EXIN

EXIN Information Security ISO/IEC 27001

ESSENTIALS

Certified by EXIN

Preparation Guide

Edition 202602

Content

1. Overview

EXIN Information Security Essentials based on ISO/IEC 27001 (ISE.EN)

Scope

The EXIN Information Security Essentials based on ISO/IEC 27001certification confirms that the professional understands information security principles and concepts applied in the work environment and knows how to mitigate risks.

This certification includes the following topics:

- Information and security
- Threats and risks
- Security controls
- Legislation, regulations, and standards

Summary

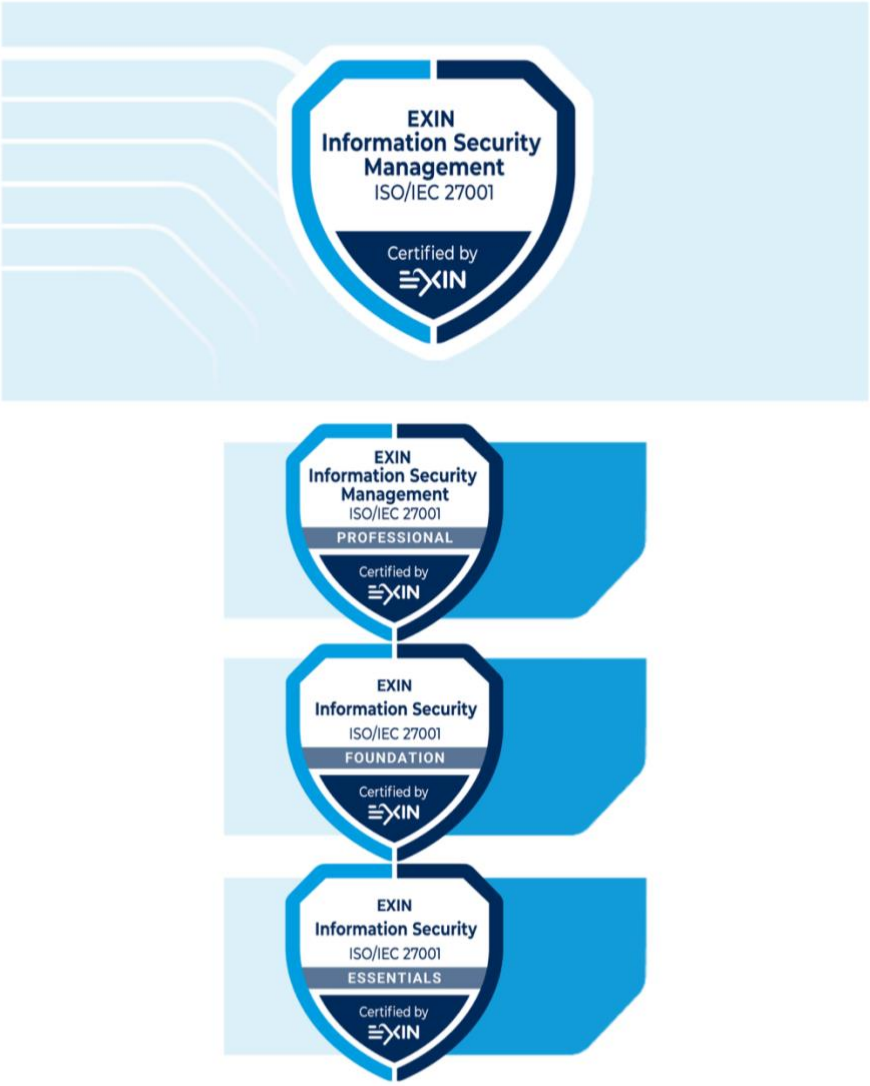
As the world becomes more connected and the globalization of the economy accelerates, organizations and individuals share more information than ever. This information often travels across national borders and moves between personal and work spaces. It also flows between companies, customers, and suppliers. With this constant exchange, the responsibility for managing and protecting information grows. 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.

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.

The EXIN Information Security Essentials based on ISO/IEC 27001 certification tests the key concepts of information security and their relationships. It validates that the candidate understands the basics of keeping information safe, thereby helping to protect an organization's information and keep daily operations secure, compliant, and running smoothly. The certification also provides a solid starting point for further learning in information security.

Context

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



Target group

The EXIN Information Security Essentials certification based on ISO/IEC 27001 certification is intended for:

- All employees handling information, across any department
- Non-IT professionals in HR, administration, management, or operations
- Entrepreneurs and small business owners
- Beginners in information processing
- Entry-level information security professionals

Requirements for certification

- Successful completion of the EXIN Information Security Essentials based on ISO/IEC 27001 exam.

Examination details

Examination type:	Multiple-choice questions
Number of questions:	20
Pass mark:	65% (13/20 questions)
Open book:	No
Notes:	No
Electronic equipment/aides permitted:	No
Exam duration:	30 minutes

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

Bloom level

The EXIN Information Security Essentials certification tests candidates at Bloom levels 1 and 2 according to Bloom's revised taxonomy:

- Bloom level 1: Remembering – relies on recall of information. Candidates will need to absorb, remember, recognize and recall.
- Bloom level 2: Understanding – a step beyond remembering. Understanding shows that candidates comprehend what is presented and can evaluate how the learning material may be applied in their own environment. This type of questions aims to demonstrate that the candidate is able to organize, compare, interpret and choose the correct description of facts and ideas.

Training

Contact hours

The recommended number of contact hours for this training course is 7. This includes group assignments, exam preparation and short breaks. This number of hours does not include lunch breaks, homework and the exam.

Indication study effort

28 hours (1 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 and security		**30%**
	1.1 Concepts relating to information security management	5%
	1.2 Reliability aspects	10%
	1.3 Securing information in the organization	15%
2. Threats and risks		**20%**
	2.1 Threats and risks	20%
3. Security controls		**45%**
	3.1 Organizational controls	17.5%
	3.2 People controls	5%
	3.3 Physical controls	5%
	3.4 Technical controls	17.5%
4. Legislation, regulations, and standards		**5%**
	4.1 Legislation and regulations	2.5%
	4.2 Standards	2.5%
	Total	**100%**

Exam specifications

1 Information and security

1.1 Concepts relating to information

The candidate can…

1.1.1 explain information security management concepts.

1.2 Reliability aspects

The candidate can…

1.2.1 explain the value of the CIA-triangle.

1.3 Securing information in the organization

The candidate can…

1.3.1 outline the objectives and the content of an information security policy.

1.3.2 outline roles and responsibilities relating to information security.

2 Threats and risks

2.1 Threats and risks

The candidate can…

2.1.1 explain threat, risk, and risk management.

2.1.2 describe types of damage.

2.1.3 describe risk strategies.

2.1.4 describe risk analysis.

3 Security controls

3.1 Organizational controls

The candidate can…

3.1.1 explain how to classify information assets.

3.1.2 describe controls to manage access to information.

3.1.3 explain threat and vulnerability management, project management, and incident management in information security.

3.1.4 explain the value of business continuity.

3.2 People controls

The candidate can…

3.2.1 explain how to attain awareness regarding information security.

3.3 Physical controls

The candidate can…

3.3.1 describe physical entry controls.

3.4 Technical controls

The candidate can…

3.4.1 outline how to manage information assets.

3.4.2 name controls that ensure network security.

3.4.3 describe technical controls to manage access.

3.4.4 describe how to protect information systems against malware, phishing, and spam.

4 Legislation, regulations, and standards

4.1 Legislation and regulations

The candidate can…

4.1.1 give examples of legislation and regulations relating to information security.

4.2 Standards

The candidate can…

4.2.1 outline the ISO/IEC 27000, ISO/IEC 27001, and ISO/IEC 27002 standards.

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.

access control
accountability
annualized loss expectancy (ALE)
annualized rate of occurrence (ARO)
asset
auditability
authentication
authorization
availability
backup
biometrics
business continuity management (BCM)
business continuity plan
certificate
change management
chief information security officer (CISO)
classification
code of conduct
compliance
confidentiality
controls

- corrective
- detective
- insurance
- preventive
- reductive
- repressive (suppressive)

cryptography
cyber crime
damage

- direct damage
- indirect damage

data
digital signature
due care
due diligence
escalation
exposure
(business) impact
incident cycle
information
information analysis
information management
information security management system (ISMS)
information security manager (ISM)
information security officer (ISO)
information security policy
information security strategy
information system
integrity
likelihood
non-disclosure agreement (NDA)
Plan, Do, Check, Act (PDCA)
personally identifiable information (PII)
phishing
privacy
public key infrastructure (PKI)
reliability
risk
risk analysis

- qualitative risk analysis
- quantitative risk analysis

risk assessment
risk management
risk strategy

- risk avoiding
- risk bearing (risk acceptance)
- risk neutral

risk treatment
security incident
segregation of duties
single loss expectancy (SLE)
stand-by arrangement
threat

- human threat
- non-human threat

threat agent
validation
verification
virtual private network (VPN)
vulnerability

4. Literature

Exam literature

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

A. Baars, H., Hintzbergen, J., and Hintzbergen, K.
Foundations of Information Security – Based on ISO 27001 and ISO 27002
Van Haren Publishing: 4th fully revised edition, 2023
ISBN: 978 94 018 0958 0 (hardcopy)
ISBN: 978 94 018 0959 7 (eBook)
ISBN: 978 94 018 0960 3 (ePub)

Literature matrix

Exam requirements	Exam specifications	Reference
1. Information and security		
	1.1 Concepts relating to information security management	Chapters 3.1 – 3.3, 4.7 – 4.9
	1.2 Reliability aspects	Chapters 3.4, 4.4 – 4.6
	1.3 Securing information in the organization	Chapters 4.2, 4.3, 4.11 – 4.14, 5.1 – 5.6, 5.14, 5.19 – 5.23, 5.35, 7.7, 7.9, 7.10, 8.30
2. Threats and risks		
	2.1 Threats and risks	Chapters 3.5, 3.7, 3.9 – 3.11
3. Security controls		
	3.1 Organizational controls	Chapters 3.6.2, 3.6.3, 5.3, 5.7 – 5.18, 5.24 – 5.30, 5.35, 5.36, 6.8
	3.2 People controls	Chapters 6
	3.3 Physical controls	Chapters 7
	3.4 Technical controls	Chapters 4.10, 8
4. Legislation, regulations, and standards		
	4.1 Legislation and regulations	Chapters 5.31 – 5.34
	4.2 Standards	Chapters 1, 3.6, 3.12, 4.1, 4.12, 5.36

EXIN

Certified for what’s next

Contact EXIN

www.exin.com