



Australian Government

Department of Education, Employment and Workplace Relations

ICANWK529A Install and manage complex ICT networks

Release: 1

ICANWK529A Install and manage complex ICT networks

Modification History

Release	Comments
Release 1	This Unit first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to install and manage enterprise-wide information and communications technology (ICT) networks.

Application of the Unit

This unit applies to information technology (IT) professionals who work in the complex computing environment of medium-sized to large companies to provide network services and resources.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the required skills and knowledge section and the range statement. Assessment of performance is to be consistent with the evidence guide.</i>

Elements and Performance Criteria

1. Plan and design a complex network to meet business requirements	1.1 Review network design, business requirements and latest vendor technical specifications for network components 1.2 Research options available for providing the network functionality required 1.3 Plan network implementation to provide network services and resources to meet business requirements
2. Design and implement a security strategy	2.1 Analyse requirements for internal and external security 2.2 Design security strategy to meet requirements 2.3 Implement security strategy 2.4 Undertake ongoing monitoring of the viability and reliability of network security, through testing and use of technical tools 2.5 Continually monitor internal and external network access for security breaches
3. Install and configure a complex network to meet business requirements	3.1 Check and install cabling and associated components according to industry standards 3.2 Install and configure servers, routers, switches or other devices to provide internet protocol (IP) addressing and routing 3.3 Install and configure servers, routers, switches or other devices to provide name resolution 3.4 Install and configure servers, routers, switches or other devices to provide network services 3.5 Install and configure remote access services 3.6 Install and configure devices to provide data management services
4. Provide integrated network services across a complex network	4.1 Integrate multiple network services across network 4.2 Analyse and resolve interoperability issues 4.3 Optimise performance 4.4 Rectify security conflicts arising from integrating services
5. Plan, design and implement voice and video business communications system	5.1 Install software and configure and test voice over internet protocol (VoIP) and videoconferencing services 5.2 Incorporate the use of a communications server to provide real-time multimedia communications 5.3 Select common voice and videoconferencing codecs according to standards and practices
6. Manage and support a	6.1 Identify and evaluate appropriate network management tools

complex network	to assist in the administration of the complex network 6.2 Select and install network management tools according to industry and organisational standards 6.3 Set and monitor alerts and logs 6.4 Capture and analyse network performance data 6.5 Implement automated server updates 6.6 Implement desktop management policies 6.7 Implement automated virus checking 6.8 Use remote management tools
7. Test network functionality and obtain sign-off	7.1 Test network functionality and record results 7.2 Record results of network functionality test 7.3 Complete network documentation according to organisational standards

Required Skills and Knowledge

This section describes the skills and knowledge required for this unit.

Required skills

- analytical skills to use complex technical data to develop network designs
- communication skills to consult with customers
- literacy skills to:
 - interpret technical documentation
 - write reports
- numeracy skills to:
 - take test measurements
 - interpret results
 - evaluate performance and interoperability of network services
- problem-solving skills to solve a range of predictable network problems
- research skills to identify, analyse and evaluate broad features of a particular business domain and best practice in networking technologies, including hardware and software to be installed
- technical skills to:
 - implement dynamic name system (DNS), IP addressing and secure virtual private network (VPN) tunnels
 - install and configure application software to provide specific services
 - install, configure and secure server operating systems
 - install, configure and secure switches and routers
 - integrate multiple network services without conflict
 - set up and use network monitoring and management tools
 - test network functionality.

Required knowledge

- firewall configuration
- IP addressing and network configuration
- network:
 - infrastructure
 - load-balancing for applications
 - security
 - server operating systems
 - service configuration, including:
 - DNS
 - dynamic host configuration protocol (DHCP)
 - file transfer protocol (FTP)
 - mail
 - network time protocol (NTP)
 - proxy
 - server messages block (SMB)

- web
 - service management
- troubleshooting tools and techniques, including network diagnostic utilities
- user authentication and directory services
- VoIP
- VPN.

Evidence Guide

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	Evidence of the ability to: • design and implement a complex network that involves integrating multiple network services to meet business requirements • design and implement an appropriate security strategy for a complex network • monitor and test the performance of aspects of the solution • provide ongoing management and support of the network.
Context of and specific resources for assessment	Assessment must ensure access to: • network design and business requirements documents • a complex network or hardware and software required to build a network involving multiple servers, multiple physical locations (or simulation of) and a combination of network services • appropriate learning and assessment support when required. Where applicable, physical resources should include equipment modified for people with special needs.
Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • review of report that outlines design process undertaken, including challenges faced and how these were addressed • direct observation of the candidate installing and configuring components of a complex network • technical documentation detailing configuration of the complete network • verbal or written questioning of candidate to assess required skills and knowledge • evaluation of report that outlines testing procedures, test results and changes made as a result of testing • evaluation of system designed and implemented in terms of performance and suitability for business needs.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where

	appropriate. Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level, language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.
--	--

Range Statement

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

Network components may include:	• cables • digital subscriber line (DSL) modems • local area network (LAN) • modems • routers • servers • switches • WAN • wireless access point.
Network services may include:	• database service • DHCP • DNS • FTP • firewall • hypertext transfer protocol (HTTP, HTTPS) • internet message access protocol (IMAP) • network file system (NFS) • NTP • post office protocol (POP) • print services • proxy • SMB • simple mail transfer protocol (SMTP) • simple network management protocol (SNMP) • transmission control protocol or internet protocol (TCP/IP).
Network resources may include:	• backup and data security • business applications • collaboration tools • conferencing • data storage • databases • email • internet services • printers, faxes and scanners

	• streaming video • VoIP.
Security strategy may include:	• automated updates: • Red Hat Network (RHN) • Windows Server Update Services (WSUS) • encryption • Firewall - demilitarised zone (DMZ) • proxy • public key infrastructure (PKI) and secure socket layer (SSL) certificates • secure remote access • server hardening • smart cards • tokens • user authentication • virus checking • VPN.
Tools may include:	• cable testing • carrier connection tests • data and voice integration measurements • equipment testing • frequency analysers • network performance software • packet tracers • policing and shaping tools.
Data management services may include:	• backup and recovery • disk quotas • distributed file systems • indexing • online and offline storage • storage area networks (SANs).
Integrate multiple network services may include:	• Kerberos • lightweight directory access protocol (LDAP) • Samba • seamless access to Linux and Windows hosted data and services • single login to gain access to multiple services (federated authentication) • VoIP over VPN.

Unit Sector(s)

Networking