



# **EUCIP - IT Administrator**

## **Module 5 – IT Security**

**Version 2.0**

## Module 5 Goals

**Module 5** Module 5, *IT Security*, requires the candidate to be familiar with the various ways of protecting data both in a single PC and in a LAN with internet connection. More specifically the candidate should be able to protect the company data from loss, virus attack and hacking. Also he/she should be able to know and handle the most common utilities and programs designed for this purposes.

Category	Knowledge Area	Ref.	Knowledge Item
5.1. General	5.1.1. Basic concepts	5.1.1.1	Know what are the main aspects of information security: confidentiality, integrity
		5.1.1.2	Be aware of availability, authentication, and non-repudiation.
	5.1.2. Risk management	5.1.2.1	Know what are the main issues involved in risk assessment (value of information, vulnerability, threat, hazard, violation, impact, level of risk).
		5.1.2.2	Know the most common classification of technical mean to control the risk (identification and authentication, access control, accountability, audit, object reuse, accuracy, reliability of service, secure data exchange).
		5.1.2.3	Know the distinction between functionality and assurance, and the importance of achieving both of them to control the risk.
	5.1.3 Information Security Management	5.1.3.1	Know the role of a security policy in driving the management of IT security
		5.1.3.2	Know what are the main processes to be implemented in an organization aiming at achieving information security
		5.1.3.3	Be aware of the need of disaster recovery and business continuity planning
		5.1.3.4	Know responsibilities of all the roles involved in an organization, (security officers, system administrators, everyday users)
		5.1.3.5	Know how to participate in a Computer Security Incident Response Team (CSIRT).
	5.1.4 Standards and standardization bodies	5.1.4.1	Know what are the main standardization bodies and their role.
		5.1.4.2	Know the availability of a methodology to assess different levels of assurance (ITSEC, Common Criteria).

Category	Knowledge Area	Ref.	Knowledge Item
		5.1.4.3	Know the essence of a published standards (ISO/IEC 17799, BS 7799 part 2) aimed at helping in building a security management infrastructure inside the organization
		5.1.4.4	Know the Internet Standards process
5.2. Cryptography	5.2.1 General	5.2.1.1	Know basic scopes of cryptography: symmetric and asymmetric encryption, hashing algorithms.
	5.2.2. Symmetric encryption	5.2.2.1	Be aware of principles of symmetric encryption.
		5.2.2.2	Know main symmetric encryption standards and their main differences ( DES, 3DES,AES ...)
	5.2.3. Asymmetric encryption	5.2.3.1	Be aware of principles of asymmetric encryption.
		5.2.3.2	Know main public-key standards
	5.2.4 Hash and digest functions	5.2.4.1	Be aware of principles of hash and digest functions
		5.2.4.2	Know the main hashing functions standards
	5.2.5 Comparison between encryption methods	5.2.5.1	Know the main advantages and disadvantages of symmetric and asymmetric encryption.
		5.2.5.2	Be able to distinguish various level of security and their respective weight
		5.2.5.3	Know the key distribution problem both in symmetric and asymmetric cryptography
		5.2.5.4	Know role played by open source in enforcing cryptography availability and robustness.
	5.2.6 Usage	5.2.6.1	Know how to use encryption mechanisms to achieve authenticity
		5.2.6.2	Be aware of the usage of hashing and digest in enforcing integrity and authentication .
		5.2.6.3	Know main aspects of electronic signature in enforcing non-repudiation and authentication.
		5.2.6.4	Know principles and main characteristics of encryption in enforcing confidentiality.
	5.2.7 Applications	5.2.7.1	Be aware of the usage of cryptography to protect data in on-line transactions such as in e-commerce and e-banking
		5.2.7.2	Be aware of the usage of digital signature to enforce non-repudiation
		5.2.7.3	Know main working aspects of PGP.
		5.2.7.4	Be able to install and setup a software product that manages pgp protocol.

Category	Knowledge Area	Ref.	Knowledge Item	
		5.2.7.5	Know working principles of SSH.	
		5.2.7.6	Be able to install and setup a software product that manages ssh protocol.	
		5.2.7.7	Know the working principles of S/MIME	
		5.2.7.8	Know the working principles of SSL	
		5.2.7.9	Be aware of the usage of smartcards.	
5.3 Authentication and Access Control	5.3.1. General concepts of authentication	5.3.1.1	Know different authentication schemes.	
	5.3.2. Passwords	5.3.2.1	Know principles of password management.	
	5.3.3 Token	5.3.3.1	Know the principles of token authentication	
	5.3.4 Biometrics	5.3.4.1	Know different biometric authentication schemes and their effectiveness	
	5.3.5 Network authentication		5.3.5.1	Know the different requirements for network vs. host authentication
			5.3.5.2	Know different network protocols for users authentication (PAP, CHAP...)
			5.3.5.3	Know different network protocols for (distributed) processes authentication
			5.3.5.4	Be aware of complexity of single sign-on architectures
			5.3.5.5	Know main working principles of Kerberos
	5.3.6 Access Control		5.3.6.1	Know the principles of access control
			5.3.6.2	Know what is an Access Control List and what is a list of capabilities
			5.3.6.3	Know how to manage access control in common file systems
			5.3.6.4	Know how to manage access control in a Relational Database Management System
5.4 Availability	5.4.1 General	5.4.1.1	Know different types of information availability requirements	
		5.4.1.2	Know different kinds of infrastructure requirements needed for ICT (UPS, air-conditioning, cabling etc.)	
	5.4.2 Resilience	5.4.2.1	Be aware of different kinds of Hard-Disk real-time replica mechanisms (RAID etc.)	
		5.4.2.2	Be aware of different kinds of host replication and load distribution mechanisms	

Category	Knowledge Area	Ref.	Knowledge Item
		5.4.2.3	Know different kinds of network availability infrastructures (for LAN, WAN, WLAN etc.)
	5.4.3 Backup	5.4.3.1	Be able to implement effective back-up procedures (local and network)
		5.4.3.2	Know how to test a backup and to implement a recovery
5.5 Malicious Code	5.5.1. Programs	5.5.1.1	Know what can command a computer: operating system, programs, shells, macros.
		5.5.1.2	Know about input validation requirements for security
		5.5.1.3	Be aware of different kind of overflows and how they can be used to execute code
		5.5.1.4	Be aware of cross site scripting
		5.5.1.5	Be aware of Denial of Service and how different environments and resources can be affected
		5.5.1.6	Know the doors from which a computer can be accessible: floppy, cdrom, emails, web browsing, chat clients.
		5.5.1.7	Know what can be considered good practice in Internet access.
		5.5.1.8	know the risks of adware and spyware
	5.5.2 Automatic file type management	5.5.2.1	Know how GUI can recognize what action is to be performed on an attachment using MIME type and extension.
		5.5.2.2	Know how mail client programs can recognize what action is to be performed on an attachment using MIME type and extension.
	5.5.3 Downloadable code	5.5.3.1	Know how applications can handle more than text to perform various OS commands using macros.
		5.5.3.2	Know how people can maliciously use MIME types and how to defend a PC from them.
		5.5.3.3	Know how people can maliciously use macros and how to defend a PC from them.
		5.5.3.4	Know how people can maliciously use applets and how to defend their PC from them.
	5.5.4 Viral Software	5.5.4.1	Know basic categories of viral software (trojan, virus, worms, etc)
		5.5.4.2	Know anti-virus program main working principles.

Category	Knowledge Area	Ref.	Knowledge Item
		5.5.4.3	Be aware of limits and dangerousness of anti virus programs.
		5.5.4.4	Be able to install, setup and update an anti virus program.
		5.5.4.5	Know what can be considered good practice in securing and using a workstation.
5.6 Public Key Infrastructure	5.6.1 PKI	5.6.1.1	Be aware of public-keys distribution problem, even in relation with owner identification issue.
		5.6.1.2	Know the meanings of Certificates and Certificate Revocation Lists.
		5.6.1.3	Know the X.509.V3 Certificates.
		5.6.1.4	Know what PKI means and its principal components, as Registration Authority and Certification Authority.
		5.6.1.5	Be able to use a browser to generate keys and certification request to a CA.
		5.6.1.6	Be able to import and export a certificate into a browser.
		5.6.1.7	Be able to access a CRL from a browser, be able to use Online Certificate Status Protocol
		5.6.1.8	Be able to import a CRL into a browser, be able to use Online Certificate Status Protocol
	5.6.2 Directory services	5.6.2.1	Know LDAP server.
		5.6.2.2	Be able to use a browser to query an LDAP server to obtain data belonging to a particular Distinguished Name.
		5.6.2.3	Know the meanings of Common Name, Distinguished Name, and Attribute.
		5.6.2.4	Know the meanings of X509.
		5.6.2.5	Know how LDAP servers can be used to support user profiles management and authentication
5.7 Network Security	5.7.1. Basic Telecommunication Concepts	5.7.1.1	Be aware of analog and digital communications. Know the basic concepts of ISO/OSI security architecture.
		5.7.1.2	Know the difference of continuous and packet communications.
		5.7.1.3	Know how Ethernet works (MAC address, CSMA/CD).

Category	Knowledge Area	Ref.	Knowledge Item
		5.7.1.4	Understand main aspects of TCP/IP (Addresses, port numbers, main flow of operations).
		5.7.1.5	Know TCP/IP encapsulation in Ethernet.
		5.7.1.6	Understand network services as done in TCP/IP environment.
		5.7.1.7	Be able to install and operate a network analyser.
		5.7.1.8	Be aware of main type of attacks to the TCP/IP stack: sniffing, spoofing, rerouting, connection hijacking, (distributed) denial of service...
		5.7.1.9	Know what switches and VLANs can provide to LAN security
	5.7.2 Wireless networks	5.7.2.1	Know about the main wireless technologies
		5.7.2.2	Know the security risks related to wireless networks and the different technologies, and the available solutions
	5.7.3 Services	5.7.3.1	Be aware of services as access points of servers.
		5.7.3.2	Know the minimum and safest set of services that can be enabled on Internet servers.
		5.7.3.3	Know the set of services that are usually enabled on non-internet servers.
		5.7.3.4	Be aware of main type of wicked usage: abusive usage, denial of service, data falsification, ...
		5.7.3.5	Now the risks of DNS misuse
		5.7.3.6	Be aware of usual authentication schemes and their vulnerability.
		5.7.3.7	Be aware how weakness of protocols or software can be exploited on servers.
		5.7.3.8	Be aware of the fact that clients can be as vulnerable as servers.
		5.7.3.9	Be aware of the risks of Peer-to-peer technologies and programs
		5.7.3.10	Know what can be considered good practice in securing and using a non-internet server.
		5.7.3.11	Know what can be considered good practice in securing and using an internet server.
	5.7.4 Access control	5.7.4.1	Be aware of how network authentication works and how to manage it.

Category	Knowledge Area	Ref.	Knowledge Item
		5.7.4.2	Be aware of cryptographic key based network authentication and how to manage it.
		5.7.4.3	Know domain-based authentication.
	5.7.5 Log management	5.7.5.1	Know the most relevant security informations that can be found in a system log files
		5.7.5.2	Know how to setup logging in applications
		5.7.5.3	Know how to setup a centralized log service
		5.7.5.4	Know how to protect logs from tampering
	5.7.6 HTTP services access control	5.7.6.1	Know differences between http and https-based web sites.
		5.7.6.2	Know how interaction between the web service and other system components can affect security
		5.7.6.3	Be able to implement a secure version of a non-secure web site generating keys and certification request and inserting keys and certificates.
		5.7.6.4	Be able to configure a web site to use plain text password to manage client identification and authorization.
		5.7.6.5	Be able to configure a web site to use certificates to manage client identification and authorization as in SSL V.3.
		5.7.6.6	Know what kinds of access on a directory's objects can be restricted in web sites.
		5.7.6.7	Be able to apply correct access restrictions on a given website directory.
	5.7.7 Email services access control	5.7.7.1	Be aware that e-mail source address and information can be forged
		5.7.7.2	Be able to set up plain password authenticated access on POP and IMAP services.
		5.7.7.3	Be able to set up cryptographic certificate authenticated access on POP and IMAP services.
		5.7.7.4	Know how to setup SASL-based SMTP authentication
		5.7.7.5	Be able to set up cryptographic tunnel access on POP and IMAP services.
		5.7.7.6	Know SPAM and how to control it
	5.7.8 Firewalls	5.7.8.1	Know what a firewall is, its limits and potentials, different firewall architectures (gateways, circuits etc)
		5.7.8.2	Be aware of term DeMilitarized Zone.
		5.7.8.3	Know what is a proxy and how it works

Category	Knowledge Area	Ref.	Knowledge Item
		5.7.8.4	Be aware of usage of a proxy to both save IP addresses and secure internal network.
		5.7.8.5	Know what Network/Port Address Translation (NAT) is and how it affects security
		5.7.8.6	Know IP firewall principles in restricting IP services access.
		5.7.8.7	Know proxy firewall principles in restricting and securing protocol handling.
		5.7.8.8	Be able to install a firewall and a proxy server and implement a security policy.
		5.7.8.9	Be able to hide IP-addresses using a firewall.
		5.7.8.10	Be able to set up NAT on a firewall.
		5.7.8.11	Be able to set up access control rules on a firewall.
	5.7.9 Intrusion Detection	5.7.9.1	Know basic categories of intrusion detection systems.
		5.7.9.2	Know how to monitor security logs and events.
		5.7.9.3	Be aware of Intrusion Prevention Systems
		5.7.9.4	Be able to deploy and basically configure an Intrusion Detection System
	5.7.10 Virtual Private Networks	5.7.10.1	Know IPSEC/IKE protocols
		5.7.10.2	Know about circuit-based (MPLS) VPNs
		5.7.10.3	Know what security can be provided by different technologies
		5.7.10.4	Know about other encapsulating protocols (PPTP, IP over UDP...) and their usage
		5.7.10.5	Be able to install a VPN client
5.8 Social, Ethical and Legal Aspects of Computer Security	5.8.1 Basic concepts	5.8.1.1	Know what is meant by the terms privacy, anonymity, pseudonymity .
	5.8.2 PETs	5.8.2.1	Know the balance between authentication and privacy
		5.8.2.2	Know privacy enhanced technologies (PETs) categories
		5.8.2.3	Know cookies and how to manage them.

Category	Knowledge Area	Ref.	Knowledge Item
		5.8.2.4	Know ethical issues (monitoring in the job, surveillance )
		5.8.2.5	Know basic deontology codes and code of Ethics (case studies: ACM, BCS, IEEE, etc)
		5.8.2.6	Know basic aspects of hacker ethics
		5.8.2.7	Know basic forms of computer crime
		5.8.2.8	Know basic mailing-lists and URLs concerning all above security areas.
		5.8.2.9	Be aware of ethical and privacy aspects of biometrics
	5.8.3 European laws	5.8.3.1	Be aware of the legal aspects of digital signature, also with respect to European Community rules.
		5.8.3.2	Know Data Protection Legislation (European 95/46 Directive) and what it implies in personal data processing.
		5.8.3.3	Be aware of general and legal aspects regarding evidences and computer forensics