

TM



EUCIP

European Certification of
Informatics Professionals

EUCIP Security Adviser

Elective Level Profile Specification

Version 2.4, February 2007

Short Description

A EUCIP Security Adviser is expected to be very effective in identifying security requirements for ICT systems and defining reliable and manageable solutions. A wide and thorough ICT competence has to be combined with the ability to interact with other ICT functions to foster the integration of security technologies within the ICT infrastructure.

This profile requires a minimum work experience of **36** months in a compatible job role; if this requirement is not fulfilled, the candidate might be certified as an **Associate** Security Adviser.

Tasks Overview

Takes care of the security requirements, managing the provision of agreed security level and identifying suitable solutions to be integrated into the organization IT infrastructure.

Collaborates with network management and application/service functions (particularly to not impair network performance, achieve application needs).

Identifies potential security exposures of all components of systems and defines prioritised actions to address the potential exposures to a level approved by the organisation's senior management.

Assists in defining, planning and justifying (in business terms) projects aimed to achieve an agreed level of security according to previously identified threats and business constraints.

Prepares, or contributes to risk analyses and risk mitigation.

Participate as a project member in the design, development and test phases of projects, like new applications or networks, which exhibit security requirements, taking account of the requirements for security versus the constraints of system performance, functionality and cost.

Reviews security technology and operation costs against external managed security providers. Evaluates the need of new developments and new technologies. Obtains and evaluates proposals from suppliers of equipment, software, and other security technology and service providers.

Analyses organization's data and resources and support system administrators and project managers in defining appropriate access control policies according to security requirements and service functionality.

Takes responsibility for planning, managing, and enforcing organizational security policies and access control including privacy rules for protecting sensible data.

Takes responsibility for deploying and updating security technologies for all organization's assets, like network devices, application servers, database servers, backup servers/technology, workstations, and mobile devices. Responsibilities are extended to all communication means, like Internet connections, wireless connections, dial-up connections and intranet connections.

Takes responsibility of efficient security patch management and testing to keep systems update without incurring in negative side effects due to incorrect patches.

Takes responsibilities of the security architecture possibly composed by several network components and appliances, distributed systems and dedicated networks.

Uses monitoring and log analyses tools to prevent security incidents and to identify possible weaknesses in the security management. Creates reports for showing the actual degree of security and submit proposals for improvement.

Uses incident response techniques to diagnose, contain and solve security incidents and to determine the consequences in terms of compromised hosts, network failures and downtime. Creates reports with detailed analysis of every incident.

Maintain awareness of relevant security trends and security alarms and inform senior managers when immediate responses, with possible negative impact of business operations, must be taken.

Maintains awareness of the implication of relevant legislation or other external regulations which affect security within any defined scope and activity.

Essential Behavioural Skills [3]¹

The Security Advisor role requires flexibility and a rational mental attitude capable of conceptual and analytical thinking, in particular under stressful conditions.

Attention to the client, interaction, ability to collect information, plus keen organisational sensitivity are required to understand the client's needs.

Strategic vision, ability to mediate between conflicting requirements (business vs. security) and an analytical mindset able to focus on most effective ways to achieve a preset risk reduction are required for a successful security management.

Another essential set of skills is the ability to communicate and interact effectively (in both oral and written form) with colleagues from network management and from application development/management.

¹ numbers in brackets represent EUCIP points

Detailed Skills Required

Deep competence level [22]

A7.06 Access-control policies, models and mechanisms [2]

- Definition of security models and mechanisms:
 - o Discretionary (DAC)
 - o Mandatory (MAC)
 - o Role-based (RBAC)
- Describe basic concepts of discretionary policies:
 - o Access matrix model
 - o Implementation of the access matrix
- Explain vulnerabilities of the discretionary policies
- Describe basic concepts of mandatory policies:
 - o Security classifications
 - o Secrecy-based policies
 - o The Bell-LaPadula model
 - o The Biba model
- Explain application of mandatory policies to databases.
- Explain limitations of mandatory policies.
- Explain integration of DAC and mandatory restrictions:
 - o The Chinese Wall policy
 - o Authorisation-based information flow policies
- Understand advanced concepts of discretionary policies:
 - o Closed and Open policies
 - o Temporal authorisations
 - o Administrative policies
 - o Integrity policies
- Describe basic concepts of role-based policies:
 - o Authorisation management
 - o Hierarchical roles
 - o Least privilege principle
 - o Separation of duties
- Design and apply a vulnerability assessment test focusing on access-control.

C4.06 Network attack prevention [2,5]

- Understand the phases of a network attack.
- Explain the reconnaissance phase according to:
 - o Social engineering risks and techniques
 - o Available information on the Web
 - o Reconnaissance tools
- Explain the scanning phase carried out by:
 - o Tools and techniques for network mapping
 - o Port scanning and OS fingerprinting
 - o Vulnerability scanners
- Explain the intrusion phase in following areas:
 - o Gain access using application and operating system attacks
 - o Automatic tools and script kiddies
 - o Vulnerable services
 - o Password attacks
 - o Web application attacks

- Client software attacks
- Distinguish attacks to services availability considering:
 - Basic denial-of-service techniques
 - Distributed denial-of-services
- Recognize techniques to maintain illegal accesses
 - Identify backdoors
 - Recognize trojan horses
 - Remove spyware
- Explain methods to cover tracks of an intrusion in the following areas:
 - Event logs alteration
 - Accounts modifications
 - Covert channels
 - Prevention techniques and tools
- Describe principles of intrusion detection and prevention covering following topics:
 - Misuse and anomaly detection
 - Incidence of false positive and false negative
 - Network-based and host-based intrusion detection
 - Signature-based NIDS
 - Protocol-decoding techniques
 - Deep-packet inspection
 - Active responses
 - Intrusion prevention systems
- Design and apply a vulnerability assessment test focusing on wired networks.

C5.02 **Wireless security [2]**

- Understand fundamentals of wireless security:
 - Wireless networks threats
 - Security standards in wireless networks
- Understand fundamentals of wireless local area networks (WLAN)
 - IEEE 802.11 standards
 - Threats to WLANs
- Define basic security solutions for Wi-Fi
 - Design principles for Wi-Fi architectures
 - Characteristics of the Wireless Encryption Protocol (WEP)
 - Vulnerability of WEP
- Understand advanced Wi-Fi security technologies:
 - WPA
 - RSN
 - IEEE 802.11i
 - TKIP
- Describe access control technologies for WLAN:
 - IEEE 802.1X
 - EAP
 - RADIUS
- Understand fundamentals of mobile phone security, in particular Bluetooth vulnerabilities
- Design and apply a vulnerability assessment test focusing on wireless networks.

B2.13 Database security [3]

- Explain the differences between object-based logical model, record-based logical model and physical data model.
- Define entities and entity keys.
- Distinguish database objects like constraints, indexes, stored procedures, tables, triggers, user-defined functions, and views.
- Use SQL for producing queries and manipulating data.
- Distinguish:
 - o distributed data storage and networking
 - o basic DBMS architecture
 - o the role of DBMS in distributed systems
 - o the role of DBMS in multi-tiers Web applications
- Explain the role of databases for backups.
- Define object-level security including column-level permissions.
- Evaluate the importance of preventing unauthorized access to business-critical data.
- Analyse risks by probability and severity and identify adequate countermeasures.
- Design procedures for obtaining, using and storing sensitive personal data in compliance with specific requirements, such as
 - o information on why, how and by whom the data are used
 - o right to access personal records and to have them deleted
 - o anonymity and secrecy
- Propose effective ways to train employees about processes, and responsibilities (both organisational and personal).
- Analyse storage solutions and business practices in terms of security and appropriate availability.
- Know how to avoid SQL Injection
- Design and apply a vulnerability assessment test focusing on databases.

C2.05 Operating Systems security [2]

- Explain permissions management in Linux/Unix and Windows.
- Describe hardening procedures in Linux/Unix and Windows
 - o Secure configuration of available services
 - o Explain differences between static kernel modules and dynamically loaded modules
 - o Constrain a process run-time environment
 - o Configure processes with least privilege
 - o Vulnerability assessment
- Describe tools and techniques for file system integrity
- Understand patch management
 - o Set up a test environment for compatibility checks
 - o Analyze the characteristics of automatic patch management tools
 - o Understand time issues regarding patches
- Describe memory management security vulnerability
 - o Buffer overflow concepts
 - o Types of buffer overflow: stack, heap and string overflows
 - o Describe prevention techniques and tools
- Explain risks from rootkits: kernel and application rootkits

- Design and apply a vulnerability assessment test focusing on operating systems.

C4. 07 Web application security [2,5]

- Understand fundamentals of client-side application security:
 - o Application attack points
 - o Client identification and authentication
 - o User permissions
 - o Functional and data restrictions
- Explain HTTP security threats:
 - o HTTP header analysis
 - o HTTP header expiration
- Understand client-side application code:
 - o Session IDs
 - o Navigational tools
 - o Client-side data.
 - o Cookies
 - o Hidden fields
 - o URL
 - o Local data files
 - o Windows registry
- Describe technology for secure client transmissions:
 - o Encryption techniques and digital certificates.
 - o Mobile application code, ActiveX controls and Java Applets
- Analyse Internet browser vulnerabilities and security settings.
- Understand fundamentals of server-side application security:
 - o Common Gateway Interface (CGI)
 - o Permissions and directories
 - o Third-party CGI scripts
 - o Server Side Includes (SSIs)
 - o Dynamic code
- Explain management techniques for input data:
 - o Invalid data types
 - o Invalid ranges
 - o Escape characters
- Understand server-side data:
 - o Data filenames
 - o Data integrity
 - o Data vaults.
 - o Data encryption.
- Explain fundamentals of single-sign-on (SSO)

B3. 06 Secure programming [2]

- Understand and apply the principles of secure coding:
 - o Appropriate access control
 - o Least privilege concept
 - o Validation and control of input data
 - o Buffer overflow concept
- Understand secure programming issues:
 - o Socket security
 - o RPC and DCOM security
 - o Java applet and ActiveX control security

- EJB and RMI
- Minimise, isolate and simplify code running with raised privileges.
- Cope with main security issues related to code and data structures.
- Distrust all values external to the program (e.g. arguments, environment variables, etc.).
- Avoid use of any function that copies without checking buffer lengths.
- Avoid link with dynamic libraries, link statically.
- Avoid creation of temporary files in world-writable directories (e.g. /tmp).
- Recognise race conditions.
- Design the security infrastructure. Design the deployment architecture: considerations include security, performance, maintainability, extensibility, availability, scalability, and reliability.
- Monitor performance counters and event logs.
- Understand fundamentals of static analysis of source code.
- Define security code review processes.
- Define secure software deployment procedures.

A2.05 **Business continuity planning [2]**

- Understand the dependence of business continuity on the IT infrastructure
- Define the main causes of downtimes
- Analyze the cost of downtime:
 - Tangible costs
 - Intangible costs
- Understand business continuity management planning:
 - Analyze the company's business
 - Perform a business impact analysis
- Explain risk management phases:
 - Risk analysis
 - Risk mitigation
 - Risk transfer
- Understand fundamentals of backup, recovery and continuous data protection:
 - Basic technology for backup and recovery
 - Alternate sites strategy
 - Trade-offs in the off-site location choice
 - Disaster recovery procedures and costs.
- Understand backup and recovery for web-based hosting services.
- Explain storage technologies for data backup and recovery:
 - Well-established technologies
 - Remote mirroring
 - Disk-to-disk backup
 - Storage area networking (SAN)
 - SAN security issues
 - Internet SCSI
- Understand the importance of training and testing:
 - Implementation of business continuity training process
 - Testing processes and procedures for day-to-day operations
 - Testing processes and procedures for disaster recovery

- Keep up-to-date information on fundamentals of business continuity laws and regulations.
- Analyze fundamentals of investment decisions in business continuity.

A7.07 Risk analysis and management [2]

- Distinguish available guidance.
- Explain principles of Enterprise/Operational Risk management.
- Understand IT insurance risk.
- Explain risk identification.
- Explain risk assessment tools and techniques.
- Explain risk evaluation.
- Explain risk management.
- Distinguish risk classes:
 - o Application risks,
 - o Network risks,
 - o Communication risks,
 - o Distributed system risks,
 - o Data management risks,
 - o Physical risks.
- Evaluate the risk of intrusions and ethical issues:
 - o basic forms of computer crime
 - o basic categories of intrusion detection systems
 - o ethical issues (monitoring in the job, surveillance)
 - o basic deontology codes and code of Ethics (case studies: ACM, BCS, IEEE, etc)
 - o basic aspects of hacker ethics
 - o basic mailing-lists and URLs concerning all above security areas
 - o ISO17799 standard, its purposes and its implementation process

A3.05 IT security economics and business strategies [2]

- Specify the business need for recovery and back-up of data and for protection against viruses.
- Evaluate the need for encryption of data (at rest/in transit) in the light of network “threats” to data integrity.
- Evaluate the risks to the business caused by security threats to IS/IT.
- Contribute to a Security policy for (part of) a business organisation.
- Explain the principal concepts of the laws in force in the own country and compare them with European recommendations and different jurisdictions.
- Analyse issues related to data protection, personal rights regarding privacy and free access to information held by public authorities.
- Determine which rights, restrictions and obligations apply in a given real case, and what they mean to the organisation.
- Define a robust organisational approach to cope with such regulations and business priorities.

Incisive competence level [7]

A7.09 IS audit process [1]

- Describe the IS audit process:
 - o Distinguish accepted auditing standards
 - o Audit planning and chartering
 - o Complete the preliminary review
 - o Prepare an audit plan
 - o Identify audit tools and techniques
 - o Produce an audit report and follow-up
 - o Post-audit actions
- Evaluate and select between different audit techniques
- Use of Computer-assisted audit tools and techniques
- Define a plan and related organizational aspects for auditing the various processes:
 - o Planning and analysis of new systems,
 - o IT strategies and standards,
 - o Planning and controlling,
 - o Process management,
 - o Quality management.

A2.06 Key IT process control [1]

- Conduct IT acquisition and implementation audit:
 - o Audit of software acquisition procedures
 - o Audit of systems implementation
- Conduct change and configuration management audit:
 - o Verify vulnerabilities in software development
 - o Explain software configuration management
 - o Understand impact assessment
 - o Explain revisions to documentation and procedures
 - o Define software release and distribution policies
 - o Explain organizational change management.

C3.04 IP communications [1,5]

- Explain the characteristics of Internet Protocol (IP) and other protocols:
 - o ICMP
 - o DHCP
 - o ARP
 - o the IP addressing scheme
 - o the relationship between IP addresses and network classes
- Apply subnetting and CIDR concepts.
- Distinguish logical from physical addresses.
- Evaluate the functions of a router, and those of a layer-3 switch.
- Differentiate between a generic port and a well-known-port.
- Explain the purposes and characteristics of TCP and UDP protocols:
 - o TCP main mechanisms (PAR, flow control, multiplexing, urgent data signalling, etc.)
 - o TCP session opening and closing
 - o features of UDP protocol
 - o differences between TCP and UDP

- Differentiate between PPP and SLIP.
- Explain the purposes and operations of
 - o Network Address Translation (NAT)
 - o (address) proxy
 - o a firewall and its functions
 - o Domain Name System (DNS)
 - o naming of Internet hosts
 - o resource descriptor
- Outline how a Domain Name is translated into an IP address.
- Differentiate between the purpose and the working principles of TELNET and FTP protocol.
- Use an FTP program for simple file transfers (connect as normal user or guest, change and list directories on local and remote computer, set passive mode; send / receive one or multiple files using binary and/or ASCII transfer).
- Obtain IP base parameters: IP number, IP Mask, Default gateway, DNS server(s).
- Configure IP base parameters on different platforms (Windows, Apple, Linux), such as IP address, WINS, Gateway and DNS.
- Install, configure and remove network services on a server.

C2.01 Operating Systems [2]

- Differentiate between the most widespread operating systems:
 - o Linux/Unix
 - o Windows
 - o MacOS
- Install and upgrade the above OSs.
- Cope with OS conceptual problems:
 - o concurrency management, deadlock and starvation
 - o scheduling
 - o I/O operation and management
 - o file management systems
 - o user and access management
- Analyse network capabilities.
- Configure network interfaces.
- Configure various network protocols and services (including http, SMTP, POP, IMAP, DNS).
- Start and stop various network services.
- Publish resources on the network (e.g. shared printers and folders).
- Measure and monitor system load:
 - o CPU (both mono- and multi-processor)
 - o network
 - o memory and virtual memory
 - o storage
 - o processes and threads
 - o usage of shared resources
- Tune the system to reach required performances.
- Manage user accounts and groups and set up related security policies.
- Apply interoperability tips (file formats, available protocols, etc.).

- Set up systems to reach the needed level of interoperability between heterogeneous OSs.
- Use performance boosting techniques such as clustering.
- Set up clustering.
- Perform troubleshooting.
- Perform system recovery.

B4.06 Web-based applications [1,5]

- Explain the role of Web proxies.
- Distinguish MIME types.
- Explain the the aim of main markup languages (HTML, XML, CSS, XSL).
- Distinguish between application providing static contents and others producing dynamic content.
- Distinguish between different solutions providing status information, i.e. URL parameters, hidden tags and cookies.
- Understand the design of multi-tiered Web-based applications.
- Explain the role of active content, i.e. Java applets and ActiveX.
- Explain the role of Web Services and of the SOAP protocol.
- Understand the features of widespread programming languages and frameworks, i.e. PHP, Java Servlet/JSP, .NET C#.
- Understand main features of JavaScript and AJAX.

External references to SFIA[®] version 3 by the SFIA Foundation

Skill 23: Safety Engineering

“The application of appropriate methods to assure safety during all lifecycle phases of safety-related system developments, including maintenance and reuse. These include safety hazard and risk analysis, safety requirements specification, safety-related system architectural design, formal method design, safety validation and verification and safety case preparation.”

Levels 4 and 5

Skill 46: Security Administration

“The authorisation and monitoring of access to IT facilities or infrastructure in accordance with established organisational policy. Includes the investigation of unauthorised access, compliance with data protection and performance of other administrative duties relating to security management.”

Levels 4 and 5

Skill 50: Data Protection

“The development and implementation of policies, procedures, working practices and training to comply with the requirements of legislation regulating the holding, use and disclosure of personal information such as, in the UK, the Data Protection Act, Computer Misuse Act, Freedom of Information Act.”

Level 5

Skill 65: Safety Assessment

“The assessment of safety-related software systems to determine compliance with standards and required levels of safety integrity. This involves making professional judgements on software engineering approaches, including the suitability of design, testing, and validation and verification methods, as well as the identification and evaluation of risks and the means by which they can be reduced. The establishment, maintenance and management of an assessment framework and practices may also be included.”

Level 5

External references to AITTS by the German Government – *Arbeitsprozessorientierten Weiterbildung in der IT-Branche*

Profil 3.5 : IT Security Coordinator (IT-Sicherheitskoordinator/in)
*“IT Security Coodinator konzipieren angemessene IT Sicherheitslösungen
entsprechend geltender technischer Standards, Gesetze und Vorschriften, begleiten
deren Umsetzung und passen sie laufend den aktuellen Gegebenheiten an.”*

External references to Nomenclature 2005 by CIGREF (club informatique des grandes entreprises françaises)

Métier 5.3 : Expert méthode et outils / qualité / sécurité
*“Il assure un rôle de conseil, d’assistance, d’information, de formation et d’alerte. Il
peut intervenir directement sur tout ou partie d’un projet qui relève de son domaine
d’expertise.
Il effectue un travail de veille technologique sur son domaine et propose des
évolutions qu’il juge nécessaires.
Il est l’interface reconnue des experts externes.”*

**Métier 5.4b : Responsable sécurité des systèmes d’information
(RSSI)**
*“Sa mission première est de dèfinir la politique de sécurité du SI et de veiller ° son
application.
Le RSSI assure un rôle de conseil, d’assistance, d’information, de formation et
d’alerte. Il peut intervenir directement sur tout ou partie des syst\$èmes informatiques
et télécoms de son entité.
Il effectue un travail de veille technologique et réglementaire sur son domaine et
propose des évolutions qu’il juge nécessaires pour garantir la sécurité logique et
physique du système d’information dans son ensemble. Il est l’interface reconnu des
exploitants st des chefs de projet mail aussi des experts et des intevenants
extérieurs pour les problématiques de sécurité de tout ou partie du SI.”*