference	Inspection procedures
4	Obtain an up to date understanding of the firm's procedures to manage information security incidents	ISQC1 46 **ISQM1 33 (a)** *DORA Art. 8-9*	1. Understand and evaluate the firm's procedures to detect, record and manage information security incidents.
		DORA Art. 10- 11	2. Understand and evaluate the firm's solutions to ensure the continuity of activities.
5	Evaluate compliance with the firm's procedures to protect the firm and the clients' information	**ISQM 1 32 (f)**	1. Test the audit firm's controls regarding acquisition, development, enhancement, implementation and operation of IT environment including IT applications as well as access to IT environment including IT applications to ensure the proper implementation and operating of the relevant IT systems.
		ISQM1 35	2. Obtain and review the results of internal and external assessments and ensure that the firm took corrective actions when applicable.
		DORA Art. 12	3. For a sample of employees, including new joiners, ensure that they participated to training and/or awareness sessions.
			4. Ensure that there is a contract with third-parties, including members of the Network when relevant, and that they include clauses about the roles and responsibilities for protection of information.
			5. For a sample of IT systems, review the rules for passwords as implemented in the system and review the list of user access rights to verify that only relevant personnel are granted access.
			6. Obtain and review the results of the last review of user access rights to ensure that the audit firm performs a regular post control of the user access rights and that actions are taken on a timely basis when exceptions are detected.
6	Evaluate compliance with the firm's procedures in case of security incidents	ISQC1 46 *DORA Art. 15* GDPR Data Breach Notification	1. For a sample of information security incidents, review the supporting documentation and ensure that actions were taken on a timely manner and in compliance with national legislation.
		ISQM1 32 (f) DORA Art. 10	2. Confirm that tests are performed on a regular basis to ensure that backups can be restored, and that DRP/BCP are effective and updated if necessary.

Additional resources	
ISACA	COBIT framework, Cybersecurity Nexus, IT knowledge (https://www.isaca.org/)
ISO	ISO/IEC 2700x series (https://www.iso.org/)
ITIL	Information Technology Infrastructure Library (ITIL)
BSI	BSI (Federal Office for Information Security, Germany) (https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html)
NIST	NIST (National Institute of Standards and Technology, USA) (https://www.nist.gov/cyberframework)
GDPR	GDPR (General Data Protection Regulation (EU) 2016/679) (https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en#legislation)

Notes

1. **Disclaimer** about the objectives of the Information security & Cybersecurity inspection work program

    - Applying the Information security & Cybersecurity inspection work program requires appropriate IT skills including information and cyber-security, IT risk management, IT governance and IT audit knowledge and skills. It is not intended that an Information security & Cybersecurity inspection work program will replace a sound education and training in IT and IT audit as well as in-depth professional experiences in the area of IT and IT audit.
    - The respective inspection team will **not** perform a detailed audit and provide **no assurance** over effectiveness of all controls and audit regulators will **not** provide any type of **certification** regarding the **level** of the **audit firm's Information security & Cybersecurity system and measures.**

2. The work program takes into consideration the Digital Operational Resilience Act (DORA), which is currently under preparation. In case audit firms are excluded from the scope of DORA, references in the work program should therefore be considered as references to "good/best practices".
   Digital Operational Resilience Act (DORA) proposal builds on European and internationally recognized technical standards or industry best practices, insofar they are fully compliant with supervisory instructions on the use and incorporation of such international standards. This regulation also covers the integrity, safety and resilience of physical infrastructures and facilities that support the use of technology and the relevant ICT-related processes and people, as part of the digital footprint of a financial entity's operations. The decision whether or not to make this enforceable to Audit firms is still not known. Nevertheless, there is an expectation that they operate to the same level to achieve industry best practices and European and internationally recognized technical standards.