EUCIP
European Certification of Informatics Professionals

EUCIP IT Administrator - Module 4
IT Security

Syllabus Version 3.0

Disclaimer
Although every care has been taken by ECDL Foundation in the preparation of this publication, no warranty is given by ECDL Foundation, as publisher, as to the completeness of the information contained within it and neither shall ECDL Foundation be responsible or liable for any errors, omissions, inaccuracies, loss or damage whatsoever arising by virtue of such information or any instructions or advice contained within this publication. Changes may be made by ECDL Foundation at its own discretion and at any time without notice.

The official version of *EUCIP IT Administrator - Module 4 - IT Security* is the version published on the EUCIP website: www.eucip.org

EUCIP
European Certification of Informatics Professionals

EUCIP IT Administrator – IT Security

This document details the syllabus for *EUCIP IT Administrator – IT Security*. The syllabus describes, through learning outcomes, the knowledge and skills that a candidate for *EUCIP IT Administrator – IT Security* should possess. The syllabus also provides the basis for the theory and practice-based test in this module.

Module Goals

EUCIP IT Administrator – IT Security requires the candidate to understand key principles of IT security and implement associated IT security measures for a network.

The candidate shall be able to:

- Recognise the main risk and security management principles and be aware of related standards.
- Recognise common encryption methods and be able to apply related cryptography protocols.
- Understand the key authentication and access control principles.
- Know about availability concepts relating to resilience and know how to implement backup procedures.
- Understand the main malicious code types and threats and be able to protect a system from attack.
- Know about public key infrastructure and apply related principles.
- Understand the key aspects of network security and be able to use firewalls, access controls and log management.
- Know about the main social, ethical and legal aspects of computer security.

CATEGORY	SKILL SET	REF.	TASK ITEM
4.1 Security Management	*4.1.1 Basic Concepts*	4.1.1.1	Describe the main aspects of information security: confidentiality, integrity, availability.
		4.1.1.2	Define the terms authentication, and non-repudiation.
	4.1.2 Risk Management	4.1.2.1	Recognise the main issues involved in risk assessment like: value of information, vulnerability, threat, hazard, violation, impact, level of risk.
		4.1.2.2	Outline the relationship between business processes/objectives and IT risk management, and the role of IT security in risk mitigation.
		4.1.2.3	Outline the most common high-level security functionalities like: identification and authentication, access control, accountability, audit, object reuse, accuracy, reliability of service, secure data exchange.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.1.2.4	Distinguish between functionality and assurance, and recognise the importance of achieving both to control IT security risk.
	4.1.3 Information Security Management	4.1.3.1	Describe the role of a security policy in driving the management of IT security.
		4.1.3.2	Recognise key processes to implement in an organisation to enhance information security like: ISO/IEC 17799, BS 7799.
		4.1.3.3	Understand the need for disaster recovery and business continuity plans in an organisation.
		4.1.3.4	Outline the key responsibilities of staff in an organisation like: security officers, system administrators, everyday users.
		4.1.3.5	Understand how to participate in a Computer Security Incident Response Team (CSIRT).
	4.1.4 Standards and Standardisation Bodies	4.1.4.1	Recognise the main standardisation bodies and understand their role.
		4.1.4.2	Recognise methodologies to assess different levels of assurance (ITSEC, ISO/IEC 15408 - Common Criteria).
		4.1.4.3	Outline the key elements of published standards aimed at security management infrastructure in an organisation like: ISO/IEC 17799, BS 7799 part 2.
4.2 Cryptography	*4.2.1 General*	4.2.1.1	Recognise basic concepts of cryptography like: cleartext, cyphertext, cryptographic algorithms.
	4.2.2 Symmetric Encryption	4.2.2.1	Recognise key principles of symmetric encryption like: common secret key, algorithms.
		4.2.2.2	Distinguish between the main symmetric encryption standards like: DES, 3DES, AES.
	4.2.3 Asymmetric Encryption	4.2.3.1	Outline the key principles of asymmetric encryption.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.2.3.2	Recognise the main public-key standards like: Public Key Cryptography Standard (PKCS) #1, PKCS #7.
	4.2.4 Hash and Digest Functions	4.2.4.1	Outline the key principles of hash and digest functions.
		4.2.4.2	Recognise the main hashing functions standards like: MD5, SHA1.
	4.2.5 Encryption method Comparisons	4.2.5.1	List the advantages and disadvantages of symmetric and asymmetric encryption.
		4.2.5.2	Understand the strength of different encryption methods like: asymmetric, symmetric. Be aware of the concept of keyspace.
		4.2.5.3	Understand the key distribution problems in symmetric and asymmetric cryptography.
		4.2.5.4	Describe the role played by Kerckhoffs's principle and open source in enforcing cryptography availability and robustness.
	4.2.6 Usage	4.2.6.1	Outline the use of encryption mechanisms like digital signatures to achieve authenticity.
		4.2.6.2	Distinguish between the security of an algorithm and the security of a cryptographic protocol.
		4.2.6.3	Outline the use of hashing and digest to enforce integrity and authentication.
		4.2.6.4	Describe how an electronic signature enforces non-repudiation and authentication.
		4.2.6.5	Understand the key principles and characteristics of encryption for enforcing confidentiality.
	4.2.7 Applications	4.2.7.1	Describe how cryptography is used to protect data in on-line transactions.
		4.2.7.2	Install and setup software to manage the PGP protocol.
		4.2.7.3	Understand the main principles of SSH.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.2.7.4	Install and setup software to manage the SSH protocol.
		4.2.7.5	Understand the main principles of S/MIME.
		4.2.7.6	Understand the main principles of TLS/SSL.
		4.2.7.7	Understand how smartcards are used.
4.3 Authentication and Access Control	*4.3.1 Authentication Concepts*	4.3.1.1	Describe different authentication schemes like: PAP, CHAP, Kerberos.
		4.3.1.2	Recognise the key principles of password management like: complexity, storage, periodical changes.
		4.3.1.3	Describe the key workings of token authentication.
		4.3.1.4	Recognise different biometric authentication schemes like: fingers, iris scanning, voice recognition.
	4.3.2 Network Authentication	4.3.2.1	Identify the different requirements for network and host authentication.
		4.3.2.2	Identify different Wi-Fi authentication schemes like: WEP, WPA and their limits.
		4.3.2.3	Identify different network protocols for distributed process authentication like: Kerberos.
		4.3.2.4	Outline the complexity of single sign-on architectures.
		4.3.2.5	Outline the main working principles of Kerberos like: ticket exchange.
		4.3.2.6	Describe Web services-security, XML-Encryption and XML-Signature.
	4.3.3 Access Control	4.3.3.1	Recognise the main approaches in access control: MAC, DAC, RBAC.
		4.3.3.2	Outline what an Access Control List and a list of capabilities are.
		4.3.3.3	Describe how to manage access control in common file systems.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.3.3.4	Describe how to manage access control in a Relational Database Management System (RDBMS).
4.4 Availability	*4.4.1 Availability Concepts*	4.4.1.1	Recognise different types of information availability requirements.
		4.4.1.2	List different kinds of infrastructure requirements needed for ICT like: UPS, air-conditioning, cabling.
	4.4.2 Resilience	4.4.2.1	Recognise different kinds of hard disk real-time replica mechanisms like: RAID.
		4.4.2.2	Outline different kinds of host replication and load distribution mechanisms.
		4.4.2.3	Recognise different kinds of network availability infrastructures for LAN, WAN, WLAN.
	4.4.3 Backup	4.4.3.1	Implement effective local and network back-up procedures.
		4.4.3.2	Test a backup and implement a recovery.
4.5 Malicious Code	*4.5.1 Programs*	4.5.1.1	Recognise what can command a computer: operating system, programs, shells, macros.
		4.5.1.2	Describe input validation requirements for security.
		4.5.1.3	Recognise different kinds of overflows and outline how they can be used to execute code.
		4.5.1.4	Describe the different kinds of attacks in browser/webserver interaction like: cross site scripting.
		4.5.1.5	Describe Denial of Service and how it can affect different environments and resources.
		4.5.1.6	Describe potential ways a computer can be attacked like: CD-Rom, emails, web browsing, chat clients.
		4.5.1.7	Recognise good practice in Internet access.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.5.1.8	Outline the risks of adware and spyware.
	4.5.2 Automatic File Type Management	4.5.2.1	Describe how a GUI recognises an action to be performed on an attachment using MIME type and extension.
		4.5.2.2	Describe how mail client programs recognise an action to be performed on an attachment using MIME type and extension.
	4.5.3 Downloadable Code	4.5.3.1	Describe how MIME types can be used maliciously and how to defend a PC from them.
		4.5.3.2	Outline how macros can be used maliciously and how to defend a PC from them.
		4.5.3.3	Outline how applets can be used maliciously and how to defend a PC from them.
	4.5.4 Viral Software	4.5.4.1	Recognise the main types of viral software like: trojan, virus, worms.
		4.5.4.2	Understand how an anti-virus program works.
		4.5.4.3	Outline the different tools that can be used for anti-malware protection: antispyware, personal firewalls.
		4.5.4.4	Understand the purpose and limitations of anti-virus programs.
		4.5.4.5	Install, setup and update an anti-malware program.
4.6 Public Key Infrastructure	*4.6.1 Using PKI*	4.6.1.1	Recognise public-key distribution problems like: owner identification issue.
		4.6.1.2	Understand the purpose of Certificates and Certificate Revocation Lists (CRL).
		4.6.1.3	Describe X.509.V3 Certificates.
		4.6.1.4	Understand public key infrastructure (PKI) and its principal components: Registration Authority and Certification Authority.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.6.1.5	Use a browser to generate keys and certification requests to a certification authority.
		4.6.1.6	Import and export a certificate into a browser.
		4.6.1.7	Access a CRL and import it into a browser.
		4.6.1.8	Use Online Certificate Status Protocol (OCSP).
		4.6.1.9	Recognise the different tolls and warning offered by browsers in order to alert the user on certificate validity status.
	4.6.2 Directory Services	4.6.2.1	Recognise the Lightweight Directory Access Protocol.
		4.6.2.2	Use a browser to query an LDAP server to obtain data belonging to a particular Distinguished Name.
		4.6.2.3	Define Common Name, Distinguished Name, and Attribute.
		4.6.2.4	Describe the X.509 standard in terms of Certification Authority, certificate structure, and certificate extensions.
		4.6.2.5	Outline how LDAP servers can be used to support user profile management and authentication.
4.7 Network Security	*4.7.1 Telecommunication Concepts*	4.7.1.1	Understand how Ethernet works in terms of MAC address, CSMA/CD.
		4.7.1.2	Understand the main aspects of TCP/IP: addresses, port numbers, main flow of operations.
		4.7.1.3	Describe TCP/IP encapsulation in Ethernet.
		4.7.1.4	Describe network services in the TCP/IP environment.
		4.7.1.5	Install and operate a network analyser.
		4.7.1.6	Describe the main types of TCP/IP stack attacks: sniffing, spoofing, rerouting, connection hijacking, (distributed) denial of service.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.7.1.7	Outline what switches and VLANs can provide to LAN security.
	4.7.2 Wireless Networks	4.7.2.1	Recognise the main wireless technologies like: WiFi, Bluetooth, Home Wireless.
		4.7.2.2	Describe the security risks related to wireless networks and the available solutions.
	4.7.3 Services	4.7.3.1	Describe services as access points of servers.
		4.7.3.2	Recognise malicious usage like: abusive usage, denial of service, data falsification.
		4.7.3.3	Outline the risks of DNS misuse.
		4.7.3.4	Describe common authentication schemes and their vulnerability.
		4.7.3.5	Outline how servers can be exploited due to protocols or software weaknesses.
		4.7.3.6	Understand that clients can be as vulnerable as servers.
		4.7.3.7	Outline the risks of peer-to-peer technologies and programs.
	4.7.4 Access Control	4.7.4.1	Describe how network authentication works and how to manage it.
		4.7.4.2	Describe cryptographic key based network authentication and how to manage it.
		4.7.4.3	Describe domain-based authentication in systems like Windows.
	4.7.5 Log Management	4.7.5.1	Recognise relevant security information that can be found in system log files.
		4.7.5.2	Setup logging in applications.
		4.7.5.3	Setup a centralised log service.
		4.7.5.4	Outline how to protect logs from tampering.

CATEGORY	SKILL SET	REF.	TASK ITEM
	4.7.6 HTTP Services Access Control	4.7.6.1	Distinguish between http and https based web sites.
		4.7.6.2	Understand how interaction between the web service and other system components can affect security.
		4.7.6.3	Implement a secure version of a non-secure web site, generating keys and certification requests, and inserting keys and certificates.
		4.7.6.4	Configure a web site to use plain text passwords to manage client identification and authorisation.
		4.7.6.5	Configure a web site to use certificates to manage client identification and authorisation like: SSL V.3.
		4.7.6.6	Recognise what kinds of access on a directory's objects can be restricted in web sites.
		4.7.6.7	Apply correct access restrictions on a given web site directory.
	4.7.7 Email Services Access Control	4.7.7.1	Understand that an e-mail source address and associated information can be forged.
		4.7.7.2	Set up plain password authenticated access on POP and IMAP services.
		4.7.7.3	Set up cryptographic certificate authenticated access on POP and IMAP services.
		4.7.7.4	Setup SASL-based SMTP authentication.
		4.7.7.5	Set up cryptographic tunnel access on POP and IMAP services.
		4.7.7.6	Define the term spam. Outline methods to control spam.
	4.7.8 Firewalls	4.7.8.1	Define the term firewall. Outline the limits and potential of a firewall and recognise different firewall architectures like: gateways, circuits.
		4.7.8.2	Define the term demilitarized zone (DMZ).

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.7.8.3	Describe what a proxy is and how it works.
		4.7.8.4	Understand how to use a proxy to save IP addresses and secure internal network.
		4.7.8.5	Describe what Network/Port Address Translation (NAT) is and how it affects security.
		4.7.8.6	Understand IP firewall principles for restricting IP services access.
		4.7.8.7	Understand proxy firewall principles for restricting and securing protocol handling.
		4.7.8.8	Install a firewall and a proxy server and implement a security policy.
		4.7.8.9	Hide IP-addresses using a firewall.
		4.7.8.10	Set up NAT on a firewall.
		4.7.8.11	Set up access control rules on a firewall.
	4.7.9 Intrusion Detection	4.7.9.1	Recognise basic categories of intrusion detection systems like: network IDS, host-based IDS.
		4.7.9.2	Monitor security logs and events.
		4.7.9.3	Recognise Intrusion Prevention Systems like: network-based IPS, wireless IPS, host-based IPS.
		4.7.9.4	Deploy and basically configure an Intrusion Detection System.
	4.7.10 Virtual Private Networks	4.7.10.1	Outline the principles of IPSEC/IKE protocols.
		4.7.10.2	Outline the security properties of circuit-based (MPLS) traffic separation.
		4.7.10.3	Describe what security can be provided by different technologies like: SSL, IPSEC.
		4.7.10.4	Install a VPN client.

CATEGORY	SKILL SET	REF.	TASK ITEM
4.8 Social, Ethical and Legal Aspects of Computer Security	*4.8.1 Basic Concepts*	4.8.1.1	Define the terms privacy, anonymity, pseudonymity.
	4.8.2 Privacy Enhancement Technologies	4.8.2.1	Recognise the balance between authentication and privacy.
		4.8.2.2	Understand ethical issues associated with monitoring in the job, surveillance.
		4.8.2.3	Outline basic deontology codes and code of ethics.
		4.8.2.4	Outline the basic aspects of hacker ethics.
		4.8.2.5	Recognise basic forms of computer crime like: cracking, identity theft, data theft, fraudulent access.
		4.8.2.6	Understand ethical and privacy issues relating to biometrics.
	4.8.3 European Laws	4.8.3.1	Outline the legal aspects of digital signature and the Community framework for electronic signatures.
		4.8.3.2	Recognise Data Protection Legislation (European 95/46 Directive) and understand the associated implications for personal data processing.
		4.8.3.3	Recognise the main considerations regarding computer forensics and computer evidence.