Preparation Guide

Edition 202306

Content

1. Overview

EXIN Information Security Management Professional based on ISO/IEC 27001 (ISMP.EN)

Scope

EXIN Information Security Management Professional based on ISO/IEC 27001 certification confirms that the professional can manage organizational, people-related, physical and technological information security risks, while respecting stakeholder interests.

This certification covers:

- information security perspectives
- risk management
- information security controls

Summary

Globalization of the economy is leading to an ever-growing exchange of information. This information crosses not only national borders but also the thin lines between private and business domains. The scope of accountability grows together with the information that is managed. This information must be protected against unauthorized access, safeguarded from accidental or malicious modification or destruction, and must remain available when needed.

There are other trends that are enhancing the importance of the information security discipline:

- Compliance requirements are increasing. Most countries have multiple laws or regulations governing the use and requiring protection of various types of data. These laws are increasing in number and their requirements are growing.
- Many industries, particularly the financial world, have regulations in addition to those imposed by a government. These are growing in number and complexity too.
- Security standards are being developed and refined at industrial, national and international levels.
- Security certifications and auditable proof that an organization is complying with security standards and/or best practices are sometimes being required as a condition of conducting business.

The international standard for information security management ISO/IEC 27001 is a widely respected and referenced standard and provides a framework for the organization and management of an information security program. Implementing a program based on this standard will serve an organization well in its goal of meeting many of the requirements faced in today's complex operating environment. A strong understanding of this standard is important to the personal development of every information security professional.

In the EXIN Information Security Management based on ISO/IEC 27001 program, the following definition is used: information security is the preservation of confidentiality, integrity, and availability of information.

Context

The EXIN Information Security Management Professional based on ISO/IEC 27001 certification is part of the EXIN Information Security Management based on ISO/IEC 27001 qualification program.

Target group

This certification is intended for all security professionals who are involved in the implementation, evaluation and reporting of an information security program, including the following roles:

- information security manager (ISM)
- Information security officer (ISO)
- line manager
- process manager
- project manager with security responsibilities.

Requirements for certification

- Successful completion of the EXIN Information Security Management Professional based on ISO/IEC 27001 exam.
- Accredited EXIN Information Security Management Professional based on ISO/IEC 27001 training, including completion of the practical assignments.

Examination details

Examination type:	Multiple-choice questions
Number of questions:	30
Pass mark:	65% (20/30 questions)
Open book:	No
Notes:	No
Electronic equipment/aides permitted:	No
Exam duration:	90 minutes

The Rules and Regulations for EXIN's examinations apply to this exam.

Bloom level

The EXIN Information Security Management Professional based on ISO/IEC 27001 certification tests candidates at Bloom levels 3 and 4 according to Bloom's Revised Taxonomy:

- Bloom level 3: Application – shows that candidates have the ability to make use of information in a context different from the one in which it was learned. This type of questions aims to demonstrate that the candidate is able to solve problems in new situations by applying acquired knowledge, facts, techniques and rules in a different, or new way. These questions usually contain a short scenario.
- Bloom level 4: Analysis – shows that candidates have the ability to break learned information down into its parts to understand it. This Bloom level is mainly tested in the Practical Assignments. The Practical Assignments aim to demonstrate that the candidate is able to examine and break information into parts by identifying motives or causes, make inferences and find evidence to support generalizations.

Training

Contact hours

The recommended number of contact hours for this training course is 21. This includes practical assignments, exam preparation and short breaks. This number of hours does not include lunch breaks, homework and the exam.

Indication study effort

112 hours (4 ECTS), depending on existing knowledge.

Training organization

You can find a list of our Accredited Training Organizations at www.exin.com.

2. Exam requirements

The exam requirements are specified in the exam specifications. The following table lists the topics of the module (exam requirements) and the subtopics (exam specifications).

Exam requirements	Exam specifications	Weight
1. Information security perspectives		**10%**
	1.1 Business interest of information security	3.3%
	1.2 Customer perspective on governance	3.3%
	1.3 Supplier's responsibilities in security assurance	3.3%
2. Risk management		**30%**
	2.1 Principles of risk management	10%
	2.2 Control risks	10%
	2.3 Deal with residual risks	10%
3. Information security controls		**60%**
	3.1 Organizational controls	20%
	3.2 Technological controls	20%
	3.3 Physical controls and people controls	20%
	Total	**100%**

Exam specifications

1 Information security perspective

1.1 Business interest of information security

The candidate can…

1.1.1 distinguish types of information based on their business value.

1.1.2 explain the characteristics of a management system for information security.

1.2 Customer perspective on governance

The candidate can…

1.2.1 explain the importance of information governance when outsourcing.

1.2.2 recommend a supplier based on security controls.

1.3 Supplier's responsibilities in security assurance

The candidate can…

1.3.1 distinguish security aspects in service management processes.

1.3.2 support compliance activities.

2 Risk management

2.1 Principles of risk management

The candidate can…

2.1.1 explain principles of analyzing risks.

2.1.2 identify risks for classified assets.

2.1.3 calculate risks for classified assets.

2.2 Control risks

The candidate can…

2.2.1 categorize controls based on confidentiality, integrity, and availability.

2.2.2 choose controls based on incident cycle stages.

2.2.3 choose relevant guidelines for applying controls.

2.3 Deal with residual risks

The candidate can…

2.3.1 distinguish risk strategies.

2.3.2 produce business cases for controls.

2.3.3 produce reports on risk analyses.

3 Information security controls

3.1 Organizational controls

The candidate can…

3.1.1 write policies and procedures for information security.

3.1.2 implement information security incident handling.

3.1.3 perform an awareness campaign in the organization.

3.1.4 implement roles and responsibilities for information security.

3.1.5 support the development and testing of a business continuity plan.

3.2 Technological controls

The candidate can…

3.2.1 explain the purpose of security architectures.

3.2.2 explain the purpose of security services.

3.2.3 explain the importance of security elements in the IT infrastructure.

3.3 Physical controls and people controls

The candidate can…

3.3.1 recommend controls for physical access.

3.3.2 recommend security controls for employment life cycle.

3. List of basic concepts

This chapter contains the terms and abbreviations with which candidates should be familiar.

Please note that knowledge of these terms alone does not suffice for the exam; the candidate must understand the concepts and be able to provide examples.

acceptance
access management
asset
attack
audit
authentication
authorization
availability
avoidance
awareness (campaigns)
business continuity (plan)
business impact analysis (BIA)
certificate authority (CA)
cloud computing
code of practice for information security
compliance
confidentiality
controls
cryptography
defense
disaster recovery plan
encryption
escrow agreement
event management
firewall
host-based intrusion detection and prevention system (host-based IDPS)
incident management
incident response plan
information security management system (ISMS)
information security perspectives
information security program
integrity
ISO/IEC 27001
ISO/IEC 27002
IT strategy
legislation
logical access control
mitigation
mitigation plan
network content filter
network-based intrusion detection and prevention system (network-based IDPS)
open design
perimeter
physical access control
Plan-Do-Check-Act (PDCA) cycle
policy
private key
problem management
procedure
protocol
public key
public key infrastructure (PKI)
Recovery Point Objective (RPO)
Recovery Time Objective (RTO)
residual risk
retention policy
risk
risk analysis
risk appetite
risk assessment
risk management framework
risk manager
risk strategy
risk treatment (plan)
security architecture
security governance
security services
Service Oriented Architecture (SOA)
Statement of Applicability (SoA)
third party
threat
topic-specific policy
Total Cost of Ownership (TCO)
transference
virtual private network (VPN)
vulnerability
zoning

4. Literature

Exam literature

The knowledge required for the exam is covered in the following literature:

A. EXIN
EXIN Information Security Management Professional based on ISO/IEC 27001 Body of Knowledge
EXIN (2023)
Go to www.exin.com. Click on 'Professionals' and then on 'Certifications' to find the certification. The free download can be found under 'Required reading'.

Additional literature

B. ISO/IEC 27000:2018
Information technology – Security techniques – Information security management systems – Overview and vocabulary
Switzerland, ISO/IEC, 2018
www.iso.org

C. ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection – Information security management systems – Requirements
Switzerland, ISO/IEC, 2022
www.iso.org

D. ISO/IEC 27002:2022
Information security, cybersecurity and privacy protection – Information security controls
Switzerland, ISO/IEC, 2022
www.iso.org

E. ISO/IEC 27005:2022
Information security, cybersecurity and privacy protection – Guidance on managing information security risks
Switzerland, ISO/IEC, 2022
www.iso.org

Comment

Additional literature is for reference and depth of knowledge only.

Literature matrix

Exam requirements	Exam specifications	Reference
1. Information security perspectives		
	1.1 Business interest of information security	A, Slides 010 – 019
	1.2 Customer perspective on governance	A, Slides 020 – 022
	1.3 Supplier's responsibilities in security assurance	A, Slides 023 – 035, 111 – 113
2. Risk management		
	2.1 Principles of risk management	A, Slides 026 – 057
	2.2 Control risks	A, Slides 009 – 011, 028 – 068, 115
	2.3 Deal with residual risks	A, Slides 028 – 035, 049 – 052
3. Information security controls		
	3.1 Organizational controls	A, Slides 023 – 025, 031 – 034, 052 – 053, 058 – 085, 091 – 095
	3.2 Technological controls	A, Slides 058 – 068, 098 – 115
	3.3 Physical controls and people controls	A, Slides 058 – 068, 086 – 097

Contact EXIN

www.exin.com