
# Preparation Guide

Edition 201804

# Content

1. Overview 4
2. Exam requirements 7
3. List of Basic Concepts 11
4. Literature 13

# 1. Overview

EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.EN)

### Scope

EXIN Information Security Foundation based on ISO/IEC 27001 is a certification that validates a professional's knowledge about:

- Information and security: the concept, the value, the importance and the reliability of information;
- Threats and risks: the concepts of threat and risk and the relationship with the reliability of information;
- Approach and organization: the security policy and security organization including the components of the security organization and management of (security) incidents;
- Measures: the importance of security measures including physical, technical and organizational measures
  and
- Legislation and regulations: the importance and impact of legislation and regulations.

### Summary

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is gaining importance in the Information Technology (IT) world. Globalization of the economy is leading to an ever-increasing exchange of information between organizations (their employees, customers and suppliers) and an explosion in the use of networked computers and computing devices.

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 EXIN's Information Security modules the following definition is used: Information Security deals with the definition, implementation, maintenance, compliance and evaluation of a coherent set of controls (measures) which safeguard the availability, integrity and confidentiality of the (manual and automated) information supply.

In the module EXIN Information Security Foundation based on ISO/IEC 27001, the basic concepts of information security and their relationships are tested. One of the objectives of this module is to raise the awareness that information is valuable and vulnerable, and to learn which measures are necessary to protect information.

## Context

The Certificate EXIN Information Security Foundation based on ISO/IEC 27001 is part of the qualification program Information Security. The module is followed up by the Certificates EXIN Information Security Management Professional based on ISO/IEC 27001 and EXIN Information Security Management Expert based on ISO/IEC 27001.


## Target group

The examination for EXIN Information Security Foundation based on ISO/IEC 27001 is intended for everyone in the organization who is processing information. The module is also suitable for entrepreneurs of small independent businesses for whom some basic knowledge of information security is necessary.
This module can be a good start for new information security professionals.

## Requirements for certification

- Successful completion of the EXIN Information Security Foundation exam.

## Examination details

| | |
|---|---|
| Examination type: | Multiple-choice questions |
| Number of questions: | 40 questions |
| Pass mark: | 65% |
| Open book/notes: | No |
| Electronic equipment/aides permitted: | No |
| Time allotted for examination: | 60 minutes |

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

### Bloom level

The EXIN Information Security Foundation based on ISO/IEC 27001 certification tests candidates at Bloom Level 1 and Level 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. This is the building block of learning before candidates can move on to higher levels.
- 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 minimum number of contact hours for the course is 14. This number includes group assignments, exam preparation and short coffee breaks. Not included are: homework, the logistics related to the exam session, the exam session and lunch breaks.

### Indication study effort

60 hours, depending on existing knowledge

### Training provider

You can find a list of our accredited training providers 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 requirement | Exam specification | Weight |
|---|---|---|
| **1. Information and Security** | | **10%** |
| | 1.1 The Concept of Information | 2.5% |
| | 1.2 Value of Information | 2.5% |
| | 1.3 Reliability Aspects | 5% |
| **2. Threats and Risks** | | **30%** |
| | 2.1 Threats and Risks | 15% |
| | 2.2 Relationships between Threats, Risks and the Reliability of Information | 15% |
| **3. Approach and Organization** | | **10%** |
| | 3.1 Security Policy and Security Organization | 2.5% |
| | 3.2 Components | 2.5% |
| | 3.3 Incident Management | 5% |
| **4. Measures** | | **40%** |
| | 4.1 Importance of Measures | 10% |
| | 4.2 Physical Security Measures | 10% |
| | 4.3 Technical Measures | 10% |
| | 4.4 Organizational Measures | 10% |
| **5. Legislation and Regulation** | | **10%** |
| | 5.1 Legislation and Regulations | 10% |
| | Total | 100% |

## Exam specifications

**1 Information and Security**

1.1 The concept of Information

The candidate can …

1.1.1 Explain the difference between data and information.

1.1.2 Describe the storage medium that forms part of the basic infrastructure.

1.2 Value of Information

The candidate can …

1.2.1 Describe the value of data/information for organizations.

1.2.2 Describe how the value of data/information can influence organizations.

1.2.3 Explain how applied information security concepts protect the value of data/information.

1.3 Reliability Aspects

The candidate can …

1.3.1 Name the reliability aspects of information.

1.3.2 Describe the reliability aspects of information.

**2 Threats and Risks**

2.1 Threat and Risk

The candidate can …

2.1.1 Explain the concepts threat, risk and risk analysis.

2.1.2 Explain the relationship between a threat and a risk.

2.1.3 Describe various types of threats.

2.1.4 Describe various types of damage.

2.1.5 Describe various risk strategies.

2.2 Relationships between threats, risks and the reliability of information

The candidate can …

2.2.1 Recognize examples of the various types of threats.

2.2.2 Describe the effects that the various types of threats have on information and the processing of information.

**3 Approach and Organization**

3.1 Security Policy and Security Organization

The candidate can…

3.1.1 Outline the objectives and the content of a security policy.

3.1.2 Outline the objectives and the content of a security organization.

3.2 Components

The candidate can..

3.2.1 Explain the importance of a code of conduct.

3.2.2 Explain the importance of ownership.

3.2.3 Name the most important roles in the information security organization.

3.3 Incident Management

The candidate can..

3.3.1 Summarize how security incidents are reported and what information is required.
3.3.2 Give examples of security incidents.
3.3.3 Explain the consequences of not reporting security incidents.
3.3.4 Explain what an escalation entails (functionally and hierarchically).
3.3.5 Describe the effects of escalation within the organization.
3.3.6 Explain the incident cycle.

## 4 Measures

4.1 Importance of Measures

The candidate can..

4.1.1 Describe various ways in which security measures may be structured or arranged.
4.1.2 Give examples for each type of security measure.
4.1.3 Explain the relationship between risks and security measures.
4.1.4 Explain the objective of the classification of information.
4.1.5 Describe the effect of classification.

4.2 Physical Security Measures

The candidate can…

4.2.1 Give examples of physical security measures.
4.2.2 Describe the risks involved with insufficient physical security measures.

4.3 Technical Measures

The candidate can…

4.3.1 Give examples of technical security measures.
4.3.2 Describe the risks involved with insufficient technical security measures.
4.3.3 Understand the concepts cryptography, digital signature and certificate.
4.3.4 Name the three steps for online banking (PC, web site, payment).
4.3.5 Name various types of malicious software.
4.3.6 Describe the measures that can be used against malicious software.

4.4 Organizational Measures

The candidate can…

4.4.1 Give examples of organizational security measures.
4.4.2 Describe the dangers and risks involved with insufficient organizational security measures.
4.4.3 Describe access security measures such as the segregation of duties and the use of passwords.
4.4.4 Describe the principles of access management.
4.4.5 Describe the concepts identification, authentication and authorization.
4.4.6 Explain the importance to an organization of a well set-up Business Continuity Management.
4.4.7 Make clear the importance of conducting exercises.

## 5 Legislation and Regulations

5.1 Legislation and Regulations

The candidate can…

5.1.1 Explain why legislation and regulations are important for the reliability of information.

5.1.2 Give examples of legislation related to information security.

5.1.3 Give examples of regulations related to information security.

5.1.4 Indicate possible measures that may be taken to fulfill the requirements of legislation and regulations.

# 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
Asset

Audit
Authentication
Authenticity
Authorization
Availability
Backup
Biometrics
Botnet
Business Continuity Management (BCM)
Business Continuity Plan (BCP)
Business Assets
Category
Certificate
Change Management
Classification (grading)
Clear desk policy
Code of conduct
Code of practice for information security (ISO/IEC 27002)
Completeness
Compliance
Computer criminality legislation
Confidentiality
Continuity
Controls
Copyright legislation
Corrective
Correctness
Cryptography
Cyber crime
Damage
Data
Detective
Digital signature
Direct damage
Disaster
Disaster Recovery Plan (DRP)
Encryption
Escalation
- o Functional escalation
- o Hierarchical escalation

Exclusivity
Hacking
Hoax
Identification
Impact
Incident cycle
Indirect damage
Information
Information analysis
Information architecture
Information management
Information security review
Information system
Infrastructure
Integrity
Interference
ISO/IEC 27001
ISO/IEC 27002

Key
Logical access management
Managing business assets
Maintenance door
Malware
Non-disclosure agreement
Non-repudiation
Patch
Personal data protection legislation
Personal firewall
Phishing
Precision
Preventive
Priority
Privacy
Production factor
Public Key Infrastructure (PKI)
Public records legislation

Qualitative risk analysis
Quantitative risk analysis
Reductive
Redundancy
Reliability of information
Repressive
Risk
Risk analysis
Risk assessment (Dependency & Vulnerability analysis)
o Risk avoiding
o Risk bearing
Risk management
o Risk neutral
Risk strategy
Robustness
Rootkit
Secret authentication information
Security in development
Security event
Security incident
Security measure
Security Organization
Security Policy
Security regulations for the government
Segregation of duties
Social engineering
Spam
Spyware
Stand-by arrangement
Storage medium
System acceptance testing
Threat
Timeliness
Trojan
Uninterruptible Power Supply (UPS)
Urgency
User access provisioning
Validation
Verification
Virtual Private Network (VPN)
Virus
Vulnerability
Worm

# 4. Literature

## Exam literature

The knowledge required for the EXIN Information Security Foundation based on ISO/IEC 27001 exam is covered in the following literature:

**A.** Hintzbergen, J., Hintzbergen, K., Smulders, A. and Baars, H.
**Foundations of Information Security – Based on ISO 27001 and ISO 27002**
Van Haren Publishing, 3rd edition, 2015
ISBN 978 94 018 0012 9
eBook 978 94 018 0541 4

## Literature matrix

| Exam requirement | Exam specification | Literature |
|---|---|---|
| **1. Information and Security** | | |
| | 1.1 The Concept of Information | Ch. 3 and §4.10 |
| | 1.2 Value of Information | Ch. 3 and 4 |
| | 1.3 Reliability Aspects | Ch. 3 and 4 |
| **2. Threats and Risks** | | |
| | 2.1 Threats and Risks | Ch. 3 |
| | 2.2 Relationships between Threats, Risks and the Reliability of Information | Ch. 3 and 11 |
| **3. Approach and Organization** | | |
| | 3.1 Security Policy and Security Organization | Ch. 3, 5 and 6 |
| | 3.2 Components | Ch. 6, 7, 8 and 13 |
| | 3.3 Incident Management | Ch. 3, 15 and 16 |
| **4. Measures** | | |
| | 4.1 Importance of Measures | Ch. 3, 8 and 16 |
| | 4.2 Physical Security Measures | Ch. 3 and 11 |
| | 4.3 Technical Measures | Ch. 6, 10, 11 and 12 |
| | 4.4 Organizational Measures | Ch. 3, 6, 9, 17 and 18 |
| **5. Legislation and Regulation** | | |
| | 5.1 Legislation and Regulations | Ch. 18 |
| | | |

# Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER