COURSEWARE

Information Security Management Professional based on ISO-IEC 27001

Courseware - English

Revised edition

Van Haren PUBLISHING

EXIN INFORMATION SECURITY MANAGEMENT PROFESSIONAL based on ISO/IEC 27001

Information Security Management Professional
based on ISO/IEC 27001
Courseware revised edition – English

Colofon

Title:	Information Security Management Professional based on ISO/IEC 27001 Courseware revised edition – English
Authors:	Ing. Ruben Zeegers CISSP RSE
Publisher:	Van Haren Publishing, Zaltbommel
ISBN Hard Copy:	978 94 018 036 56
Edition:	First edition, first print, December 2017
	Second edition, first print September 2018
Design:	Van Haren Publishing, Zaltbommel
Copyright:	© Van Haren Publishing 2018
	For further information about Van Haren Publishing please e-mail us at: info@vanharen.net or visit our website: www.vanharen.net

The Certificate EXIN Information Security Management Professional 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 Advanced based on ISO/IEC 27001 and EXIN Information Security Management Expert based on ISO/IEC 27001.

About the Courseware

The Courseware was created by experts from the industry who served as the author(s) for this publication. The input for the material was based on existing publications and the experience and expertise of the author(s). The material has been revised by trainers who also have experience working with the material. Close attention was also paid to the key learning points to ensure what needs to be mastered.

The objective of the courseware is to provide maximum support to the trainer and to the student, during his or her training. The material has a modular structure and according to the author(s) has the highest success rate should the student opt for examination. For this reason, the Courseware has also been accredited, wherever applicable.

In order to satisfy the requirements for accreditation the material must meet certain quality standards. The structure, the use of certain terms, diagrams and references are all part of this accreditation. Additionally, the material must be made available to each student in order to obtain full accreditation. To optimally support the trainer and the participant of the training assignments, practice exams and results have been provided with the material.

Direct reference to advised literature is also regularly covered in the sheets so that students can easily find additional information concerning a particular topic. The decision to separate note pages (handouts) from the Courseware was to encourage students to take notes throughout the material.

Although the courseware is complete, the possibility that the trainer may deviate from the structure of the sheets or chooses to not refer to all the sheets or commands does exist. The student always has the possibility to cover these topics and go through them on their own time. It is strongly recommended to follow the structure of the courseware and publications for maximum exam preparation.

The courseware and the recommended literature are the perfect combination to learn and understand the theory.

- Van Haren Publishing

Table of content

Timetable

Day 1

09:00 - 9:30	Introduction, About this course
09:30 - 10:45	1.1 Business perspective
10:45 - 12:00	1.2 Customer perspective
10:30 - 11:15	lunch
12:30 - 15:00	Practical assignment 1
12:30 - 13:00	Lunch
15:00 - 17:00	1.3 Provider / supplier perspective

Day 2

09:00 - 10:30	2.1 Risk Analysis
10:30- 12:00	2.2 Security Controls
12:00- 12:30	lunch
12:30 - 14:00	2.3 Remaining Risk
14:00 - 17:00	Practical assignment 2

Day 3

09:00 - 09:30	3.1 Organizational Controls
09:30 - 10:30	3.2 Technical Controls
10:30 - 10:45	lunch
10:45 - 12:30	Technical Controls continued
14:00 - 16:00	3.3 Other Controls

Self-Reflection of understanding Diagram

‘*What you do not measure, you cannot control*.’’ – Tom Peters

Fill in this diagram to self-evaluate your understanding of the material. This is an evaluation of how well you know the material and how well you understand it. In order to pass the exam successfully you should be aiming to reach the higher end of Level 3. If you really want to become a pro, then you should be aiming for Level 4. Your overall level of understanding will naturally follow the learning curve. So, it’s important to keep track of where you are at each point of the training and address any areas of difficulty.

Based on where you are within the Self-Reflection of Understanding diagram you can evaluate the progress of your own training.

Level of Understanding	*Before Training (Pre-knowledge)*	*Training Part 1 (1st Half)*	*Training Part 2 (2nd Half)*	*After studying / reading the book*	*After exercises and the Practice exam*
Level 4 *I can explain the content and apply it .*					
Level 3 *I get it!* *I am right where I am supposed to be.*					Ready for the exam!
Level 2 *I almost have it but could use more practice.*					
Level 1 *I am learning but don’t quite get it yet.*					

(Self-Reflection of Understanding Diagram)

Write down the problem areas that you are still having difficulty with so that you can consolidate them yourself, or with your trainer. After you have had a look at these, then you should evaluate to see if you now have a better understanding of where you actually are on the learning curve.

Troubleshooting

Problem areas:	*Topic:*
Part 1	
Part 2	
You have gone through the book and studied.	
You have answered the questions and done the practice exam.	

Information Security Management Professional

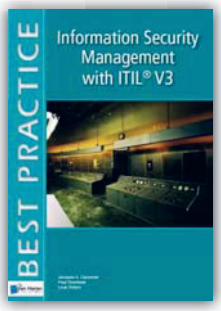
INFORMATION SECURITY MANAGEMENT PROFESSIONAL based on ISO/IEC 27001

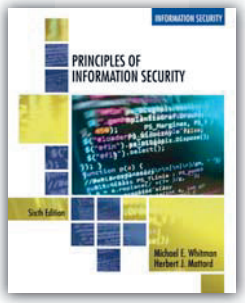
COURSEWARE

Here is the link from the slide to the theory in the book, with the number of the chapter or the paragraph (Par.) and possibly the name of the subtitle in the book

About the Courseware

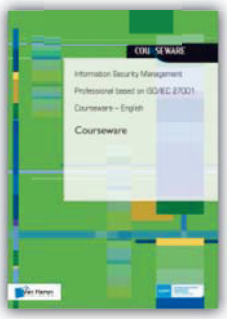
Literature: A B C D





ISO 27001

ISO Standaard - Information Security Management
NEN-ISO IEC 27001: 2013



Program

Day 1	
9:00 – 9:30	Introduction
9:30 – 10:45	1.1 Business perspective
10:45 – 12:00	1.2 Customer perspective
12:00 – 12:30	lunch
12:30 – 15:00	Practical assignment 1
15:00 – 17:00	1.3 Provider / supplier perspective

Day 2	
9:00 – 10:30	2.1 Risk Analysis
10:30 – 12:00	2.2 Security Controls
12:00 – 12:30	lunch
12:30 – 14:00	2.3 Remaining Risk
14:00 – 17:00	Practical assignment 2

Day 3	
9:00 – 10:30	3.1 Organizational Controls
10:30 – 12:00	3.2 Technical Controls
12:00 – 12:30	lunch
12:30 – 14:00	Technical Controls continued
14:00 – 16:00	3.3 Other Controls

Information Security Management Professional
About this course

EXIN INFORMATION SECURITY MANAGEMENT PROFESSIONAL based on ISO/IEC 27001

The course

Course subject

- Information security perspectives: Business, Customer, Service provider/supplier
- Risk Management: Analysis, Controls, Remaining risks
- Information security controls: Organizational, Technical, Physical.

Exam requirements

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 information 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 (10%)

1.1 Business (3.3%)
The candidate understands the business interest of information security.
The candidate is able to:
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 (3.3%)
The candidate understands the customer perspective on information governance.
The candidate is able to:
1.2.1 Explain the importance of information governance when outsourcing
1.2.2 Recommend a supplier based on assurance controls

1.3 Service provider / supplier (3.3%)
The candidate understands the supplier's responsibilities in security assurance.
The candidate is able to:
1.3.1 Distinguish security aspects in service management processes
1.3.2 Support compliance activities

2. Risk management (30%)

2.1 Analysis (10%)
The candidate understands the principles of risk management.
The candidate is able to:
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 Controls (10%)
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 Remaining risks (10%)
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 (60%)

3.1 Organizational (20%)
The candidate has knowledge of organizational controls.
The candidate is able to:
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 Technical (20%)
The candidate has knowledge of technical controls.
The candidate is able to:
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 Other controls (20%)
The candidate has knowledge of physical, employment-related and continuity controls.
The candidate is able to:
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

EXIN INFORMATION SECURITY

Information Security Management Professional
Module I Information Security Perspective

Van Haren PUBLISHING COURSEWARE

Information security perspectives

1.1 Business perspective

1.2 Professional / Customer perspective

1.3 Service provider / supplier perspective

A: § 2.1; Chapter 3; §5.6
B: Chapter 4; Chapter 9

Module 1.1

BUSINESS PERSPECTIVE

Information Security

Exin Basic training material

What is information security?

Information security is the protection of information and its critical characteristics (**confidentiality, integrity, and availability**), including the systems and hardware that use, store, and transmit that information, through the application of policy, training and awareness programs, and technology.

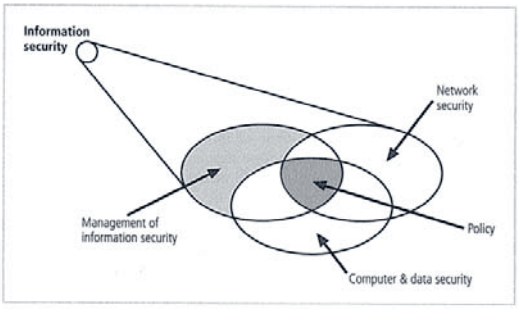


Figure 1-1 Components of information security

Perspectives on Information Security

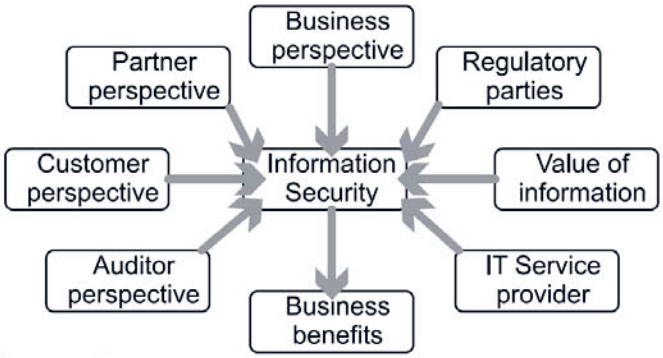


Figure 2.1: Different perspectives on information security

Business perspective

Exin Basic training material

The business perspective (1/2)

- Information has become the most important asset for the majority of business
- Protecting that valuable asset from loss, tampering and disclosure is vital
- Information is everywhere; even outside the organization's perimeter, making protection difficult but even more necessary
- Custodians of information need to show that they are trustworthy; governance and compliance is key
- International respected standards such as the ISO 2700x series help to understand how to deal with the above

The business perspective (2/2)

- Law and regulations force organizations to comply with data privacy and intellectual property best practice
- Customers and even suppliers demand transparency and compliance
- Stories of incidents travel fast; damage to reputation can be outside your control, a focus on prevention is required
- Monitoring, logging and a pro-active organization are key elements; immediate detection of incidents and incident management are crucial processes
- Since information is everywhere, information security and awareness of risks needs everyone's attention – information security needs to be embedded in the organization

How to manage information security

Exin Basic training material

How to manage information security

The starting point is effective organization of information security, in which responsibilities, authorities and duties are clearly specified in increasing levels of detail:

- Policy and/or codes of conduct (which control objectives aligned with business requirements are we aiming for)
- Processes (what has to happen to achieve those objectives)
- Procedures (who does what and when)
- Work instructions (how do we specifically do that, when and where and how does reporting take place).

How to manage information security

Examples of changes in input which require adaptation of the process are:

- changes in business demands
- organizational changes, mergers, acquisitions
- changes in tasks or the importance of tasks
- physical alterations, e.g. after relocating business premises
- environmental alterations
- changes in assessment of the IT used
- changes in legislation
- changes in hardware and/or software
- changes in threats
- the introduction of new technology
- ageing or obsolete technology

The Information Security Management System

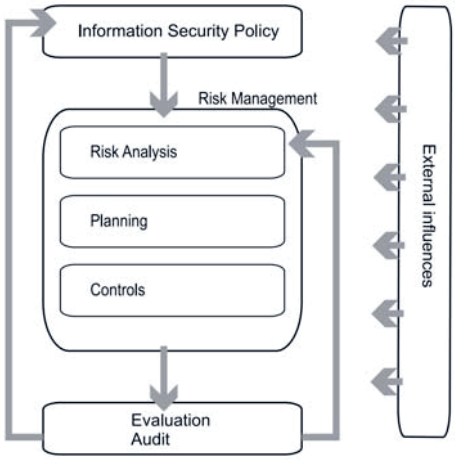
Exin Basic training material

The Information Security Management System

The management system represents the complete information security process during all the phases of its cycle, from policy to maintenance.

It is comparable to the management systems found in standards such as ISO 9000 and ISO/IEC 27001.

Plan-do- check-act (Deming circle)



Value and importance of Information

Literature A: Information Security Management with ITIL v3

Value of Information

Information security is intended to safeguard information. Security is the means of achieving an acceptable level of residual risks. Aspects that enable discussing the value of the information are:

- **confidentiality:** protecting sensitive information from unauthorized disclosure or intelligible interception
- **integrity:** safeguarding the accuracy, completeness and timeliness of information
- **availability:** ensuring that information and vital IT services are available when required.

Aspects derived from CIA

- **privacy:** the confidentiality and integrity of information traceable to a particular person
- **anonymity:** the confidentiality of a user's identity
- **authenticity:** the state in which there is no dispute about the identity of the participants involved
- **auditability:** the possibility of verifying that information is being used in line with the security policy and the ability of demonstrating that the security controls are working as intended.

Importance of information

Internal importance

An organization can only operate effectively if it has timely access to confidential, accurate and complete information. Information security has to be in line with this, ensuring that confidentiality, integrity and availability of information and information services is maintained.

External importance

An organization's processes supply products and/or services, which are made available in the market or the community, in order to achieve set objectives.

Types of security measures – controls

Literature A: Information Security Management with ITIL v3

Types of security measures – controls

Security measures are effective only when used harmoniously with business processes.

The security organization has to manage and maintain an appropriate balance.

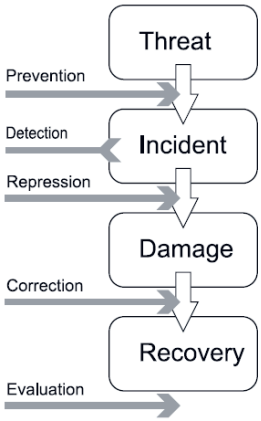


Figure 2.2: From threat to recovery; different types of countermeasures

Information Security Policy

Literature B: Management of Information Security

Information Security Policy

The success of an information resources protection program depends on:

- the policy generated, and ;
- the attitude of management toward securing information on automated systems.

"Policy is the essential foundation of an effective information security program" (Charles Cresson Wood)

WHY POLICY?

Information security policy :

- explains the will of the organization's management in controlling the behavior of its employees;
- is designed to create a productive and effective work environment;
- properly developed and implemented policies enable the information security program to function almost seamlessly within the workplace.

Shaping a policy

Some basic rules must be followed when shaping a policy:

Policy should never conflict with law.

Policy must be able to stand up in court if challenged.

Policy must be properly supported and administered.

Different types of policy

Types:

- Enterprise Information Security Policy
- Issue-Specific Security Policy
- System-Specific Security Policy