IT-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: IT-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.

Information security rests on three pillars: people, processes, and technology. The SECO Institute's IT-Security course introduces you to the main technical tools and the related vocabulary in an accessible way.

Context

The IT-Security Foundation (S-ITSF) certificate constitutes the first level of the SECO-Institute's IT-Security track within the Cyber Security & Governance Certification Program. The successful completion of this foundation course provides candidates with sufficient knowledge to be able to advance their career by continuing with the Practitioner level.

Exam topics

- Technological aspects of an IT infrastructure;
- TCIP/IP Networking, Computer Systems, Applications & Databases;
- Cryptography, Identity & Access Management;
- Cloud Computing and Exploiting Vulnerabilities.

Target audience

The IT-Security Foundation certification (S-ITSF) is suitable for those who need to demonstrate basic technical knowledge and familiarity with IT security concepts.

For example:

- Starting information security professionals;
- IT-Auditors;
- Service Management staff;
- Service Desk staff.

Prerequisites

None. However, attending an accredited IT-Security course is recommended.

Exam information

SECO-Institute provides the official IT-Security Foundation courseware for accredited training providers. 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.

Rules can be downloaded from the SECO-institute's website.

Exam requirements

The following tables list the exam requirements and exam specifications.

IT-Security Foundation										
Requirements	**1.** Security in Networks, Systems, Software and Databases **2.** Assuring security through crypto and access control **3.** Cloud Computing & Exploiting Vulnerabilities									
Required prior knowledge	None (However, basic ITSM and technical knowledge/experience is preferable).									
Learning levels	x	Know	x	Understand		Apply		Analyse, Synthesise		Create

Exam specifications

Taxonomies:

1_Knowing
2_Understanding

	Requirements, specifications, testing levels			Bloom level
1.	**Security in Networks, Systems, Software, and Databases**			
	1.1	The candidate understands the concept of computer systems, their components, and how they can be vulnerable to threats.		
		The candidate is able to:		
		1.1.1	Recall types of computer systems and their components.	2
		1.1.2	Describe security measures for computer hardware.	2
		1.1.3	Recall the types of distributed computing.	1
		1.1.4	Explain the concept of computer virtualisation.	2
		1.1.5	Recall types of vulnerabilities in operating systems.	1
		1.1.6	Describe different types of defence and measures against malicious software.	2
Exam topics and terms	• Computer architecture • I/O services • Driver • Communication ports (hardware) • Emanations • Covert channels • RAID • OS: monolithic, layered, client/server • Tiers • SPOF • Multi-tier • Peer-to-peer • Grid computing			

			• Virtualisation • Virtual machine • Middleware • Embedded systems • Vulnerabilities	
	1.2	The candidate understands the concept of TCP/IP networking and related vulnerabilities.		
		The candidate is able to:		
		1.2.1	Recall the definitions of TCP/IP networking.	1
		1.2.2	Describe the TCP/IP and OSI architecture models.	2
		1.2.3	Explain the concept of network nodes and node addressing.	2
		1.2.4	Describe Important security protocols and techniques	1
		1.2.5	Describe the concept and techniques of IP-addressing, and related vulnerabilities.	2
		1.2.6	Recall data communication types and techniques.	1
Exam topics and terms			• TCP/IP • OSI • Protocols: HTTP, TCP, IP, Ethernet, WiFi, ARP, UDP, FTP, VoIP, DNS, MIME, etc. • Node • Link • Network • Protocol • Interface • Network model • Hub, switch, bridge, router • Firewall • Security protocol • Network filter • Network topology • Node addressing • DMZ • Proxy server • Bastion host • IPv4, IPv6 • Port, port scanning • Penetration testing • Man-in-the-middle attack	
	1.3	The candidate understands the concept of computer applications and related vulnerabilities.		
		The candidate is able to:		
		1.3.1	Recall common problems and security issues for application programmers.	1
		1.3.2	Recall critical web application security risks.	1

		1.3.3	Describe application security policies.	2
Exam topics and terms			• Patch management • API • HTML • Javascript • Flash • Sandbox • Malware • OWASP	
	1.4	The candidate understands the concept of databases and related vulnerabilities.		
		The candidate is able to:		
		1.4.1	Recall the definition of a database.	1
		1.4.2	Explain the different integrity mechanisms for databases.	2
		1.4.3	Describe different concepts related to the relational database model.	2
		1.4.4	List different types of database vulnerabilities and countermeasures.	1
		1.4.5	Explain the concept of auditing & monitoring.	2
Exam topics and terms			• DBMS • Relational database model • SQL: DDL, DML, DCL • Data warehouse • Metadata • Data dictionary • Directory services • Aggregation • Bypass attack • Concurrency • Data contamination • Deadlocking • DoS, DDoS • Inference	

	Requirements, specifications, testing levels			level
2.	**Assuring security through crypto and access control**			
	2.1	The candidate understands the concept of cryptography.		
		The candidate is able to:		
		2.1.1	Recall the concepts of encryption.	1
		2.1.2	Describe encryption systems.	1
		2.1.3	Explain the concepts of Asymmetric, Symmetric, and hybrid encryption.	2
		2.1.4	Explain security techniques based on encryption.	2

		2.1.5	Describe the concepts of Public Key Infrastructure (PKI).	2
		2.1.6	Describe types of Cryptographic Security techniques	2
Exam topics and terms			• Identity and access management • Identity • Authentication • Authorisation • Accountability • Keys, algorithms • Plaintext, cleartext, ciphertext, cryptogram • Encryption, decryption • Symmetric, asymmetric, Hybris (encryption) • Hash • Work factor • Substitution, transposition • Digital signature • Non-repudiation • Kerckhoff's principle • PKI • CRL, OCSP • TSL, SSL, IPSec, PGP,	
	2.2	The candidate understands the concept of Identity & Access Management.		
		The candidate is able to:		
		2.2.1	Recall the key terms of Identity & Access Management.	1
		2.2.2	Explain different types of authentication.	2
		2.2.3	Describe different types of identification techniques.	2
		2.2.4	Explain the concept of accountability.	2
Exam topics and terms			• Identification, authentication, authorisation, accountability • Multifactor, Continuous (authentication) • Biometrics • Password management • Password salting • Cookies • SSO • Kerberos • OpenID, OAuth • Authorisation: MAC, DAC, RBAC, ABAC • IAM (services) • Federation	

	Requirements, specifications, testing levels	level
3.	**Cloud Computing & Exploiting Vulnerabilities**	

	3.1	The candidate understands the concept of Cloud computing.		
		The candidate is able to:		
		3.1.1	Recall Cloud computing characteristics and models.	1
		3.1.2	Describe Cloud computing service models.	2
		3.1.3	Explain the risks of using the cloud.	2
Exam topics and terms		• On-demand self-service • Broad network access • Resource pooling • Rapid elasticity • Measured service • Private cloud • Community cloud • Public cloud • Hybrid cloud • Software as a Service (SaaS) • Platform as a Service (PaaS) • Infrastructure as a Service (IaaS) • Security as a Service (SECaaS) • Identity as a Service (IDaaS)		
	3.2	The candidate understands the concepts of exploiting vulnerabilities.		
		The candidate is able to:		
		3.2.1	Recall the components of the STRIDE model.	1
		3.2.2	Recall attack categories.	1
		3.2.3	Describe the actors of exploiting vulnerabilities.	2
		3.2.4	List the steps for penetration.	1
		3.2.5	Recall types of attacks.	1
		3.2.6	Describe different tools and their purpose.	2
Exam topics and terms		• STRIDE • Full penetration • Denial of service • Information theft or disclosure • Social engineering • Zero-day exploit • Hackers: White, Black, Grey hats • Script kiddy • Hacktivist • Fingerprinting • Penetration • Privilege escalation • Undirected & Directed attacks •		

Literature

Required	*Course material for ITSF: 4 modules (including the introductory module)*
Optional	No additional literature

Exam-literature matrix

Exam requirement	Exam specification	Literature (A, B, C)	Chapter reference(s)
1	1.1	**Module 1**	Computer systems
	1.2	**Module 1**	TCP/IP Networking
	1.3	**Module 1**	Applications
	1.4	**Module 1**	Databases
2	2.1	**Module 2**	Cryptography
	2.2	**Module 2**	Identity & Access Management
3	3.1	**Module 3**	Cloud computing
	3.2	**Module 3**	Exploiting Vulnerabilities

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 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

ITSF-EN-2018-01a