

TM



EUCIP

European Certification of
Informatics Professionals

EUCIP Network Manager

Elective Level Profile Specification

Version 2.4, February 2007

Short Description

A EUCIP Network Manager is expected to be very effective in managing a networked information system of medium complexity, and improving its performances. Should also be proficient in interactions with network architects and possible external suppliers across all phases of a network's lifecycle.

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** Network Manager.

Tasks Overview

Takes care of the communication requirements, managing the provision of agreed quality of services and support, keeping in touch with client/user representatives to ensure that requirements (particularly network performance, recovery, and security needs) are reflected in the overall specifications. Identifies potential exposures of all components of network systems and defines prioritised actions to address the potential exposures to a level approved by the organisation's senior management.

Working alone on moderately complex network systems, or with consultants on larger or more complex networks, defines network design policies, philosophies and criteria, specifies user/system interfaces, documenting all work using required standards, methods and tools and plays a leading role in scheduling installation work, liaising with all concerned to ensure that installation priorities are met and disruption to the organisation is minimised.

Where service is provided by an external supplier, supports contract negotiation to provide the service level required, establishing problem resolution procedures and defining consequences of non-compliance. Interfaces with designers and planners from external suppliers and network service providers and works within the team which administers the procurement of equipment, software, transmission services, and other services for communication networks, including action on non-compliance.

Takes responsibility for installing and upgrading of local and wide area networks for the communication of data, voice, text or images carrying out routine configuration/installation and reconfiguration of hardware and software utilising the appropriate tools and test equipment.

Diagnoses and solves problems (e.g. poor performance) and faults (e.g. system failure) occurring in the operation of hardware and software, ensuring that account is taken of agreed levels of service and the needs for quality, security, availability and safety.

Uses network management system tools to investigate, diagnose and solve network problems and to determine network load and model performance statistics. Compares service levels achieved to agreed levels, creating reports and proposals for improvement.

Responds to enquiries by users, specialists or others and deals effectively with a broad range of problems of moderate complexity, ensuring that documentation of the supported systems and software is available and in an appropriate form. Maintains records to ensure that problems are managed in accordance with agreed standards and procedures.

Investigates and reconciles violation reports and loggings generated by automated policing mechanisms. Interviews offenders and compiles reports and recommendations for management follow-up. Provides advice and handles enquiries relating to security, contingency planning and activities of the function. Recognises requirements for, and creates, auditable records, user documentation and security awareness literature for all services and systems within IS Security Management, ensuring that the records provide a comprehensive history of violations, resolutions and corrective action. In touch with security consultants, devises and documents new

or revised procedures relating to security control of all network related environments, systems, products or services in order to demonstrate continual improvement in control.

Evaluates design enhancements, capacity changes, contingency and recovery arrangements as required and is aware of operational requirements especially in terms of service levels, network availability, response times, security and repair times. Reviews network costs against external service providers, new developments and new services, initiating proposals to change network design where appropriate cost reductions and benefits can be achieved. Obtains and evaluates proposals from suppliers of equipment, software, and other network service providers.

Maintains awareness of the main ICT infrastructure used in the employing organisation and takes care of the alignment of the network structure to business needs.

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

Essential Behavioural Skills [2]¹

The Network Manager role requires initiative, flexibility and a rational mental attitude capable of conceptual and analytical thinking, even under stressful conditions: a persistent goal-oriented approach in a strategic perspective has to be combined with strong attention to detail.

Another essential set of skills is the ability to communicate and interact effectively (in both oral and written form) with colleagues and clients: this shall include a high organisational and cross-functional awareness, leadership, efficiency in information acquisition, as much as the ability to plan, organise, make decisions, provide direction and follow-up.

Last but not least, the capacity to compare different technologies and products in respect to business needs is a must.

¹ numbers in brackets represent EUCIP points

Detailed Skills Required

Deep competence level [12]

C4.01 Network security [3]

- Explain what can be considered good practice in Internet access.
- Distinguish between basic categories of viral software (trojan, virus, worms, etc.).
- Install and operate a network analyser.
- Evaluate the risk of services as access points of servers.
- Set up the minimum and safest set of services that can be enabled on Internet servers.
- Disable the set of services that are usually enabled on non_internet servers only.
- Adopt countermeasures against the main types of wicked usage:
 - o abusive usage,
 - o denial of service,
 - o data falsification.
- Adopt countermeasures against the main points of vulnerability:
 - o usual authentication schemes,
 - o weakness of protocols or software on servers,
 - o clients that can be as vulnerable as servers.
- Know how to limit spoofing in its various flavours (IP, ARP, email,...).
- Recognise good practice in
 - o securing and using a non-internet server,
 - o securing and using an internet server.
- Manage network authentication.
- Manage cryptographic key-based network authentication.
- Use domain_based authentication.
- Evaluate a firewall, its limits and potentials, different firewall architectures (gateways, circuits etc.).
- Properly use the term “DeMilitarised Zone” and assist in its implementation.
- Evaluate a proxy and its functionality
 - o to save IP addresses,
 - o to secure internal network.
- Explain what a Network Address Translation (NAT) is and how it works.
- Apply IP firewall principles in restricting IP services access.
- Apply proxy firewall principles in restricting and securing protocol handling.
- Use network utilities to configure, manage and trace network usage.
- Know how to create and configure a local proxy.
- Install a firewall and a proxy server and implement a security policy.
- Hide IP-addresses using a firewall.
- Set up NAT on a firewall.
- Set up access control rules on a firewall.
- Evaluate the risk of intrusions and ethical issues:

- basic forms of computer crime,
- basic categories of intrusion detection systems,
- ethical issues (monitoring in the job, surveillance),
- basic deontology codes and code of Ethics (case studies: ACM, BCS, IEEE, etc),
- basic aspects of hacker ethics,
- basic mailing lists and URLs concerning all above security areas,
- ISO17799 standard, its purposes and its implementation process.
- Know how to monitor security logs and events.
- Know cookies and how to manage them (enable - disable cookies).
- Install and manage a cookie buster program.
- Comply with legal requirements such as the 2002/58/EC directive on privacy and electronic communication.

C3.02 Ethernet [1,5]

- Evaluate an Ethernet system:
 - Data transmission rates
 - Transmission media
 - Maximum lengths and nodes
 - Different types of Ethernet networks such as 10BASE-2, 10BASE-5, 10BASE-T
 - Related standards (such as IEEE 802.3)
- Explain the CSMA/CD operations.
- Explain level 2 operations, MAC address.
- Explain Broadcasting and unicasting.
- Connect a computer to a Ethernet segment.
- Connect in cascade hubs or switches using crossed ports, crossed cables or coax cables.
- Recognise the different Network adapter connectors, Coax/BNC, DIX/AUI/DB15, RJ45 etc. Also know their use.
- Install network card driver on different platforms (Windows, Apple, Linux).
- Know how to update NIC drivers.

C3.04 IP communications [2,5]

- Explain the characteristics of Internet Protocol (IP) and other protocols:
 - ICMP
 - DHCP
 - ARP
 - the IP addressing scheme
 - 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 UCP protocols:
 - TCP main mechanisms (PAR, flow control, multiplexing, urgent data signalling, etc.)

- TCP session opening and closing
- features of UDP protocol
- differences between TCP and UDP
- Differentiate between PPP and SLIP.
- Explain the purposes and operations of
 - Network Address Translation (NAT)
 - (address) proxy
 - a firewall and its functions
 - Domain Name System (DNS)
 - naming of Internet hosts
 - 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.

C5.01 Wireless networking protocols [1,5]

- Classify the transmission media and techniques for wireless LANs (infrared, spread spectrum, narrowband microwave) and their range of operation:
 - technologies used for wireless communications
 - major wireless standards
 - problems characterising wireless and mobile computing
 - limitations of the wireless technology
 - main components of a Wireless LAN
- Differentiate between 802.11 sub-protocols:
 - 802.11
 - 802.11b
 - 802.11a
 - 802.11g
- Explain the functions of the main wireless communication standard:
 - mobile IP
 - Wireless Application Protocol (WAP)
 - Bluetooth
 - range of applicability of each protocol
- Know how to implement interoperability tips in wireless broadband systems (WiFi standard, Bluetooth, 802.11).
- Know how to use security hints about 802.11 such as WEP40, WEP128.
- Explain European and national wireless LAN regulations (ETSI2).

C3.03 Apparatus and structured cabling [1]

- Describe structured cabling systems (behaviour, use and benefits).
- Describe structured cabling system components (plug, sockets, patch-cords, racks, etc.).
- Describe non-certificated add-ons for structured cabling systems.
- Illustrate the main network topologies (bus, star, ring, tree).
- Distinguish between types of network cables that can be used such as coaxial, twisted pair, fiber optic:
 - o their capabilities and limitations
 - o structured cabling regulations and warranties
- Differentiate between active components:
 - o a hub and a repeater
 - o a switch and a bridge
 - o a gateway
- Observe installation constraints: health, security, warranty, technical approval.

C6.02 Network troubleshooting [1,5]

- Diagnose the reason why a user cannot gain access to the network.
- Locate the source of the problem (server, cable, NIC, drivers, etc).
- Diagnose and troubleshoot user permissions.
- Diagnosing and troubleshoot local and domain user accounts, if any domain is available.
- Diagnose and repair communication problems, such as modem and internet communication problems.
- Troubleshoot problems with hardware.
- Diagnose printing problems.
- Diagnose hardware problems such as problems with the cable, NIC, etc.
- Use heartbeat and related loop led indicators.
- Diagnose and troubleshoot the TCP/IP protocol.
- Diagnose and troubleshoot performance problems.
- Use ICMP to test network.
- Use the "ping" command to test name lookup.
- Use "nslookup" or "dig" to test DNS operations.
- Use the "route" command to verify outgoing packets.
- Use the "tcpdump" to monitor packets.
- Use the "tracert" command to check how packets reach a given server.
- Use the "nslookup" MX query to discover mail servers.
- Use the telnet program to manually simulate SMTP simple session, verify existence of an account, and send an email.
- Use the Telnet program to simulate a POP3 / IMAP session and get a list of pending messages.
- Use the Telnet program to simulate a HTTP session and download a page to test server operations.
- Measure performance according to appropriate units of measure.
- Monitor the network to analyse traffic.
- Maintain statistical and historical traffic data.

A7.01 Health and safety [1]

- Apply the special H&S considerations pertinent to hardware.
- Plan actions to minimise or eliminate potential H&S hazards.
- Observe the main relevant EU and national H&S legislation and directives.

Incisive competence level [18]

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.

C3.01 Network principles and standards [1,5]

- Evaluate the basic components of a network, such as server, client, NIC, protocols, Network Operating System (NOS), shared resources.
- Evaluate a Server, its requirements, and function. Also evaluate the basic server components.
- Build or order a server, dimensioning it to cover the network needs.
- Evaluate a Client, its requirements, and function. Also evaluate the basic client components.
- Build or order a client, dimensioning it to covers both user's and applications' needs.
- Evaluate the function of a Network Interface Card (NIC). Also be able to choose the appropriate card for a network.
- Differentiate between the basic network topologies:
 - o Busnet,
 - o Ringnet,
 - o Starnet,
 - o their function, capabilities and limitations.
- Differentiate between a Local Area Network (LAN) and a Wide Area Network (WAN).
- Recognise "de facto" and "de jure" standards in data transmission:
 - o the TCP/IP suite,
 - o the OSI model,
 - o purpose of the layered reference model (principle of encapsulation and service access points in layer models),
 - o main standard organisations, such as CCITT, ITU-TS, IEEE, ISO and IAB and domains they are focusing on,
 - o aim of the different layers (physical, data link, network, transport, session, presentation, and application).

C3.06 Modem and modulations [1,5]

- Explain the main principles and standards in modulation:
 - o properties of analog and digital signals,
 - o the need for modulation,
 - o the function of a modem,
 - o DTE and DCE,
 - o three basic encoding techniques: ASK, FSK and PSK
 - o QPSK and QAM,
 - o the most common modem protocols such as XMODEM, YMODEM, ZMODEM, KERMIT etc.,
 - o the most common modem communications standards, such as V.90, V.42 etc.,
 - o how hardware (RTS/CTS) and software (XON/XOFF) flow control works,
 - o HAYES standard and its most common commands such as AT, ATZ, ATD, ATH etc.
- Distinguish between communication modes (simplex, half-duplex, full duplex).
- Distinguish between transmission types (asynchronous, synchronous, serial, parallel).
- Explain the following concepts and standard elements:
 - o start bit, stop bit, parity and data bit,

- SYNC, STX, ETX, ACK and NACK,
- channels and bandwidths,
- how data is transferred via a modem,
- the difference between BPS and Baud and when they are used
- what UART does,
- the different types of UART and their features,
- how ISDN-communication works and its benefits,
- the different types of ISDN and the differences between B- and D channel,
- how DSL- technology works and its benefits,
- the different types of DSL, such as ADSL, HDCL, SDSL and VDCL. Also explain the differences between them,
- RAS & PPP/SLIP negotiation phase hints.
- Install and manage modems and WAN links using the above concepts.

C3.05 Non-IP network protocols [1,5]

- Connect a computer to a token ring network, being aware of:
 - the token ring architecture (topology, physical layer media and data transmission rates)
 - the medium access control protocol in a token ring network
 - pros and cons of a token passing system
- Differentiate between other protocols, i.e. FDDI, ATM and Frame Relay:
 - FDDI network system structure.
 - data rate and distance limits in a FDDI network system
 - medium access control in a FDDI system
 - ATM logical connections (transmission path, virtual path, virtual channel)
 - distinguish cells from packets
 - the ATM layer functions (switching, multiplexing, routing, congestion management)
 - the range of data transmission rates in ATM systems
 - Frame Relay logical connections (virtual circuit, permanent virtual circuit, datalink connection identifier, multilink frame relay, aggregated virtual circuit)
 - the FR layer functions (switching, multiplexing, routing, congestion management)
 - the range of data transmission rates in Frame Relay systems

C4.02 World Wide Web [2]

- Configure clients and support users in understanding:
 - the definition of Universal Resource Locator (URL),
 - the WWW as a client-server application,
 - the role of the server,
 - the role of the client and the configuration of its browser,
 - the operations of HTTP and S-HTTP protocols,
 - http content-type headers vs MIME standard,
 - the aim of main markup languages (HTML, SGML, XML, CSS, XSL) and style sheet,
 - the concept of the Common Gateway Interface (CGI),
 - the concept of an applet,

- cookies, their benefits and dangers.
- Perform main browser setup (proxy, plug-in, etc.).
- Install configure and manage a simple web service.
- Explain how to distinguish a secure connection from an insecure one and when it is necessary to use a secure transaction.
- Enable and disable cookies, ActiveX, Java, and JavaScript. server etc.
- Apply and support users in understanding the common rules of Netiquette.
- Verify and explain how to verify correct implementation of standards in web pages.
- Know the accessibility guidelines and the tools used to evaluate them.
- Know standard bodies such as W3C (World Wide Web Consortium).

C4.03 E-Mail principles and management [2]

- Install and use mail client software, supporting other users to understand:
 - e-mail addresses structure,
 - RFC822 standard,
 - POP3 protocol,
 - IMAP protocol,
 - SMTP protocol,
 - SMTP and its components (sender, protocol, receiver),
 - relaying and related problems,
 - data transmission limitation with SMTP,
 - MIME standard,
 - ASCII, ANSI and UNICODE standards, the ASCII limits on national languages (concept of character set), computers internal data encoding (binary files vs. text files, test files EOL encoding in DOS/Windows, Apple and Unix/Linux system), and computers internal number encoding (high end vs. low end, canonical representation),
 - Different compressed formats (HQX, BIN), the purposes of file compression and the main standards for known platforms (ZIP, GZ, ARC for DOS/Windows; SIT, CPT for Macintosh; GZ, Z, TAR, ZIP for Unix),
 - chat and messaging systems,
 - the purposes and uses of mailing lists,
 - the purposes, uses, and working of Usenet and newsgroups,
 - the purposes, uses and working principles of forums,
 - the purpose of Netiquette,
- Configure the mail software, such as POP3, IMAP, HTTP, News server etc.
- Configure e-mail accounts and related items (POP or IMAP server, SMTP server, etc.).
- Configure e-mail automatic handling rules.
- Setup coding rules (HTML vs. text).
- Access and use webmail applications.
- Install, configure and manage a simple mail server on different platforms (Linux, Windows, Apple).

C2.02 Resource sharing [2]

- Explain and differentiate between different resource sharing principles:
 - o the DAC, MAC, RBAC policies,
 - o the purposes of file sharing,
 - o different permission levels,
 - o the concepts of login and logon-script,
 - o different types of shareable objects: files, folders, printers, modems, ...
 - o the principle of operations, main features and differences of NetBIOS, NETBEUI, SMB and CIFS protocols,
 - o the server browsing operation,
 - o the master browser elections and operations,
 - o main principles of Apple sharing services (AFP, ...),
 - o main principles of Novell IPX/SPX protocols.
- Compare the different protocols and their interoperability.
- Check the available shared resources in a network.
- Know how to create shared resources, such as folders and printer.
- Know how to check which users use shared resources at any one time.
- Control the permissions to shared resources.
- Know how to remove shared resources.
- Know how to disconnect users from a shared resource.
- Evaluate the risk associated with a network logical drive.
- Connect a logical network drive to a shared resource.
- Connect a client to a shared print resource, using a logical print port.
- Connect a client to a shared resource on a server.
- Distinguish between Peer to Peer and Domain based Networks.
- Establish a policy on permissions for shared resources available through the operating system.
- Set up a validation level (user vs. share).
- Set, remove and modify permissions for a user or a group.
- Use the shared resource manager utilities.
- Check users' login and know how to force a user to log out from the network.
- Maintain users/groups in a domain both with Windows, MacOS, and Unix/Linux systems.
- Configure access to Novell network from Windows systems.
- Install Novell IP tunnelling.
- Install Ethernet and IP encapsulated sharing services on Windows and Linux/Unix platforms.
- Know how to install a network printer.
- Know how to connect and use a shared printer and control permissions.
- Know how to cancel or pause a print job. Also know how to reorder it if possible.
- Access shared objects (disks, directories, modem, printers) using Windows, Apple Macintosh, Linux/Unix.
- Stop network printing.

- Activate and deactivate auto-mounting of shared objects using Windows or Apple Macintosh.
- Use sharing services through VLAN over the Internet.
- Setup VLAN to share services over the Internet.

C7.02 Service management essentials [1]

- Establish a proper Service Level Management process and explain its benefits for the organisation.
- Evaluate the main elements of a Service Level Agreement.
- Compare the uses and purposes of Service Level Agreements, underpinning contracts and Operational Level Agreements.
- Negotiate SLA (Service Level Agreement) with internal /external customers and suppliers.
- Identify roles/responsibilities in order to control the actual service level against SLA.
- Promote initiatives for customers satisfaction and benchmarking.
- Set up a proper policy for availability and capacity planning and for IT Service contingency planning.
- Design and assure automatic capture of information for SLA.

C3.08 Network segmenting and VLANs [1]

- Apply the concept of LAN segmentation:
 - o reasons for segmentation,
 - o segmentation through use of bridges / routers / switches.
- Identify switching characteristics:
 - o layer 2 vs layer 3 switching,
 - o Ethernet switching (latency, ...),
 - o collision domains / broadcast domains,
 - o loop avoidance: spanning tree algorithm.
- Know how to configure virtual LANs.
- Troubleshoot most frequent problems in VLANs.

C3.07 Routing [1,5]

- Apply routing concepts:
 - o OSI model, addressing and routing,
 - o ES and IS protocols,
 - o static and dynamic routing, interior and exterior routing.
- Describe autonomous systems, their needs and main characteristics.
- Differentiate between the main routing algorithms:
 - o distance vector algorithms,
 - o link state algorithms.
- Distinguish the main routing protocols:
 - o RIP,
 - o EGP,
 - o BGP,
 - o IGRP, EIGRP.
- Explain the characteristics of TCP/IP routing.

C4.04 VOIP/QOS [1]

- Distinguish the main VOIP protocols:
 - o H323,

- SIP,
- Manage the main VOIP applications:
 - Videoconferencing,
 - IP telephony.
- Recognise the main problems:
 - Delay,
 - Jitter,
 - Congestions.
- Know how to solve the above problems using QOS or overprovisioning.
- Know how to warrant QOS using MPLS.

C6.01 Network management [1]

- Use the functions of a Network Management System.
- Differentiate between architectures of Network Management systems.
- Apply the main components of the protocol (SNMP):
 - their interaction,
 - main services provided by the protocol,
 - main limitations of the protocol,
 - the most important Network Management tools,
- Manage the different parameters in a network (performance, failures, configuration settings).
- Maintain a database about network components and their configuration/policies.

Annexes

Sample Learning Modules	EUCIP Points
EUCIP CORE PLAN	X
EUCIP CORE BUILD	X
EUCIP CORE OPERATE	X
EUCIP IT ADMINISTRATOR	
1. Hardware	D 2/8
2. Operating Systems	B 4/4
3. LAN & Network Services	C 5/5
4. Network expert use	E 5/5
5. IT Security	F 6/6
6. Network Design	D 6/8
ITIL (by EXIN or ISEB)	
IT Service Mgmt. Foundations	A 2/2
Univ. Information Systems	A 2/2
Univ. Telecommunication Networks	E 5/5
Univ. Operating Systems	C 5/5
Univ. IT Security	F 6/6
Cisco Networking Academy	
CCNA1 + CCNA2	C 5/5
	E 5/5
CCNA3 + CCNA4	D 8/8
Cisco Wireless LAN Support Specialist	D 2/8
IT Essentials I	D 2/8
IT Essentials II	C 5/5
IBM AIX Admin	C 5/5
IBM LPI L1	C 5/5
Microsoft Certified Systems Administrator (MCSA*)	
MS 70-270: Installing, Configuring, and Administering Microsoft Windows XP Professional	B 4/4
MS 70-290: Managing and Maintaining a Microsoft Windows Server 2003 Environment	C 5/5
MS 70-291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	E 5/5
	F 4/6
MS 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network (or equivalent*)	F 2/6
Sun Certif. System Administrator for the Solaris OS	B 3/4
	D 1/8
Sun Certif. Network Administrator for the Solaris OS	D 4/8
	E 5/5
Sun Certif. Web Component Developer for J2EE	C 2/5
Sun Certif. Security Administrator for the Solaris OS	F 4/6

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

Skill 53: Network control and operation

“The day-to-day support, operation and control of all equipment within an IT network infrastructure.”

Levels 4 and 5

Skill 56: Network support

“The provision of network maintenance and support services. Support may be provided both to users of the systems and to service delivery functions. Support typically takes the form of investigating and resolving problems and providing information about the systems. It may also include monitoring their performance. Problems may be resolved by providing advice or training to users about the network’s functionality, correct operation or constraints, by devising work-arounds, correcting faults, or making general or site-specific modifications.”

Levels 4 and 5

Skill 52: Management and operations

“The management and operation of the IT infrastructure (typically hardware, software and communications) and the resources required to plan for, develop, deliver and support properly engineered IT services and products to meet the needs of a business. Includes preparation for new or changed services, management of the change process and maintenance of regulatory, legal and professional standards, management of performance of systems and services in relation to their contribution to business performance and management of bought-in services including, for example, public network, virtual private network and outsourced services.”

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 20: Network design

“The production of network designs and design policies, strategies, architectures and documentation, covering voice, data, text, e-mail, facsimile and image, to support business requirements and strategy. This may incorporate all aspects of the communications infrastructure, internal and external, mobile, public and private, Internet, intranet and call centres.”

Level 5

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

Profil 5.1: Network Administrator (Netzwerkadministrator/in)

*“Netzwerk Administrator konfigurieren, betreiben, überwachen und pflegen
Datennetze für Computer sowie integrierte Telekommunikationsnetze für Telefonie,
Videokonferenzen oder Funknetze.”*

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

Métier 3.3b: Technicien réseaux ou télécoms

*“Le technicien réseaux / télécoms est garante du bon fonctionnement et de la
disponibilité des réseaux ou des télécoms dont il a la responsabilité.
Il assure la prévention des dysfonctionnements des réseaux ou des télécoms et
contribue au bon fonctionnement du système d’information.”*

Métier 3.5a:

Administrateur d’outils / systèmes / réseaux et télécoms

*“Il installe, met en production, administre et exploite les moyens informatiques d’un
ou plusieurs sites informatiques.
Il participe au bon fonctionnement des systèmes d’information en garantissant le
maintien à niveau des différents outils et/ou infrastructures des logiciels systèmes
et/ou infrastructures de communication (locale, étendue, voix, image, architecture
centralisée ou client/serveur), dans un objectif de qualité, de productivité et de
sécurité.”*

Métier 5.2: Expert réseaux / télécoms

*“L’expert effectue une vielle technologique, il définit l’architecture du réseau de
l’entreprise ou de projets spécifiques.
Il est l’interface reconnue des experts externes.
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.”*

(?) Métier 6.3: Responsable télécoms

*“Le responsable télécoms et réseaux est chargé de la gestion des infrastructures de
télécommunication de l’entreprise. Considéré comme un maître d’ouvrage vis-à-vis
des opérateurs et comme un maître d’œuvre et un prestataire de services interne
vis-à-vis des autres directions de l’entreprise, ses missions vont de la définition de
l’architecture à l’achat des services télécoms, en passant par le contrôle de gestion
et la vielle au sens large. Le responsable télécoms et réseaux peut être chargé du
déploiement et de l’exploitation de l’infrastructure, ainsi que de la gestion et de
l’encadrement d’une équipe télécoms. Son champ d’action recouvre les services
voix, données et le services internet de l’entreprise au niveau national et
international. Le responsable télécoms est généralement rattaché à la direction des
systèmes d’information, au moins sur la partie données. En revanche la téléphonie
est souvent gérée dans chaque établissement ou par pays.”*