# INFORMATION SECURITY FOUNDATION

## Exam syllabus

SECO INSTITUTE

# Table of contents



**Disclaimer**

Although SECO-Institute has made every effort to ensure that the information in this exam syllabusbook was correct at publication time, SECO-institute does not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

**Copyright notice**

# Exam Syllabus: Information Security Foundation

Economic globalisation is leading to an ever-increasing exchange of information and an explosion of cybercrime. The dramatic rise in cyberattacks, in turn, results in a growing demand for certified security specialists and a new awareness of how information security (or the lack thereof) can affect one's business. The completion of this introductory course based on ISO/IEC27001 (requirements) and ISO/IEC 27002 (code of practice) demonstrates that candidates have an understanding of the most important information security aspects and know what it takes to implement and integrate information security in an organisation.

## Context

The Information Security Foundation (S-ISF) certificate constitutes the first level of the SECO-Institute's Information Security track within the Cyber Security & Governance Certification Program. The successful completion of an Information Security Foundation course provides candidates with sufficient knowledge to be able to continue with the Information Security Practitioner course.


## Exam requirements

- Requirements & Code of practice for Information Security (ISO/IEC 27001/27002).
- Information and security: the concept, the value, the importance and the reliability of information.
- Threats and risks: the concepts of threat and risk and their relationship with the reliability of information.
- Approach and organisation: security policy and security organisation including the components of the security organisation and the management of (security) incidents.
- Measures: security measures including physical, technical and organisational measures.
- Legislation and regulations: importance and impact of laws and regulations.

## Target audience

This exam is designed for professionals who are or expect to become responsible for information security, thus need to have a solid grounding in the subject. For example:

- Information security consultants
- Security managers who act at the tactical level in their organisation
- Information security coordinators
- IT auditors

## Prerequisites

- None.

## Exam information

SECO-Institute provides the official information security courseware to accredited training centres where candidates are trained by accredited instructors. Candidates can take their exams at an accredited exam centre or directly with the SECO-Institute.

## Examination details

- Computer-based
- Multiple choice with 40 questions
- Time allotted: 60 minutes
- Pass mark: 60% (out of 100)
- Open book/notes: no
- Electronic equipment permitted: no

The Rules and Regulations for SECO-Institute examinations apply to this exam.

# Exam requirements

The following tables list the exam requirements and exam specifications.

| Information Security Foundation | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Requirements** | 1. Information security: Requirements & Code of practice (ISO/IEC 27001/27002)<br>2. Information and security: the concept, the value, the importance and the reliability of information.<br>3. Threats and risks: the concepts of threat and risk and their relationship with the reliability of information.<br>4. Approach and organisation: security policy and security organisation including the components of the security organisation and the management of (security) incidents.<br>5. Measures: security measures including physical, technical and organisational measures.<br>6. Legislation and regulations: the importance and impact of legislation and regulations. | | | | | | | | | |
| **Required prior knowledge** | None | | | | | | | | | |
| | | | | | | | | | | |
| **Learning levels** | x | Know | x | Understand | | Apply | | Analyse, Synthesise | | Create |

## Exam specifications

| | Requirements, specifications, testing levels | | | Bloom level |
|---|---|---|---|---|
| **1.** | **Requirements and Code of practice** | | | |
| | 1.1 | The candidate knows what the standard involves | | |
| | | The candidate is able to: | | |
| | | 1.1.1 | List the different types of requirements set out in a standard | 1 |
| | | | | |
| | 1.2 | The candidate knows the difference between a standard and a framework | | |
| | | The candidate is able to: | | |
| | | 1.2.1 | Describe the differences between a standard and a framework | 1,2 |
| | | | | |
| | 1.3 | The candidate understands standard implementation challenges. | | |
| | | The candidate is able to: | | |
| | | 1.3.1 | List and explain implementation challenges | 1,2 |
| | | 1.3.2 | Summarise implementation stages | 2 |
| | | | | |
| | 1.4 | The candidate knows what the standard requires, and understands the relevant areas of attention | | |
| | | The candidate is able to: | | |
| | | 1.4.1 | Explain what ISO/IEC 27001 requires of an organisation | 2 |
| | | 1.4.2 | Describe the areas of attention when adopting a standard | 1 |
| | | 1.4.3 | Recall ISO/IEC 27001 paragraphs and their purpose | 1 |
| | | 1.4.4 | Recall ISO/IEC 27002 paragraphs and their purpose | 1 |
| | | | | |
| | 1.5 | The candidate knows how the standard is managed and understands what the related control measures are | | |
| | | The candidate is able to: | | |
| | | 1.5.1 | Name different improvement cycles that can be applied to standards | 1 |
| | | 1.5.2 | Recall the different stages of the Deming cycle | 1 |
| | | 1.5.3 | Explain the different stages of the Deming cycle | 2 |
| | | 1.5.4 | Recall the control objectives of ISO/IEC 27001 | 1 |
| | | 1.5.5 | Illustrate different control objectives and related control measures | 2 |

| | Requirements, specifications, testing levels | | | Bloom level |
|---|---|---|---|---|
| **2.** | **Information and security** | | | |
| | 2.1 | The candidate knows the concept of information | | |
| | | The candidate is able to: | | |
| | | 2.1.1 | Reproduce the layers of the DIKW-pyramid | 1 |
| | | 2.1.2 | Recall the rationale behind information security | 1 |
| | | 2.1.3 | Describe information security as a concept | 1 |
| | | | | |
| | 2.2 | The candidate understands that there are different kinds of information and information systems | | |
| | | The candidate is able to: | | |
| | | 2.2.1 | Recognise different types of information | 1 |
| | | 2.2.2 | Describe the different types of Information systems | 2 |
| | | | | |
| | 2.3 | The candidate understands the CIA triad (confidentiality, integrity and availability) | | |
| | | The candidate is able to: | | |
| | | 2.3.1 | Describe the CIA-triangle of information security | 1 |
| | | 2.3.2 | Explain the concept of confidentiality and corresponding measures | 2 |
| | | 2.3.3 | Explain the concept of integrity and corresponding measures | 2 |
| | | 2.3.4 | Explain the concept of availability and corresponding measures | 2 |
| | | | | |
| | 2.4 | The candidate understands the influential scope of information security | | |
| | | The candidate is able to: | | |
| | | 2.4.1 | Explain the concept of operational processes and their need for information | 2 |
| | | 2.4.2 | Recall the scope of information architecture | 1 |
| | | 2.4.3 | Describe the concept of Information management | 1 |
| | | | | |

| | Requirements, specifications, testing levels | | | Bloom level |
|---|---|---|---|---|
| **3.** | **Threats and risks** | | | |
| | 3.1 | The candidate knows the different types of risk analysis and risk assessment | | |
| | | The candidate is able to: | | |
| | | 3.1.1 | Describe the concepts of vulnerability, threat and risk | 1 |
| | | 3.1.2 | Describe the three layers of the risk process | 1 |
| | | 3.1.3 | Explain the concepts, elements and types of risk analysis | 2 |
| | | | | |
| | 3.2 | The candidate understands the different types of threats and the ways to handle them | | |
| | | The candidate is able to: | | |
| | | 3.2.1 | Recall the different types of threats | 1 |
| | | 3.2.2 | Recall the different types of security measures | 1 |
| | | | | |
| | 3.3 | The candidate knows the different types of damage that can occur | | |
| | | The candidate is able to: | | |
| | | 3.3.1 | Recall the different types of damage that may be incurred | 1 |
| | | | | |
| | 3.4 | The candidate knows the types of risk strategy | | |
| | | The candidate is able to: | | |
| | | 3.4.1 | Describe the different types of risk strategy | 1 |
| | | | | |
| | 3.5 | The candidate knows what security measures can be implemented | | |
| | | The candidate is able to: | | |
| | | 3.5.1 | Describe how security risks should be handled | 1 |
| | | | | |
| | 3.6 | The candidate knows how to avoid risks and take security measures | | |
| | | The candidate is able to: | | |
| | | 3.6.1 | Recognise examples of risk avoiding strategies | 1 |
| | | 3.6.2 | Recall examples of risk avoiding measures | 1 |

| | Requirements, specifications, testing levels | | | Bloom level |
|---|---|---|---|---|
| **4.** | **Approach and organisation** | | | |
| | 4.1 | The candidate knows what an information security policy covers | | |
| | | The candidate is able to: | | |
| | | 4.1.1 | Describe the objectives and contents of an information security policy | 1 |
| | | 4.1.2 | Outline the importance of having an information security policy | 2 |
| | | 4.1.3 | Explain the purpose of the different sections of an information security policy | 2 |
| | | | | |
| | 4.2 | The candidate can recognise an information security organisation and the way it is constructed | | |
| | | The candidate is able to: | | |
| | | 4.2.1 | Recall the objectives of an information security organisation | 1 |
| | | 4.2.2 | Describe the different roles in an information security organisation | 1 |
| | | 4.2.3 | Describe the different process components of an information security organisation (activities, resources, administration) | 1 |
| | | | | |
| | 4.3 | The candidate knows what a code of conduct means | | |
| | | The candidate is able to: | | |
| | | 4.3.1 | Explain the elements of an information security code of conduct | 1 |
| | | | | |
| | 4.4 | The candidate knows the tasks and responsibilities of an information security organisation | | |
| | | The candidate is able to: | | |
| | | 4.4.1 | Recall the tasks and responsibilities of an information security organisation | 1 |
| | | | | |
| | 4.5 | The candidate knows how security incidents are managed | | |
| | | The candidate is able to: | | |
| | | 4.5.1 | Recall the definition of a security incident | 1 |
| | | 4.5.2 | Describe the objectives of security incident management | 1 |
| | | 4.5.3 | Explain the different activities of the security incident management process | 2 |
| | | 4.5.4 | Recall possible causes for a security incident | 1 |
| | | | | |

| | Requirements, specifications, testing levels | | | Bloom level |
|---|---|---|---|---|
| **5.** | **Measures** | | | |
| | 5.1 | The candidate knows the importance of security measures | | |
| | | The candidate is able to: | | |
| | | 5.1.1 | Describe the concept of information classification | 1 |
| | | | | |
| | 5.2 | The candidate knows the different types and categories of security procedures | | |
| | | The candidate is able to: | | |
| | | 5.1.1 | Describe the different types of security measures | 1 |
| | | 5.1.2 | Explain the purpose of the different types of security measures | 2 |
| | | | | |
| | 5.3 | The candidate what safety measures can be taken (physical, technical and organisational) | | |
| | | The candidate is able to: | | |
| | | 5.3.1 | Describe the different physical measures | 1 |
| | | 5.3.2 | Describe the layered rings of physical security | 1 |
| | | 5.3.3 | Describe the different technical measures | 1 |
| | | 5.3.4 | Explain the concept and types of cryptography | 2 |
| | | 5.3.5 | Describe the different organisational measures | 1 |
| | | | | |
| | 5.4 | The candidate knows what access management involves | | |
| | | The candidate is able to: | | |
| | | 5.4.1 | Recall the objective and types of access control | 1 |
| | | 5.4.2 | Describe the elements of ‘granting access’ | 1 |
| | | | | |
| | 5.5 | The candidate understands the terms *identification, authentication, authorisation* | | |
| | | The candidate is able to: | | |
| | | 5.5.1 | Explain the concept of identification | 2 |
| | | 5.5.2 | Explain the concept of authentication | 2 |
| | | 5.5.3 | Explain the concept of authorisation | 2 |
| | | | | |
| | 5.6 | The candidate understands what business continuity management involves. | | |
| | | The candidate is able to: | | |

| | | | | |
|---|---|---|---|---|
| | | 5.6.1 | Describe the importance of business continuity management (BCM) and relate it to information security | 1 |
| | | 5.6.2 | Describe the different planning processes that form part of BCM | 1 |

| | Requirements, specifications, testing levels | | | Bloom level |
|---|---|---|---|---|
| **6.** | **Laws and regulations** | | | |
| | 6.1 | The candidate knows the most important laws and regulations related to information security | | |
| | | The candidate is able to: | | |
| | | 6.1.1 | Recall examples of legislation concerning information security | 1 |
| | | 6.1.2 | Recognise examples of different types of legislation | 1 |
| | | | | |
| | 6.2 | The candidate knows the importance of compliance | | |
| | | The candidate is able to: | | |
| | | 6.2.1 | Recall the objective of compliance | 1 |
| | | | | |
| | 6.3 | The candidate knows the different categories of compliance | | |
| | | The candidate is able to: | | |
| | | 6.3.1 | Recall categories of compliance (legislation, policies, standards, IPR) | |

## Literature

| | |
|---|---|
| **A** | Course material (Module 1-6) |
| **Optional** | Hintzbergen, J., Hintzbergen , K., Smulders, A., en Baars, H. (2015). Foundations of Information Security – Based on ISO 27001 and ISO 27002; Van Haren Publishing, 3rd edition, 2015. ISBN 9789401800129, eBook 9789401805414 |

## Exam-literature matrix

| Exam requirement | Exam specification | Literature | Chapter reference(s) |
|---|---|---|---|
| **1** | 1.1 | **Module 1** | Slide section: ISO/IEC 27001 and 27002<br>• Purpose of a standard |
| | 1.2 | **Module 1** | Slide section: ISO/IEC 27001 and 27002<br>• Standard and framework |
| | 1.3 | **Module 1** | Slide section: ISO/IEC 27001 and 27002<br>• Implementation challenges |
| | 1.4 | **Module 1** | Slide section: ISO/IEC 27001 and 27002<br>• ISO 27001 in a nutshell |
| | 1.5 | **Module 1** | Slide section: ISO/IEC 27001 and 27002<br>• Continual improvement<br>• Objectives and measures |
| | | | |
| **2** | 2.1 | **Module 2** | Slide section: Information and Security<br>• Data, information, knowledge, wisdom (DIKW)<br>• Concept of information security |
| | 2.2 | **Module 2** | Slide section: Slide section: Information and Security<br>• Information systems and information technology |

| Exam requirement | Exam specification | Literature | Chapter reference(s) |
|---|---|---|---|
| | 2.3 | **Module 2** | Slide section: Slide section: Information and Security<br>• Confidentiality, integrity, availability (CIA) |
| | 2.4 | **Module 2** | Slide section: Slide section: Information and Security<br>• Scope |
| | | | |
| **3** | 3.1 | **Module 3** | Slide section: Threats and Risks<br>• Vulnerability, threat, risk and risk analysis |
| | 3.2 | **Module 3** | Slide section: Threats and Risks<br>• Types of threats |
| | 3.3 | **Module 3** | Slide section: Threats and Risks<br>• Damage |
| | 3.4 | **Module 3** | Slide section: Threats and Risks<br>• Risk strategy |
| | 3.5 | **Module 3** | Slide section: Threats and Risks<br>• Types of security measures |
| | 3.6 | **Module 3** | Slide section: Threats and Risks<br>• Risk-avoiding strategies and measures |
| | | | |
| **4** | 4.1 | **Module 4** | Slide section: Approach and Organisation<br>• Information security policy |
| | 4.2 | **Module 4** | Slide section: Approach and Organisation<br>• Information security organisation |
| | 4.3 | **Module 4** | Slide section: Approach and Organisation<br>• Code of conduct |

| Exam requirement | Exam specification | Literature | Chapter reference(s) |
|---|---|---|---|
| | 4.4 | **Module 4** | Slide section: Approach and Organisation<br>• Tasks and responsibilities of the information security organisation |
| | 4.5 | **Module 4** | Slide section: Approach and Organisation<br>• Incident management |
| | | | |
| **5** | 5.1 | **Module 5** | Slide section: Measures<br>• Importance of security measures and classification |
| | 5.2 | **Module 5** | Slide section: Measures<br>• Types of measures |
| | 5.3 | **Module 5** | Slide section: Measures<br>• Physical, technical and organisational measures |
| | 5.4 | **Module 5** | Slide section: Measures<br>• Access control |
| | 5.5 | **Module 5** | Slide section: Measures<br>• Identification, authentication, authorisation |
| | 5.6 | **Module 5** | Slide section: Measures<br>• Business continuity |
| | | | |
| **6** | 6.1 | **Module 6** | Slide section: Legislation and Regulations<br>• Laws and regulations related to information security |
| | 6.2 | **Module 6** | Slide section: Legislation and Regulations<br>• Compliance |
| | 6.3 | **Module 6** | Slide section: Legislation and Regulations<br>• Categories of compliance |

# How to book your exam

All our exams are delivered through an online examination system called ProcterU. To enrol for an exam, go to: https://go.proctoru.com/
Make sure you are fully prepared. Use the ProctorU Preparation checklist to assess whether you are ready to take the exam.

If you are a new user, select Test Taker. Select "SECO-Institute" as the institution and fill in all the necessary information. See the instructions for more information. Once you have scheduled your exam, you will be asked to pay the exam fee. If you have an exam voucher, please fill in the access code.

Our online examination system allows you to book your exam and take it at any place convenient to you. Do you prefer your kitchen table, your home desk or your office? Would you rather take a test in the day or at night? It is all up to you!

## System requirements

To ensure the quality and security of the examination, you will have to meet specific requirements regarding your computer configuration, your exam environment and your behaviour during the exam. Click here to see the requirements.

The exam will be taken with special proctor software. To enable webcam and audio recording during the exam, you have to install software that monitors your activities.

Your exam will be recorded through your webcam and microphone. The recordings will be reviewed by multiple proctors after you have completed the exam. The proctors will check if you comply with all the requirements for the examination.

## Results

If no non-conformities are detected by the proctors, you will receive the final result by email one month after you complete the test. The email will also contain information on how to claim your certificate and digital badge as well as how to use your title.

## Digital badges


SECO-Institute and digital badge provider Acclaim have partnered to provide certification holders with a digital badge of their SECO-Institute certification. Digital badges can be used in email signatures as well as on personal websites, social media sites such as LinkedIn and Twitter, and electronic copies of resumes. Digital badges help certification holders convey employers, potential employers and interested parties the skills they have acquired to earn and maintain a specialised certification.

**Claim your title at:** https://www.seco-institute.org/claim-your-title

ISF-EN-2018-01a