ISO/IEC 27001:2022/Amd 1:2024 Test of Understanding
Level 2 – Professional

Test Syllabus

The main purpose of the ISTO Test of Understanding (the "Test") is to offer an evidence-based qualification to professionals who have demonstrated an appreciation of the intent and an accurate understanding of the requirements (and the non-requirements) of the standard, including its applicability and underlying management principles. Such knowledge and skills are crucial in providing a value-adding service related to the standard, be it implementation, advisory or auditing.

The Test of Understanding is not an auditor qualification. There are no questions directly related to auditing.

The topics set out in 1.1 to 1.3 are not intended to limit the subject matter or be all inclusive of what might be covered in the Test. Candidates will be expected to apply their knowledge to organizations with different sizes and complexity.

1.1. Applicability (A)

- ISO/IEC 27001 purpose
- ISO/IEC 27001 intended outcomes
- Scope and boundaries of an information security management system

1.2. Concepts, principles and Terminologies (Co, T)

Information security

- Information security management & information security management principles
- Typical commonly known legal requirements relevant to a sector
  (E.g. Protection of personal data, cybercrime legislation)
- Typical measurement of information security performance
  (E.g. System availability, mean time between failures, information security breaches/incidents)

ISO/IEC 27000:2018 terms and definitions

- From Clause 3.1 to Clause 3.77 (77 Terms)

Management Systems

- Risk-based thinking
- The hierarchy and interrelationship of documented information within the management system, as well as the associated risks
- Root cause analysis and simple analytical tools such as Pareto Analysis
- Application of the Plan-Do-Check-Act cycle within the management system
- Typical measurements of management system performance
  (E.g. Training hours, achievement of objectives, number of nonconformities)

ISO/IEC 27001:2022 ISMS requirements structure

- Interrelationship between leadership and commitment, policy, objectives, planning, resources, operations, monitoring and measurement, analysis and evaluation and continual improvement
- Sequence of activities in the requirements of the standard

1.3. Clause reference, Requirements and Unspecified requirements (C, U, R, AC, E)

Clause Reference (C)

- Identify the clause reference of a particular ISO/IEC 27001 requirement.
  (E.g. The requirement to determine competence is given in clause 7.2a.)

Requirements versus Unspecified requirements (R, U)

- Requirements specified in the ISO/IEC 27001 standard
  (E.g. Conduct management review)
- Differentiate from non-requirements
  (E.g. Clause 5.1 does not require a strategic plan; Clause 6.1.1 does not require a formal method for risk management or a documented risk management process.)

Key requirements of the ISO/IEC 27001 ISMS: **Management System related**

Planning

- Context, interested parties' requirements, risks/opp. & actions to address; consideration of climate change
- Leadership and commitment
- Information security policy, objectives and actions to achieve
- Roles, responsibilities and authorities
- System changes control

Performance evaluation and improvement

- Monitoring and measurement
- Analysis and evaluation
- Internal audit
- Management review
- Corrective action
- Improvement
- Management system non-requirements

Key requirements of the ISO/IEC 27001 ISMS: **Operations related**

Planning

- Information security risk assessment
- Information security risk treatment
- Statement of Applicability

Support

- Resources
- Competence and awareness
- Communication
- Documented information creation and control, and to maintain and retain

Operation

- Operational planning & control
- Information security risk assessment
- Information security risk treatment
- Annex A: Organizational controls 5.1 – 5.37
- Annex A: People controls 6.1 – 6.8
- Annex A: Physical controls 7.1 – 7.14
- Annex A: Technological controls 8.1 – 8.34
- Support and operational non-requirements

Actual documented information requirements versus Erroneous Requirements (Ac, E)

In order to provide flexibility to organizations of different sizes and background, ISO/IEC 27001 is written with minimal documentation requirements. Based on their contextual factors, organization shall determine the complexity of their documented information required to support their information security management system.

- Requirements specified in the ISO/IEC 27001 standard
  (E.g. competence documented information)
- Differentiate from non-documentation requirements
  (E.g. management system manual; documented procedure; approved supplier list)

Reference sources

The reference sources and sites detailed in this section contain information that will support your learning and better position you to pass your ISTO Test.

ISO/IEC 27000:2016
Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27001:2022/Amd 1:2024
Information security management systems — Requirements

ISO/IEC 27002:2022
Information security, cybersecurity and privacy protection — Information security controls

Reference sites *(free of charge)*

ISO Annex SL Appendix 2 (2024)	https://www.iso.org/committee/54996.html?t=-Duqtv8H-DoUiDQTNCpLN0UhREpjaZ130Orwm4_WLY97n2yln9bslL_OpNRJZCit&view=documents#section-isodocuments-top *(Note: The link above provides access to the 2024 version of Annex SL Appendix 2. It should be noted that the contents of ISO/IEC 27001:2022/Amd 1:2024 may not necessarily incorporate all the latest Annex SL changes. The ISTO Test of Understanding is based on the ISO Management System Standards (MSS) and not on Annex SL Appendix 2.)*
Centre for Cyber Security, Belgium	**Cyber Security Guide** https://ccb.belgium.be/sites/default/files/CCB-EN%20-C.pdf
European Union Agency for Network And Information Security (ENISA)	**Information security and privacy standards for SMEs** https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport
	Security guide and online tool for SMEs when going Cloud https://www.enisa.europa.eu/news/enisa-news/enisa2019s-security-guide-and-online-tool-for-smes-when-going-cloud
	A simplified approach to Risk Management for SMEs https://www.enisa.europa.eu/publications/archive/RMForSMEs

Other ISO References

International Organization for Standardization	**Glossary – Guidance on selected words used in the ISO 9000 family of standards** https://www.iso.org/files/live/sites/isoorg/files/standards/docs/en/terminology-ISO9000-family.pdf
	Guidance on the requirements for Documented Information of ISO 9001:2015 https://committee.iso.org/files/live/sites/tc176sc2/files/documents/ISO%209001%202015%20-%20Implementation%20guidance%20docs/ISO9001_2015_Guidance_on_Documented_Information.docx

J22.27001L2/240601