



Australian Government

Department of Education, Employment and Workplace Relations

ICANWK303A Configure and administer a network operating system

Release: 1

ICANWK303A Configure and administer a network operating system

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 defines the competency required to create the network configuration required by a client and to set up and use administrative tools to manage the network.

Application of the Unit

This unit applies to frontline technical support personnel who are required to maintain network continuity through changing requirements.

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. Assess network features	1.1 Determine organisational policies and administration arrangements used to administer the network 1.2 Determine the type of network operating system (NOS) and interfaces used by the existing network and potential compatibility issues caused by integration of other networks 1.3 Identify the risks associated with administration of a network to minimise the loss of data or service during operations 1.4 Determine network administration tools that can be used with the NOS to manage network performance and enforce organisational policies
2. Administer and support the system using administration interfaces	2.1 Use interfaces to format hard drives, set up security restrictions and establish user log-in information to administer a basic network 2.2 Use administration tools to develop a map of system interaction to determine the data required by particular users and how often the data is accessed 2.3 Examine existing applications and software and plan required upgrades or reconfigurations to new system or applications 2.4 Test reconfiguration for successful interface with existing system to ensure compatibility
3. Set up and manage the network file system	3.1 Create a required file and folder structure using appropriate administration and system tools 3.2 Set the security, access and sharing of file system to meet user requirements 3.3 Identify and implement the virus protection requirements for the network in line with organisational procedures 3.4 Test and document the file system to ensure that appropriate access is available to the user groups according to organisational standards
4. Administer user services and user accounts	4.1 Determine the user services required, and implement using the appropriate administration and system tools 4.2 Create users and groups as required to facilitate user security and network access according to user authorisation 4.3 Verify successful access by users to authorised

	network data and resources, and record outcomes 4.4 Set or modify user settings to ensure compliance with security and access policies 4.5 Review procedures and take action to ensure that users who are no longer part of the organisation have their accounts disabled, deleted or modified
5. Provide and support backup security	5.1 Scan and clean the network of viruses before performing backup of the network 5.2 Determine security risks to which data is exposed and provide appropriate prevention methods and recovery processes 5.3 Report identified security risks to appropriate person 5.4 Implement systems to provide backup and service restoration capability in the event of a disaster according to organisational policies 5.5 Document and disseminate the disaster-recovery procedures

Required Skills and Knowledge

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

Required skills

- analytical skills to:
 - determine NOS types and compatibility issues
 - determine risks associated with administration of a network
- communication skills to:
 - inform clients of technical procedures
 - liaise with clients and team members across different levels and in different contexts
 - undertake active listening with clients and team members
 - use open-ended questioning techniques
- literacy skills to:
 - document created file system
 - document disaster-recovery procedures
 - interpret organisational policies
- planning skills to plan upgrades and reconfigurations to new systems or applications
- technical skills to:
 - administer and configure NOS
 - identify security gaps and secure with appropriate hardware and software
 - implement systems to provide backup and service restoration capability
 - monitor user accounts according to organisational policy
 - perform compatibility testing after upgrade or reconfiguration
 - scan and clean the network of viruses before backup
 - test successful access by users to authorised network data and resources
 - test the file system access.

Required knowledge

- antivirus software, its operation, installation and update procedures
- current industry standard NOS
- facilities available in the operating environment
- features and capabilities of networking technologies
- implementation of network security in a local area network (LAN):
 - file and folder permissions
 - users and group settings
- monitoring aspects of network performance or traffic:
 - system administration tools
 - third-party tools.

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: • use network administrative tools to carry out system administration tasks • manage the network file system • create the network configuration required by the client • provide user services and user accounts • provide backup and service restoration capability.
Context of and specific resources for assessment	Assessment must ensure access to: • user network requirements • antivirus software • network administration tools • a live network with a representative range of networked environments and operating systems • a server • technical records, organisational policies, access policy and documentation • appropriate learning and assessment support when required • modified equipment 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: • direct observation of candidate: • managing a network using network administration and system tools • performing virus scans, virus removal and virus updates • review of organisational backup schedules created • verbal or written questioning to assess candidate's knowledge of the facilities available in the operating environment.
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.

Organisational policies may include:	• diagnostic • how and what the organisation will operate • maintenance • OHS • security • user enrolment.
Network may include:	• data • embedded systems • LAN • personal digital assistant (PDA) • radio frequency identification (RFID) network • smartphones • internet • virtual private network (VPN) • voice network • wide area network (WAN) • wireless network.
Network operating system may include:	• embedded OS: • digital media players • PDAs • robots • routers • smartphones: • Android • BlackBerry • Symbion • Windows CE • Fabric or XPATH OS by Brocade • JunOS by Juniper Networks • Linux • Mac • Open Enterprise Server or Netware by Novell • SAN-OS by Cisco

	• Windows Server OS.
System may include:	• application servers • billing system • computers • file servers • financial system • information system • management system • network • printer server • software • storage system • user management system.
Users may include:	• departments within an organisation • persons within a department • third parties.
Applications may include:	• database programs • email programs • internet browsers • multimedia applications • spreadsheets • voice applications • word-processing.
Software may include:	• application • commercial • customised • in-house • programming: • assembler • compiler • development tools • system: • computer security • device drivers • operating system.
File system may include:	• folder structures • multiple or single logical disks and complex directory • multiple or single servers.
User settings may include:	• log-in • passwords

	• security • usernames.
Backup may include:	• more comprehensive and complex backup facilities across the network • simple single tape-unit backup.
Security risks may include:	• file and folder sharing • open or free networks • operating system vulnerability: • service packs • security updates • social engineering • theft • trojan horses • unauthorised access: • adware • hackers • identity fraud • malware • phishing • spyware • viruses • web browser risks • worms.
Prevention methods may include:	• anti-spam software • anti-spyware • antivirus software • ensuring proper security certificate are used: • secure socket layer (SSL) • file encryption • firewalls • password best practice: • change frequency • complexity of password construction • password confidentiality • re-use • use • user awareness and education • wireless encryption: • wi-fi protected access (WPA and WPA2) • wired equivalent privacy (WEP).

<i>Appropriate person</i> may include:	• network administrator • network manager • supervisor • system administrator.
--	--

Unit Sector(s)

Networking