Preparation Guide

Edition 201811

Content

1. Overview

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

Scope

The module Information Security Management Professional based on ISO/IEC 27001 (ISMP.EN) tests understanding of the organizational and managerial aspects of information security.

The subjects of this module are:

- Information security perspectives: business, customer, service provider/supplier
- Risk Management: analysis, controls, remaining risks
- Information security controls: organizational, technical, physical.

Summary

Information security is the preservation of confidentiality, integrity and availability of information (ISO/IEC 27000 definition).

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 core activities of many companies now completely rely on IT. Enterprise resource planning (ERP) management systems, the control systems that govern how a building runs or a manufacturing machine functions, day-to-day communications - everything - runs on computers. The vast majority of information - the most valuable commodity in the world - passes through IT. Information is crucial for the continuity and proper functioning of both individual organizations and the economies they fuel; this information must be protected against access by unauthorized people, protected against accidental or malicious modification or destruction and must be available when it is needed. Companies and individual users of technology are also beginning to understand how important security is and are beginning to make choices based on the security of the technology or service.

There are other important trends that are increasing 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, too are growing in number and complexity.
- Security standards are being developed and refined at industrial, national and international levels.
- Security certifications and auditable proof that an organization is complying to security standards and/or best practices are sometimes being demanded as a condition of doing business.

The international standard for Information Security Management, ISO/IEC 27001:2013 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 which safeguard the availability, integrity and confidentiality of the (manual and automated) information supply.

Context

The Information Security Management Professional Certificate builds on the Information Security Foundation Certificate in which the basic concepts of information security are tested.

Target group

Security professionals. This module is intended for everyone who is involved in the implementation, evaluation and reporting of an information security program, such as an Information Security Manager (ISM), Information Security Officer (ISO) or a Line Manager, Process Manager or Project Manager with security responsibilities.

Basic knowledge of Information Security is recommended, for instance through the EXIN Information Security Foundation based on ISO/IEC 27001 certification.

Requirements for certification

- The Information Security Management Professional training course with an EXIN accredited training organization (ATO), including having successfully fulfilled the two practical assignments as part of the course.
- Successful completion of the exam EXIN Information Security Management Professional based on ISO/IEC 27001.

Examination details

Examination type:	Multiple-choice questions
Number of questions:	30 questions
Pass mark:	65%
Open book/notes:	No
Electronic equipment/aides permitted:	No
Time allotted for examination:	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: Applying – 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. The question usually contains a short scenario.
- Bloom level 4: Analyzing – shows that candidates have the ability to break learned information 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 minimum number of contact hours for the course is 20. This number includes practical 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

120 hours, 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 requirement	Exam specification	Weight
1. Information Security Perspectives		**10%**
	1.1 The candidate understands the business interest of information security.	3.3%
	1.2 The candidate understands the customer perspective on governance.	3.3%
	1.3 The candidate understands the supplier's responsibilities in security assurance.	3.3%
2. Risk Management		**30%**
	2.1 The candidate understands the principles of risk management.	10%
	2.2 The candidate knows how to control risks.	10%
	2.3 The candidate knows how to deal with remaining risks.	10%
3. Information Security Controls		**60%**
	3.1 The candidate has knowledge of organizational controls.	20%
	3.2 The candidate has knowledge of technical controls.	20%
	3.3 The candidate has knowledge of physical, employment-related and continuity controls.	20%
	Total	100%

Exam specifications

1 Information Security Perspective

1.1 The candidate understands the 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 The candidate understands the 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 assurance controls.

1.3 The candidate understands the 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 The candidate understands the 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 The candidate knows how to control risks.
The candidate can…
- 2.2.1 categorize controls based on Confidentiality, Integrity and Availability (CIA).
- 2.2.2 choose controls based on incident cycle stages.
- 2.2.3 choose relevant guidelines for applying controls.

2.3 The candidate knows how to deal with remaining 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 The candidate has knowledge of 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.

3.2 The candidate has knowledge of technical 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 The candidate has knowledge of physical, employment-related and continuity controls. The candidate can…

- 3.3.1 recommend controls for physical access.
- 3.3.2 recommend security controls for employment life cycle.
- 3.3.3 support the development and testing of a business continuity plan.

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
Delphi
disaster recovery plan
encryption
escrow agreement
event management
FAIR
firewall
Host-Based Intrusion Detection and Protection System (Host-Based IDPS)
incident management
incident response plan
Information Security Management System (ISMS)
information security perspectives
information security program
integrity
Intrusion Detection System
ISO/IEC 27001
ISO/IEC 27002
IT strategy
legislation
logical access control
Microsoft Risk Management Approach
mitigation
mitigation plan
network content filter
Network-Based Intrusion Detection and Protection 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
Statement of Applicability
third party
threats
topic-specific policy
Total Cost of Ownership (TCO)
Service Oriented Architecture (SOA)
transference
Virtual Private Network (VPN)
vulnerability
zoning

4. Literature

Exam literature

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

A. Cazemier, J.A., Overbeek, P. and Peters, L.
Information Security Management with ITIL V3
Van Haren Publishing: 2010
ISBN: 978 90 8753 552 0

B. Whitman, M.E., Mattord, H.J.
Management of Information Security
Cengage learning: 2018 (sixth edition)
ISBN: 978 1 337 40571 3
https://www.cengagebrain.co.uk/shop/isbn/9780357192795

C. ISO/IEC 27001:2017 (EN)
Information technology – Security techniques – Information security management systems – Requirements
Switzerland, ISO/IEC, 27001

Additional literature

D. BSI-standard 100-2
IT-Grundschutz Methodology
Bundesamt für Sicherheit in der Informationstechnik
English version available for download on Partnernet or http://bit.ly/bsi-standard_100-2

E. ISO/IEC 27005:2018 (EN)
Information technology -- Security techniques -- Information security risk management
Switzerland, ISO/IEC, 2018
www.iso.org

F. Pfleeger, Charles P. and Pfleeger, Shari Lawrence
Security in Computing, 4th edition
Upper Saddle River NJ, Prentice Hall, 2006
ISBN 978 0132390774

G. ISO/IEC 27000:2018 (EN)
Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
Switzerland, ISO/IEC, 2018
www.iso.org

H. ISO/IEC 27002:2017 (EN)
Information technology -- Security techniques – Code of practice for information security controls
Switzerland, ISO/IEC, 2017
www.iso.org

Comment

- Additional literature is for reference and depth of knowledge only.
- U.S. trainers and candidates can use the international version of literature item **B**. The book is exactly the same, apart from ISBN and book cover.
- Literature **B** provides a **Glossary** of terms which, if related to the Chapters mentioned in the overview of the literature below, are basic concepts for the exams.
- Literature **B** Chapter 6, Models on page 222 will not be tested.
- Literature **B** Chapter 6, Figure 6-3 on page 230; the arrow should turn right instead of left (Plan – Do – Check – Act).

Literature matrix

Exam requirement	Exam specification	Literature
1. Information Security Perspectives		
	1.1 The candidate understands the business interest of information security.	A: §1.1.1-1.1.4, §2.1, Ch. 3, §5.6 B: §1.1, §6.2
	1.2 The candidate understands the customer perspective on governance.	A: §5.3.4, §5.7, Annex A C: Annex A 15
	1.3 The candidate understands the supplier's responsibilities in security assurance.	A: Ch. 4, Annex A B: §1.1, §9.2, §9.4 C: Annex A 12.7, 15, 18
2. Risk Management		
	2.1 The candidate understands the principles of risk management.	A: §4.3 B: Ch. 6 C: Annex A 8
	2.2 The candidate knows how to control risks.	A: §2.1, §3.2 B: Ch. 5, §6.2, Ch. 7, §8.3 C: Annex A 6, 14
	2.3 The candidate knows how to deal with remaining risks.	A: §2.1, §4.5 B: Ch. 7, §12.2 C: §7.5, Annex A 16
3. Information Security Controls		
	3.1 The candidate has knowledge of organizational controls.	A: §2.1, §3.2, §4.5, §5.2, 5.3, §5.5, Annex A B: Ch. 10, §2.4, §3.3, Ch. 4, Ch. 5, §7.1, Ch. 8 C: Ch. 5, Annex A 5, 6.1, 7, 9, 16
	3.2 The candidate has knowledge of technical controls.	A: Ch. 2 B: Ch. 8, Ch. 12 C: Annex A 9, §12.1-12.4, §13.1-13.2
	3.3 The candidate has knowledge of physical, employment-related and continuity controls.	A: §2.2, §5.3 B: Ch. 10, Ch. 11, §12.1 C: Annex A 7, 11, 17

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER