Service Document

Information Security Foundation
based on ISO/IEC 27002

Service Document ISFS
Information Security Foundation
based on ISO/IEC 27002
edition April 2009

CONTENT

Date: 2 April 2009

1. Introduction

Service Documents are designed to help training providers develop courses and course material that meet with EXIN requirements.

The main objective of the Service Document is to identify the exam subjects, the exam requirements and specifications, and the target audience to support the development of new, high quality courses.

2. Module description

Module name

Information Security Foundation based on ISO/IEC 27002 (ISFS[1])

Module description

Information security is becoming increasingly important. Globalization of the economy leads to a growing exchange of information between organizations (their employees, customers and suppliers) and a growing use of networks, such as the internal company network, connection with the networks of other companies and the Internet.
Other relevant trends include:

- (international) standards and certification in the field of information security
- continuing computerization of (IT) management
- development of automated security tools
- remote control
- outsourcing of management tasks
- compliancy

Furthermore, activities of many companies now rely on IT, and information has become a valuable asset. Protection of information is crucial for the continuity and proper functioning of the organization: information must be reliable.
The international standard, the Code of Practice for Information Security ISO/IEC 27002:2005 structures the organization of information security. For that reason, it is an important point of departure for this module.
In the modules about Information Security, use is made of the definition of the PvIB (Platform voor Informatiebeveiliging): Information Security deals with the definition, implementation, maintenance, compliance and evaluation of a coherent set of measures which safeguard the availability, integrity and confidentiality of the (manual and automated) information supply.
In the Information Security Foundation module, based on ISO/IEC 27002 (ISFS), the basic concepts of information security and their coherence are tested. The target group of ISFS is everyone in the organization. The basic knowledge that is tested in this module contributes to the understanding that information is vulnerable and that measures are necessary to protect this information.
The module Information Security Management Advanced based on ISO/IEC 27002 (ISMAS) tests organizational and managerial aspects of information security. Its target group are people who are professionally involved with the implementation and evaluation of information security.

[1] The S in the module code stands for: based on the standard.

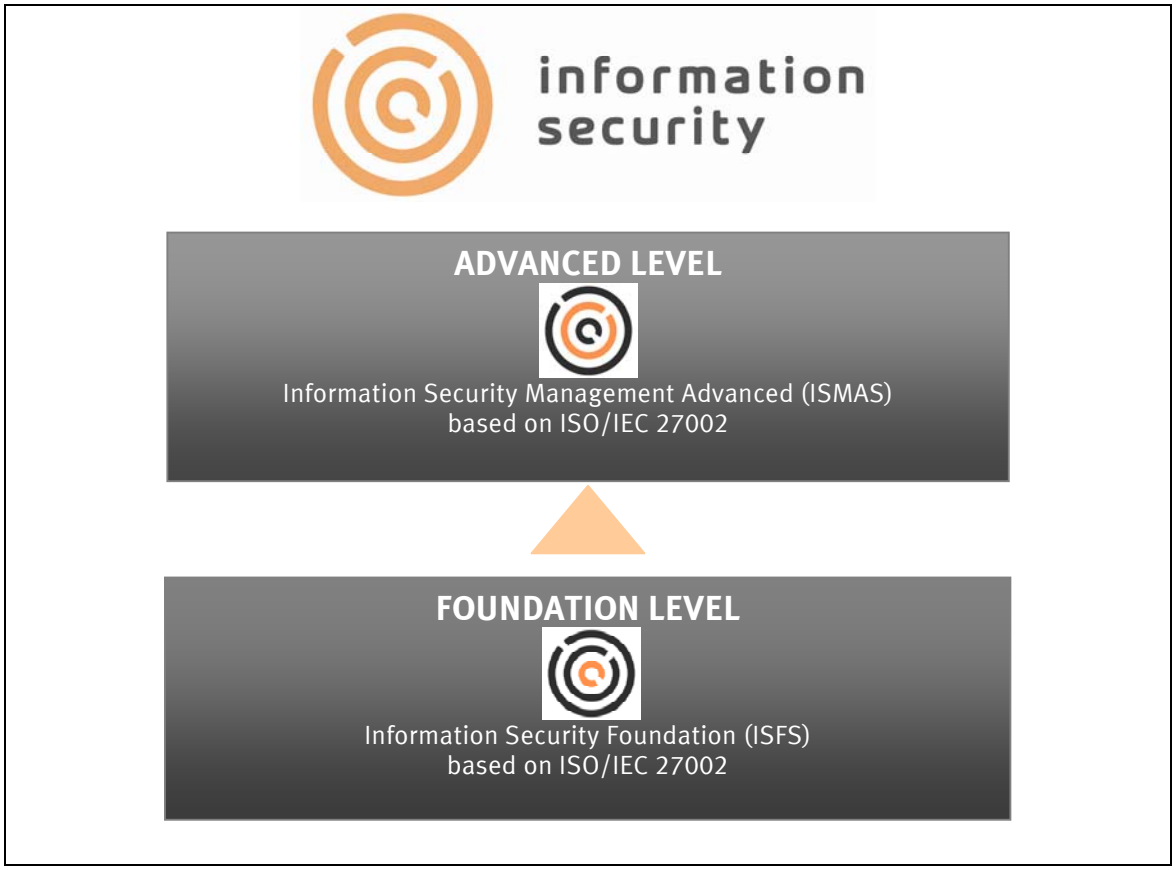
Exam requirements

- Information and security: the concepts, the value of information and the importance of reliability.
- Threats and risks: the relationship between threats and reliability.
- Approach and organization: the security policy and the set-up of information security.
- Measures: physical, technical and organizational.
- Legislation and regulations: the importance and operation.

Context

The Certificate Information Security Management Advanced based on ISO/IEC 27002 is a follow up of the Certificate Information Security Foundation based on ISO/IEC 27002.

Qualification scheme of the available certificates



Target group

Everyone in the organization who is processing information. The module is also suitable for 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.

Prerequisites

Entry requirements for the exam: None.
A course in Information Security Foundation based on ISO/IEC 27002, delivered by an EXIN accredited training provided is recommended.

Exam format

Multiple choice exam.

3. Exam requirements and exam specifications

The exam requirements are the main topics of a module. The candidate must have a thorough command of these topics. The exam requirements are elaborated in the exam specifications. EXIN applies exam specifications at six mastery levels based upon the Revised Bloom's Taxonomy (Anderson & Krathwohl, 2001).

The exam specifications are structured into two levels: the mastery level and the testing level:

The mastery level
Depending on the required difficulty, the mastery level (1.**1**) defines:

1 Remembering: the ability to recall, restate and remember learned information
2 Understanding: the ability to grasp meaning of information by interpreting and translating what has been learned
3 Applying: the ability to make use of information in a context different from the one in which it was learned
4 Analyzing: the ability to break learned information into its parts to understand it
5 Evaluating: the ability to make decisions based on in-depth reflection, criticism and assessment
6 Creating: the ability to create new ideas and information using what has been learned

The Testing level
The testing level (1.1.**1**) defines:

- What will be tested (the specific indication of the content)
- How this will be tested (for example: by asking to name or describe something; or to give examples)

This table lists the main topics of the module (exam requirements). The importance of main topics in relation to the exam is expressed as a percentage of the total (see the second column).

Exam requirements	**Weight**
1. Information and security	10%
2. Threats and risks	30%
3. Approach and organization	10%
4. Measures	40%
5. Legislation and regulations	10%

Exam specifications

1. Information and security (10%)

1.1 The concept of information (2.5%)
The candidate understands the concept information.

The candidate is able to:
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 (2.5%)
The candidate understands the value of information for organizations.

The candidate is able to:
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 (5%)
The candidate knows the reliability aspects (confidentiality, integrity, availability) of information.

The candidate is able to:
1.3.1 Name the reliability aspects of information
1.3.2 Describe the reliability aspects of information

2. Threats and risks (30%)

2.1 Threat and risk (15%)
The candidate understands the concepts of threat and risk.

The candidate is able to:
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. (15%)
The candidate understands the relationship between threats, risks and the reliability of information.

The candidate is able to:
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 (10%)

3.1 Security policy and security organization (2.5%)
The candidate has knowledge of the concepts security policy and security organization.

The candidate is able to:
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 (2.5%)
The candidate knows the various components of the security organization.

The candidate is able to:
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 (5%)
The candidate understands the importance of incident management and escalation.

The candidate is able to:
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 (40%)

4.1 Importance of measures (10%)
The candidate understands the importance of security measures.

The candidate is able to:
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 (10%)
The candidate has knowledge of both the set up and execution of physical security measures.

The candidate is able to:
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 (10%)
The candidate has knowledge of both the set up and execution of technical security measures.

The candidate is able to:
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 (10%)

The candidate has knowledge of both the set up and execution of organizational security measures.

The candidate is able to:
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 (10%)

5.1 Legislation and regulations (10%)

The candidate understands the importance and effect of legislation and regulations.
The candidate is able to:
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 fulfil the requirements of legislation and regulations

Justification of choices

Exam requirements: justification of weight distribution.
The security measures are for most staff members the first aspects of information security they encounter. Therefore the measures are central to the module and have the highest weight. The threats and risks follow in terms of weight. Finally, insight in the policy, organization and legislation and regulation in the area of information security is necessary in order to understand the importance of the information security measures.

4. Exam matrix

Exam format

Exam type: multiple choice exam
Number of questions: 40
Exam duration: 60 minutes
Pass rate: 65%

Exam matrix

The exam matrix specifies the number and weight of the questions in the exam, based on the exam requirements and specifications at mastery level.

Exam requirement	Exam specification at mastery level		Weight (%)	Number of questions
1 Information and security	Exam specification	Mastery level		
The concept of information	1.1	Understanding	2.5	1
Value of information	1.2	Understanding	2.5	1
Reliability aspects	1.3	Remembering	5	2
Subtotal			**10**	**4**
2 Threats and risks				
Threat and risks	2.1	Understanding	15	6
Relationships between threats, risks and the reliability of information.	2.2	Understanding	15	6
Subtotal			**30**	**12**
3 Approach and Organization				
Security policy and security organization	3.1	Remembering	2.5	1
Components	3.2	Remembering	2.5	1
Incident Management	3.3	Understanding	5	2
Subtotal			**10**	**4**

Exam requirement	Exam specification at mastery level		Weight (%)	Number of questions
4 Measures				
Importance of measures	4.1	Understanding	10	4
Physical security measures	4.2	Remembering	10	4
Technical measures	4.3	Remembering	10	4
Organizational measures	4.4	Remembering	10	4
Subtotal			**40**	**16**
5 Legislation and regulations				
Legislation and regulations	5.1	Understanding	10	4
Subtotal			**10**	**4**
Total			**100**	**40**

5. List of basic concepts

This chapter contains the terms with which candidates should be familiar. Terms are listed in alphabetical order. For concepts whose abbreviation and full name are included in the list, both can be examined separately.

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

List of basic concepts

- Access control
- Asset
- Audit
- Authentication
- Authenticity
- Authorization
- Availability
- Backup
- Biometrics
- Botnet
- Business Continuity Management (BCM)
- Business Continuity Plan (BCP)
- Category
- Certificate
- Change Management
- Classification (grading)
- Clear desk policy
- Code of conduct
- Code of practice for information security (ISO/IEC 27002:2005)
- Completeness
- Compliance
- Computer criminality legislation
- Confidentiality
- Continuity
- Copyright legislation
- Corrective
- Correctness
- Cryptography
- Damage
- Data
- Detective
- Digital signature
- Direct damage
- Disaster
- Disaster Recovery Plan (DRP)
- Encryption
- Escalation
  - Functional escalation
  - Hierarchical escalation
- Exclusivity
- Hacking

- Hoax
- Identification
- Impact
- Incident cycle
- Indirect damage
- Information
- Information analysis
- Information architecture
- Information management
- Information system
- Infrastructure
- Integrity
- Interference
- ISO/IEC 27001:2005
- ISO/IEC 27002:2005
- Key
- Logical access management
- Maintenance door
- Malware
- 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
- Reliability of information
- Repressive
- Risk
- Risk analysis
- Risk assessment (Dependency & Vulnerability analysis)
- Risk strategy
  - Risk avoiding
  - Risk bearing
  - Risk neutral
- Risk management
- Robustness
- Rootkit
- Security incident
- Security measure
- Security Organization
- Security Policy
- Security regulations for special information for the government
- Security regulations for the government
- Segregation of duties
- Social engineering

- Spam
- Spyware
- Stand-by arrangement
- Storage medium
- Threat
- Timeliness
- Trojan
- Uninterruptible Power Supply (UPS)
- Urgency
- Validation
- Verification
- Virtual Private Network (VPN)
- Virus
- Vulnerability
- Worm

6. Literature

Candidates are advised to read book **A** to prepare for the examination.

Book

A Hintzbergen, J., Baars, H., Hintzbergen, K. and Smulders, A.
The Basics of Information Security - A practical handbook
The Netherlands, 2009

Explanation and justification

This publication is available free of charge as a PDF file via EXIN website:
http://www.exin-exams.com/exams/exam-program/iso-iec-27000/isfs.aspx

Overview of the literature

Exam specification	Literature
1.1	**A:** Chapter 4
1.2	**A:** Chapter 4
1.3	**A:** Chapter 4
2.1	**A:** Chapter 5
2.2	**A:** Chapter 5
3.1	**A:** Chapter 9
3.2	**A:** §6.1, §6.3, Chapter 9
3.3	**A:** Chapter 6
4.1	**A:** Chapter 5, Chapter 6
4.2	**A:** Chapter 7
4.3	**A:** Chapter 8, Chapter 9
4.4	**A:** Chapter 8 and 9
5.1	**A:** Chapter 10

7. Accreditation requirements

Apart from the general requirements in the EXIN Accreditation Guide, there are a number of specific criteria for the delivery of accredited training courses for the module Information Security Foundation based on ISO/IEC 27002 that must be met:

Class size

The maximum group size for a course is 16.
(This is not applicable to distance learning /computer based training.)

Contact hours

The minimum number of contact hours time during the training is **7** hours. This includes group assignments, exam preparation and short coffee breaks, but it does not include homework, logistical exam preparation and lunch breaks.

Distance learning

- The extent of the training should be comparable to the number of contact hours for a face to face training, in effect **7** hours.
- A computer-based training could be defined within four levels: text, graphics, animation, and multimedia. Text-based courses cannot be accredited. The training must at least contain graphics.
- The computer-based training has a high level of usability (ease of navigation, sensible use of colors, availability of help-messages etc.).
- The computer-based training should be more than just a sequential course. The computer-based training has the facility to handle the subjects interactively.
- The cbt-tool supports the trainers to monitor the students' activities.
- The student is given the facility to contact a trainer. The turn-around time for enquiries is no more than one working day.
- There is an explanation about the structure of the computer based training and a clear survey of the subjects.

Trainer competency requirements

- The trainer has obtained the certificate in Information Security Foundation based on ISO/IEC 27002.

Course material

Approved courseware needs to be in place.

- There is an explanation about the structure of the computer based training and a clear survey of the subjects. (*Only applicable to distance learning/computer based training)*
- The material contains information about the background of the subject of the course and relevant publications.
- The course contains assignments in line with the exam requirements. Any further guidelines provided through the applicable Service Document are also taken into account. These assignments could be conducted in the form of discussion, (group) assignments, simulation etc.

For more information you can refer to the Accreditation Guide or you can contact EXIN's Accreditation department (accreditation@exin-exams.com).
You can download the Accreditation Guide from the EXIN Extranet.

8. Course outline

The course outline indicates the possible structure of the course. This is an indication only that by no means dictates how training should be conducted. However it provides a logical order for the exam topics and examples of exercises and questions to discuss with the participants.

Topics to be addressed in the course	Instructional method
1. Securing information • What is information? • What makes information valuable? • What makes information less valuable? • What do we do about that?	*Ask students the 4 questions listed under 1.Securing information.* *Explain:* • *Definition of information according to Webster dictionary:* ***'The communication or reception of knowledge or intelligence'.*** • *Difference between data and information* • *Valuable = money* • *Reliability requirements: CIA* • *Threats to the CIA* • *Assessing risks and taking measures*
2. Information security • What is information security?	*Explain the definition of information security.* *<u>Definition:</u> Information Security deals with the definition, implementation, maintenance, compliance and evaluation of a coherent set of measures which safeguard the availability, integrity and confidentiality of the (manual and automated) information supply.* **Exercise A** • *Which information is valuable in ‹our organization› and why?* o *Let the students prepare in pairs and then present their answers.*
3. Examples of valuable information • Employees (their knowledge and experience) • The product or service we sell • Personal data of suppliers, customers, employees • Our processes • Manuals/recipes • Financial information	**Exercise B** • *How can the information of ‹our organization› be threatened?* o *Let the students write, in two groups, as many practical examples of threats as they can think of on two whiteboards.* o *Make sure the examples are practical, and specific for ‹our organization›, not general. For example:* ***Not**: Information can be stolen.*

	***But**: I can have a business telephone call in the train about our new project and the person sitting next to me can listen in.*
4. Threats • Human and non human threats • Intentional and unintentional • Intentional human threat: Social Engineering • Disruptions in basic infrastructure Disruptions in physical environment	*Explain the difference between human and non human threats and between intentional and unintentional threats.* **Exercise C** • *Together with the students assign the threat categories to the threats listed on the whiteboards.*

5. Damage
• Direct damage
• Indirect damage
• Annual Loss Expectancy
• Single Loss Expectancy
	Exercise D
	• *Ask the students to name examples for each kind of damage:*
	  o *<u>Direct:</u> for example theft*
	  o *<u>Indirect:</u> for example loss of reputation*

6. Risk • What do we do with the threats and the damage we expect when the threat materializes? • Risk analysis • Risk strategies: bearing, neutral, avoiding	*Explain the difference between a threat and a risk.* *Discuss the relationship between threats, risks and the reliability of information.*

7. Security measures during the incident cycle
• When and what can we do to prevent or reduce damage?
• Incident cycle
• Kinds of measures:
  o Reductive
  o Preventive
  o Detective
  o Repressive
  o Corrective
	Exercise E
	• *Let the students think of a measure for each of the threats that have been listed on the whiteboards and, in case the measure is too expensive, let them decide to accept the related risk.*

<table>
<tr>
<td>8. Physical measures
• Cabling, equipment, protection rings

9. Technical measures
• Access management
• Validation of input and output data
• Encryption and PKI

Explain the concepts without giving technical details. The candidates only need to understand the concepts ‘cryptography’, ‘digital signature’ and ‘certificate’ without technical knowledge about how they work.

10. Organizational measures
• Management of assets
• Classification
• Policy
• Reporting incidents
• ISO/IEC 27002 (standard)
• Personnel
• Awareness
• Disasters and business continuity
• Change Management
• Testing
• Segregation of duties
• Outsourcing
• Protection against malware and phishing
• Back-up
• Handling media, mobile equipment, exchange of information
• Clear desk policy</td>
<td>Exercise F
• Together with the students assign the category of measures (Reductive, Preventive, Detective, Repressive and Corrective) to the measures on the whiteboards.

Questions to discuss with the students:

o What are assets in ‹our organization›? (building, furniture, pc’s, documents, system logs, services, people, reputation)
o Classification: What kind of information do you want to register about our assets if you don’t want to give them all the same level of security? (owner, location, type, value, level of confidentiality)
o Examples of disasters?
o What measures can you take? Examples of Reductive, Preventive, Detective, Repressive and Corrective measures.</td>
</tr>
<tr>
<td>11. Legislation and regulations
• Compliance to national legislation before company regulations
• ISO/IEC 27002
• Intellectual property
• Protecting personal data
• Preventing abuse of IT facilities
• Computer criminality
• Sarbanes-Oxley Act
• Management responsibility
• Audit</td>
<td>Give examples of legislative acts related to information security specific to your local situation.
Explain the difference between a standard and a legislative act.</td>
</tr>
</table>