INFORMATION SECURITY FOUNDATION

Exam Syllabus

SECO INSTITUTE

Table of Contents

Disclaimer

Although the 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

Context

Information Security Foundation constitutes the first level of the Certified Information Security Officer certification track within the SECO-Institute's Cyber Security & Governance Certification Program.

Successful completion of this Foundation course provides you with sufficient knowledge to continue with the next level: Information Security Practitioner.

Target audience

The training is intended for all those who aspire to protect systems and networks against information security threats and raise cybersecurity awareness across their organisation.

Exam information

You can take your exam at an accredited exam centre or book an exam directly with the SECO-Institute.

Attending a course is not a prerequisite for taking an exam.

Examination details

- Computer-based
- 40 multiple-choice questions
- Time allotted: 60 minutes
- Pass mark: 60% (60 points out of 100)
- Open book/notes: not permitted
- Electronic equipment: not permitted

Rules to be observed by candidates: The SECO-Institute's Examination Rules and Regulations

(https://www.seco-institute.org/html/filesystem/storeFolder/10/General-Terms-and-Conditions-for-participation-in-SECO-Institute-exams-2017-11.pdf)

Exam requirements

The following tables list the exam requirements and exam specifications.

Information Security Foundation										
Requirements	1. Information Security Management System (ISO/IEC 27001) & Code of Practice for Information Security Controls (ISO/IEC 27002) 2. Information and Security 3. Threats and Risks 4. Approach and Organisation 5. Security Measures 6. Legal and Regulatory Requirements									
Required prior knowledge	None									
Learning levels	x	Know	x	Understand		Apply		Analyse, Synthesise		Create

Exam specifications

Bloom level
1. Know
2. Understand

	Requirements, specifications, testing levels			Bloom level
1.	**Information Security Management System (ISO 27001) & Code of Practice for Information Security Controls (ISO 27002)**			
	1.1	The candidate is familiar with the contents of ISO 27001 and ISO 27002		
		The candidate is able to:		
		1.1.1	Describe the difference between ISO 27001 and ISO 27002	2
		1.1.2	Describe the focus areas covered in ISO 27001 and ISO 27002	1
		1.1.3	Explain what ISO 27001 requires of an organisation	2
		1.1.4	Describe the Plan-Do-Check-Act (PDCA) cycle and explain its importance for management systems	2
		1.1.5	Define essential terms employed in ISO 27001 (control, control objective)	1
		1.1.6	List examples of the control objectives and controls described in ISO 27001	1
	1.2	The candidate can summarise the key challenges of implementing ISO 27001		
		The candidate is able to:		
		1.2.1	Recall that standards and best practices must be tailored to the organisation's context	1
		1.2.2	Describe the role of risk assessment and risk analysis in selecting suitable control measures	2

	Requirements, specifications, testing levels			Bloom level
2.	**Information and Security**			
	2.1	The candidate understands the importance of information and information security		
		The candidate is able to:		
		2.1.1	Describe the difference between data and information	1
		2.1.2	Define information security	1
		2.1.3	Define due diligence and due care	1
	2.2	The candidate can describe the main objectives of information security		
		The candidate is able to:		
		2.2.1	Describe the CIA triad (confidentiality, integrity and availability)	1
		2.2.2	Define authenticity, accountability and non-repudiation	2
		2.2.3	List measures aimed at safeguarding confidentiality	2
		2.2.4	List measures aimed at safeguarding integrity	2
		2.2.5	List measures aimed at safeguarding availability	2
	2.3	The candidate understands the scope of influence of information security		
		The candidate is able to:		
		2.3.1	Define information technology, information system, information architecture and operational process	1
		2.3.2	Describe information security's value to the business	1
		2.3.3	Define requirement analysis and information analysis	1
		2.3.4	List the basic activities of strategic information management	1

	Requirements, specifications, testing levels			Bloom level
3.	**Threats and Risks**			
	3.1	The candidate knows basic security and risk management terminology		
		The candidate is able to:		
		3.1.1	Define vulnerability, threat and risk	1
		3.1.2	Define risk analysis and risk assessment	1
		3.1.3	Define incident, disaster and calamity	1
	3.2	The candidate can describe the objectives and components of a risk assessment process		
		The candidate is able to:		
		3.2.1	List the main components of risk assessment	1
		3.2.2	Describe the objectives of risk analysis	1
		3.2.3	Define cost-benefit analysis and explain why it is an important part of risk analysis	2
		3.2.4	Describe the difference between qualitative and quantitative risk analysis	2
	3.3	The candidate knows how to treat security risks		
		The candidate is able to:		
		3.3.1	Categorise security measures (preventive, detective, repressive, corrective) and list examples in each category	2
		3.3.2	List the main types of security threats	1
		3.3.3	Define direct and indirect damage	1
		3.3.4	Define Annual Loss Expectancy and Single Loss Expectancy	1
		3.3.5	Define risk appetite and describe risk attitudes (risk-seeking, risk-neutral and risk-averse)	2
		3.3.6	Describe basic risk treatment options	2
		3.3.7	List the main factors that should be taken into account when deciding how to treat a risk	1

	Requirements, specifications, testing levels			Bloom level
4.	**Approach and organisation**			
	4.1	The candidate understands the importance of effective information security governance		
		The candidate is able to:		
		4.1.1	Summarise the objectives, structure and contents of an information security policy	1
		4.1.2	Understand the importance of communicating, maintaining and enforcing the policy	2
		4.1.3	List issue-specific policies relating to information security	2
	4.2	The candidate knows how an information security organisation should be designed and operated		
		The candidate is able to:		
		4.2.1	Recall the objectives of an information security organisation	1
		4.2.2	Summarise top management's responsibility in supporting and organising information security	2
		4.2.3	Summarise ISO 27001 requirements for organising information security	1
		4.2.4	Summarise the importance and the potential contents of a code of conduct	1
		4.2.5	Summarise the importance of assigning ownership	2
		4.2.6	Describe roles and responsibilities in relation to information security (top management, asset owners, Chief Information Security Officer, Information Security Officer, Data Protection Officer)	2
	4.3	The candidate has a basic understanding of information security incident management		
		The candidate is able to:		
		4.3.1	Describe the objectives of information security incident management	1
		4.3.2	List the stages of the incident management process	1
		4.3.3	List the main causes of information security incidents	1
		4.3.4	Recall the incident cycle	1

	Requirements, specifications, testing levels			Bloom level
5.	**Security Measures**			
	5.1	The candidate can categorise security measures		
		The candidate is able to:		
		5.1.1	List examples of preventive, detective, repressive and corrective security measures	1
	5.2	The candidate understands the importance of information classification		
		The candidate is able to:		
		5.1.1	Explain why information should be labelled	1
		5.1.2	Describe what classification levels may exist	1
	5.3	The candidate can describe common physical, technical and organisational information security measures		
		The candidate is able to:		
		5.3.1	Describe security zoning, equipment security and facility security	1
		5.3.2	Summarise the objectives of access control and logical access management	2
		5.3.3	Recall the importance of secure cloud services	1
		5.3.4	Explain basic cryptography terms and principles (symmetric and asymmetric encryption, public key and private key, key management, Kerckhoffs's principle)	2
		5.3.5	Define TLS/SSL, VPN, S/MIME, Pretty Good Privacy and digital signatures	1
		5.3.6	Define the most common types of cybersecurity attacks (phishing, spam, malware, virus, worm, Trojan, hoax, logic bomb, spyware, ransomware, botnet, rootkit)	1
		5.3.7	Describe the importance of policy, awareness, and segregation of duties	1
		5.3.8	Describe the objectives and components of access control	1
		5.3.9	Summarise the characteristics of a password management system	1
	5.4	The candidate understands the relationship between information security and business continuity management		
		The candidate is able to:		
		5.4.1	Define business continuity management, business continuity planning and disaster recovery planning	1
		5.4.2	Recall the importance of testing and exercising information continuity processes and procedures	

	Requirements, specifications, testing levels			Bloom level
6.	**Laws and regulations**			
	6.1	The candidate understands legal and regulatory requirements relating to information security		
		The candidate is able to:		
		6.1.1	Define compliance and list compliance areas for information security	1
		6.1.1	List laws and regulations that are related to information security	1
		6.1.2	List control measures that can facilitate compliance	1

Exam-literature matrix

Exam requirement	Exam specification	Literature
1	1.1 -1.2	**Module 1**
2	2.1-2.3	**Module 2**
3	3.1-3.3	**Module 3**
4	4.1-4.3	**Module 4**
5	5.1-5.4	**Module 5**
6	6.1	**Module 6**

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 and take exams at your convenience. 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 exam, 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

The SECO-Institute has partnered with Acclaim to provide certification holders with a digital badge of their SECO-Institute certification. Digital badges can be used in email signatures, personal websites, social media sites and electronic copies of resumes.

Claim your badge and exhibit your new skills:

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