Preparation Guide

Edition 201805

Content

1. Overview

EXIN Cyber & IT Security Foundation (CISEF.EN)

Scope

The subjects of this module are:

- TCP/IP Networking
- Computer Systems
- Applications & Databases
- Cryptography
- Identity & Access Management
- Cloud Computing
- Exploiting Vulnerabilities

Summary

Security in IT is not only becoming more important but also more sophisticated. In light of this, organizations are dedicating roles to the safeguarding of their data and systems. The EXIN Cyber & IT Security program is geared towards providing candidates with the required knowledge to understand the technical side of information security. It covers the theoretical background, detailed information about security infrastructure and goes into the vulnerabilities, risks, and required measures.

Context

The Certificate EXIN Cyber & IT Security Foundation is part of the overall qualification scheme for Cyber & IT Security.

Target group

- Network Administrator
- Application Developer
- Security Officer
- Auditor
- Quality Manager
- Operational Manager

Requirements for certification

- Successful completion of the EXIN Cyber & IT Security Foundation exam.

Examination details

Examination type:	Multiple-choice questions
Number of questions:	40
Pass mark:	65%
Open book/notes:	No
Electronic equipment/aides permitted:	No
Time allotted for examination:	60 minutes

The Rules and Regulations for EXIN's examinations apply to this exam.

Bloom level

The EXIN Cyber & IT Security Foundation certification tests candidates at Bloom Level 1 and Level 2 according to Bloom's Revised Taxonomy:

- Bloom Level 1: Remembering – relies on recall of information. Candidates will need to absorb, remember, recognize and recall. This is the building block of learning before candidates can move on to higher levels.
- Bloom Level 2: Understanding – a step beyond remembering. Understanding shows that candidates comprehend what is presented and can evaluate how the learning material may be applied in their own environment. This type of questions aims to demonstrate that the candidate is able to organize, compare, interpret and choose the correct description of facts and ideas.

Training

Contact hours

The recommended number of contact hours for this training course is 16. This includes group assignments, exam preparation and short breaks. This number of hours does not include homework, the exam session and lunch breaks.

Indication study effort

60 hours, depending on existing knowledge.

Training organization

You can find a list of our accredited training organizations at www.exin.com.

2. Exam requirements

The exam requirements are specified in the exam specifications. The following table lists the topics of the module (exam requirements) and the subtopics (exam specifications).

Exam requirement	Exam specification	Weight
1. Tcp/Ip Networking		**10%**
	1.1 Nodes, Node Connections & TCP/IP Addressing	5%
	1.2 OSI Model, TCP/IP Model, Protocols	5%
2. Computer Systems		**10%**
	2.1 Computer Architecture, Operating Systems	5%
	2.2 Computer System Vulnerabilities	2.5%
	2.3 Computer System Security Measures	2.5%
3. Applications & Databases		**15%**
	3.1 Application Development	5%
	3.2 Databases	5%
	3.3 Security Issues & Countermeasures	5%
4. Cryptography		**20%**
	4.1 Encryption Methodologies & Standards	5%
	4.2 Digital Signatures, Hashing	5%
	4.3 Public Key Infrastructure (Pki)	5%
	4.4 SSL/TLS, Ipsec	5%
5. Identity & Access Management		**15%**
	5.1 Identification, Authentication, Biometrics, Single Sign-On (SSO), Password Management	10%
	5.2 Authorization	5%
6. Cloud Computing		**15%**
	6.1 Characteristics & Deployment Models	10%
	6.2 Risks	5%
7. Exploiting Vulnerabilities		**15%**
	7.1 Attack Categories & Threat Types	5%
	7.2 Actors & Tools	10%
	Total	**100%**

Exam specifications

1. TCP/IP Networking

1.1 Nodes, Node Connections & TCP/IP Addressing

The candidate can...

1.1.1 describe what a node is.

1.1.2 describe how nodes can be connected to each other.

1.1.3 explain the concepts of TCP/IP addressing of both IP v4 and IP v6.

1.2 OSI Model, TCP/IP Model, Protocols

The candidate can...

1.2.1 describe the layers and main functionalities of the OSI and TCP/IP models.

1.2.2 explain the main network protocols, what their functionality is and how they fit into the OSI and TCP/IP reference models.

2. Computer Systems

2.1 Computer Architecture, Operating Systems

The candidate can...

2.1.1 explain the components of a computer system.

2.1.2 describe how an operating system works.

2.1.3 list the main operating systems.

2.2 Computer System Vulnerabilities

The candidate can...

2.2.1 identify the most prevalent types of computer system vulnerabilities.

2.3 Computer System Security Measures

The candidate can...

2.3.1 identify the main security measures related to computer systems.

3. Applications & Databases

3.1 Application Development

The candidate can...

3.1.1 explain the different methods and phases of the systems development life cycle.

3.1.2 describe the advantages and disadvantages of each of the different methods of the systems development lifecycle.

3.1.3 explain how to address security during the systems development life cycle.

3.2 Databases

The candidate can...

3.2.1 describe the different database models.

3.2.2 explain the functionality of the database and the database management systems.

3.3 Security Issues & Countermeasures

The candidate can...

3.3.1 describe the prevalent security issues related to applications development and databases.

3.3.2 explain the countermeasures against security issues related to applications and databases.

4. Cryptography

4.1 Encryption Methodologies & Standards

The candidate can...

4.1.1 differentiate between symmetric and asymmetric encryption.

4.1.2 identify encryption algorithms and standards.

4.2 Digital Signatures, Hashing
The candidate can...
4.2.1 explain how digital signatures provide for authenticity and non-repudiation.
4.2.2 explain how hashing provides for the integrity of digital information.
4.2.3 describe the main hashing standards.
4.3 Public Key Infrastructure (PKI)
The candidate can...
4.3.1 describe the components, parties and processes of a public key infrastructure.
4.3.2 explain what digital certificates and their use cases are.
4.4 SSL/TLS, Ipsec
The candidate can...
4.4.1 explain the technology and use cases of SSL/TLS.
4.4.2 explain the technology and use cases of IPSec.

5. Identity & Access Management

5.1 Identification, Authentication, Biometrics, Single Sign-On (SSO), Password Management
The candidate can...
5.1.1 differentiate between identification and authentication.
5.1.2 describe the main technologies of authentication and two-factor authentication.
5.1.3 explain biometrics and their use cases.
5.1.4 explain the concepts and different types of Single sign-on (SSO).
5.1.5 explain password management and its use cases.
5.2 Authorization
The candidate can...
5.2.1 describe how the principles of Need to know, Least privilege and Separation of Duties (SoD) relate to authorization.
5.2.2 describe authorization models such as role-based access control (RBAC) and attribute-based access control (ABAC).
5.2.3 describe the specifications and functionality of OpenID Connect and OAuth.

6. Cloud Computing

6.1 Characteristics & Deployment Models
The candidate can...
6.1.1 differentiate between the deployment models public cloud, private cloud and hybrid cloud.
6.1.2 explain the service models SaaS, PaaS, IaaS, SECaaS and IDaaS.
6.2 Risks
The candidate can...
6.2.1 identify the risks of cloud computing.

7. Exploiting Vulnerabilities

7.1 Attack Categories & Threat Types
The candidate can...
7.1.1 identify the main attack categories of cybercrime.
7.2 Actors & Tools
The candidate can...
7.2.1 recognize Black hat hackers, White hat hackers, Grey hat hackers, Script kiddies and Hacktivists.
7.2.2 identify which tools cybercriminals use.
7.2.3 identify the steps cybercriminals take to exploit vulnerabilities.

3. List of Basic Concepts

This chapter contains the terms and abbreviations with which candidates should be familiar.

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

TCP/IP networking

Address Resolution Protocol (ARP)
Alternative routing
American National Standards Institute (ANSI)
Anomaly based
Application level
Architecture
Bastion host
Blocking
Boundary router
Broadcast domain
BSID
Cabling
Challenge-Response
Compartmentalization
Connection
Data link
Deep packet inspection
Defense Advanced Research Projects Agency (DARPA)
Defense in Depth
Demilitarized Zone (DMZ)
Destination node
Direct link
(Distributed) Denial of Sevice ((D)DoS) attack
Diverse routing
Domain Name System (DNS)
EIA/TIA
Ethernet
External footprint
False negative / False positive
File Transfer Protocol (FTP)
Filter
Firewall (rules)
Frame
Gateway
Hardware address
Honeypot
Host-based intrusion detection system (HIDS)
HTTP
Hub
Institute of Electrical and Electronics Engineers (IEEE)
Interface
Internet Engineering Task Force (IETF)
Network model
Network segmentation
Next-generation firewall
NIC
NIDS
NOC
Node
Open ports
OSI
Outbound traffic
Packet
Penetration test
Perimeter
Physical address
POP3
Port numbers
Port scanning
Private address
Protocol
Protocol flaws
Proxy (firewall / server)
Public address
Redundancy
Regional Internet Registry (RIR)
Remote access
Request for Change (RfC)
Request for Comment
Request for Proposal (RfP)
Rogue device
Screened subnet
Secure Shell
Secure Socket Layer (SSL)
Secure/Multipurpose Internet Mail Extensions (S/MIME)
Security protocols
Session hijacking
Signature based
Simple Network Management Protocol (SNMP)
SMTP
Sniffing
Source node
Source routing
Spoofing

Internet of things (IoT)
Internet protocol (IP) – IPv4 – IPv6
Intrusion detection
Intrusion prevention
Intrusion Prevention System (IPS)
IP spoofing
IPSec
Last mile
Layered defense
Link
Load balancing
Local Area Network (LAN)
Logical address
Long-haul
MAC address
Mail relay
Man-in-the-Middle
Network access
Network address translation
SSH
SSID
Star topology
Stateful / Stateless firewall
Storage Area Network (SAN)
Subnet
Switch
System on Chip (SOC)
TCP/IP
Transport Layer Security (TLS)
True negative / True positive
User Datagram Protocol (UDP)
Virtual Circuit
Virtual Network Connection (VNC)
Virtual Private Network (VPN)
Voice over IP (VOIP)
Wide Area Network (WAN)
Wire tapping

Computer systems

.Net
2-tier
3-tier
Android
Apache
Appaserver
Application server
Backdoor
Backup
Backup schedule
Buffer overflow
Client/Server (C/S)
Core
Covert channel
Data leakage
Data retention
Database server
Desktop Virtualization
Emanation
Exchange
Exploit
External hot site
Fat server
File server
File system
Firmware
Grid
Hardening
Hardware
High-availability systems
Hypertext Preprocessor (PHP)
I/O
Internet Information Services (IIS)
Kolab
Oracle
OS hardening
OS standardization
Out of band channels
Parity
Patch logs
Patch management
Peer to Peer
Peripheral
Primary storage
Print server
Process
Radio-frequency identification (RFID)
RAID
Recovery
Redundant power supply
Remote buffer overflow
Remote lock
Remote support
Remote wipe
Restore
Root kit
Secondary storage
Security domains
Security information and event management (SIEM)
Security tokens
Single Point of Failure (SPOF)
SQL server
SSD
Storage capacity
Storage device
Striping
Sun
Supercomputer

Layered OS
Log entries
Log reports
Longevity
Mail server
Mainframe
Media sanitization
Memory card
Mobile devices
Monolithic
Multiprocessing
Multithreading
MySQL
Non-volatile random-access memory (NVRAM)
N-tier
Tablet
TEMPEST
Thin client
Trojan
Unattended screens
Unix
Unpatched
Virtual memory
Virtualization
Web security
Worm
z/OS
z/VM
Zimbra

Applications

Active X
Application development
Application Programming Interface (API)
Application security
Application virtualization
Automatic Teller Machine (ATM)
Code review
Cross-site scripting (XSS)
Debugging
Dialog box
E-banking
Electronic Data Interchange (EDI)
Electronic Fund Transfer (EFT)
Electronic payment
Flash
Geographic software
HyperText Markup Language (HTML)
Implementation flaws
Input attacks
Input sanitization
Java
Java script
Java security manager
Malicious code
Mobile code
Office suits
Privileged access
Sandbox
Silverlight
Software development
SQL injection
Testing
Ubiquitous
Unicode attack
User acceptance testing
User interface
VBscript
Web applications

Databases

Aggregation
Big data
Bypass attack
Concurrency
Data Base Management System (DBMS)
Data contamination
Data Control Language (DCL)
Data custodian
Data Definition Language (DDL)
Data dictionary
Data integrity
Data Manipulation Language (DML)
Data mining
Data owner
Data warehouse
Database hardening
Deadlock
Inference
Injection attack
Integrity
Lightweight Directory Access Protocol (LDAP) - OpenLDAP
Maintainability
Metadata
Misdirection
NoSQL
Online Transaction Processing (OLTP)
Primary key
Query attack
Relational model
Reusability
Sensitive data
Structured Query Language (SQL)
Transaction persistence
Unattended disks

Directory services
Foreign key
View
X.500

Cryptography

3DES (Triple DES) - Data Encryption Standard
Advanced Encryption Standard (AES)
Algorithm
Asymmetric encryption
Authenticity
Brute force
Caesar
Certificate Authority (CA)
Certificate Revocation List (CRL)
Ciphertext
Cleartext
Closed message format
Confidentiality
Cracking
Cryptanalysis
Crypto system
Cryptogram
Data at rest
Data in situ
Decryption
Dictionary attack
Diffie-Hellman
Digital certificate
Digital signature
Elliptic curve cryptography (ECC)
Encrypted passwords
Encryption
Encryption strength
Hash value
Hashing
Hybrid encryption
International Data Encryption Algorithm (IDEA)
Kerckhoffs' principle
Key
Key length
Key management
Key rings
Keyspace
Mathematical function
MD4 , MD5
Message Authentication Code (MAC)
Message integrity
No security by obscurity
Non-repudiation
Online Certificate Status Protocol (OCSP)
Open message format
OpenPGP
Plaintext
Pretty Good Privacy (PGP)
Private key
Proof of origin
Public key
Public Key Infrastructure (PKI)
Quantum encryption
RC4, RC5, RC6
Registration Authority (RA)
Rijndael
ROT13
RSA
SAFER (Secure And Fast Encryption Routine)
Secrecy
Secret key
Secure Hash Algorithm (SHA)
Session key
Side channel attack
Substitution cipher
Symmetric encryption
Symmetric key
Temporal Key Integrity Protocol (TKIP)
Transposition cipher
Trusted Third Party
Validation Authority (VA)
Weak encryption
WiFi Protected Access (WPA)
Wired Equivalent Privacy (WEP)
Work factor
X.509

Identity & Access Management

Access control
Access control matrix
Access privileges
Access rule violations
Accessibility
Account lockout
Account ownership
Accountability
Attribute-Based Access Control (ABAC)
Audit logs
Authentication
Keystroke dynamics
Least privilege
Logical access
Mandatory
Multi-factor
Need-to-know
OASIS
OAuth 2.0
OpenID Connect
Passphrase
Physical access control

Authentication hijacking
Authentication server
Authorization
Biometric authentication
Biometrics
Cookies
Credentials
Cross-over error rate
Discretionary
eXtensible Access Control Markup Language (XACML)
Facial scanning
False match
Fingerprint scanning
Handpalm scanning
HTTP-based authentication
Identification
Identity & Access
Iris scanning
Kerberos
PIN code
Retina scanning
Role mining
Role-Based Access Control (RBAC)
Salting
Security Assertion Markup Language (SAML)
Separation of duties (SoD)
Single sign-on (SSO)
Single-factor
Smartcard
Strong authentication
Strong password
System for Cross-domain Identity Management (SCIM)
Token devices
Two-factor
User ID
Vascular pattern
Voice recognition

Cloud computing

Cloud
Cloud checklist
Community cloud
Customer lock-in
Data retrieval
Data storage
Deployments
Dropbox
EU-US Privacy Shield
Exit strategy
Google docs
Hardware platform
Hybrid cloud
iCloud
Identity as a Service (IDaaS)
Infrastructure as a Service (IaaS)
Jurisdiction
Multi-tenant
OneDrive
OpenStack
Platform as a Service (PaaS)
Private cloud
Public cloud
Safe Harbor
Security as a Service (SECaaS)
Service Level Agreement (SLA)
Software as a Service (SaaS)
Software platform
Vendor default
Vendor lock-in
Web services

Exploiting Vulnerabilities

Active probing
Actor
Advanced Persistent Threat (APT)
Anonymous
Antivirus software
Attacks
Auditing
Black hat hacker
Blackbox pentest
Confidentiality, Integrity, Availability (CIA)
Configuration weakness
Containment
Countermeasures
Cracker
Data breach
Malware
Mantrap
Metasploit
MIME content
Monitoring
Nessus
Nmap
Novice
Penetration
Pentest
Phishing
Physical security
Pivot
Prevention
Reaction

Decoy files
Defacing
Detection
Email attachments
Environmental security
Ethical hacker
Event
Evidence
Exposures
External threat
Forensics
Freenet
Gray hat hacker
Hacker
Hacktivist
Identity theft
Incident
Incident management
Incident response
Information theft
Internal threat
Logging
Macros
Reconnaissance
Remote Administration Tool (RAT)
Scanning
Script kiddie
Scripting
Security baseline
Security monitoring
Sensitivity
Social engineering
STRIDE
- Spoofing identity
- Tampering with data
- Repudiation
- Information disclosure
- Denial of Service
- Elevation of privilege

Threat assessment
Tools
Tor
Vandalism
Virus detection
Vulnerability
Vulnerability assessment
Vulnerability exploitation
Vulnerability scan
Warez
White hat hacker
Worms
Zero-day exploit

4. Literature

Exam literature

The knowledge required for the exam is covered in the following literature:

A. David Kim, Michael; G. Solomon
Fundamentals of Information Systems Security
Jones & Bartlett Learning, LLC (2018, 3rd edition)
ISBN: 978-1-284-11645-8

Additional literature

B. Hans van den Bent, Eline Kleijer
EXIN Ethical Hacking Foundation – Exam Literature
EXIN (latest version)
Downloadable on the product page, or via http://bit.ly/EHF-literature

Comment

Additional literature is for reference and depth of knowledge only. Literature B was written as complementary exam literature for EXIN Ethical Hacking Foundation and also covers specification 7.2 of the EXIN Cyber & IT Security Foundation module.

Literature matrix

Exam requirement	Exam specification	Literature
1. Tcp/Ip Networking		
	1.1 Nodes, Node Connections & TCP/IP Addressing	A: Chapter 2, 10
	1.2 OSI Model, TCP/IP Model, Protocols	A: Chapter 10
2. Computer Systems		
	2.1 Computer Architecture, Operating Systems	A: Chapter 1, 6, 11
	2.2 Computer System Vulnerabilities	A: Chapter 1, 6
	2.3 Computer System Security Measures	A: Chapter 5, 6, 7, 8
3. Applications & Databases		
	3.1 Application Development	A: Chapter 6
	3.2 Databases	A: Chapter 5, 6
	3.3 Security Issues & Countermeasures	A: Chapter 5, 6
4. Cryptography		
	4.1 Encryption Methodologies & Standards	A: Chapter 9
	4.2 Digital Signatures, Hashing	A: Chapter 9
	4.3 Public Key Infrastructure (Pki)	A: Chapter 9
	4.4 SSL/TLS, Ipsec	A: Chapter 9
5. Identity & Access Management		
	5.1 Identification, Authentication, Biometrics, Single Sign-On (SSO), Password Management	A: Chapter 5, 9
	5.2 Authorization	A: Chapter 5
6. Cloud Computing		
	6.1 Characteristics & Deployment Models	A: Chapter 5
	6.2 Risks	A: Chapter 4
7. Exploiting Vulnerabilities		
	7.1 Attack Categories & Threat Types	A: Chapter 3, 11
	7.2 Actors & Tools	A: Chapter 1, 11 B: Chapter 1, 2, 3

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER