



Australian Government

Department of Education, Employment and Workplace Relations

ICANWK406A Install, configure and test network security

Release: 1

ICANWK406A Install, configure and test network security

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, configure and test network security in an information and communications technology (ICT) network.

Application of the Unit

This unit applies to information technology (IT) professionals who install, configure and test secure networks of any size.

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 security threats and vulnerabilities to identify risk	1.1 Assess and report on current system security, according to required asset security level 1.2 Determine additional network, software, hardware and system security threats and vulnerabilities 1.3 Use identified threats and vulnerability information to identify security risks 1.4 Make recommendations to management to address security deficiencies, according to current and future commercial and business requirements
2. Implement countermeasures for identified vulnerabilities and threats	2.1 Implement required level of perimeter security based on current and future business needs 2.2 Assess and implement best practice server and network hardening techniques and measures 2.3 Implement secure authentication and user account controls 2.4 Secure data integrity and transmission
3. Test and verify functionality and performance of security system implemented	3.1 Design test items to verify key function and performance measures against criteria 3.2 Conduct function and performance tests recording results 3.3 Modify and debug security system as necessary 3.4 Develop documentation on current system settings and file for future reference
4. Provide systems for monitoring and maintaining security	4.1 Monitor current network security, including physical aspects, using appropriate third-party testing software where applicable 4.2 Review logs and audit reports to identify and record security incidents, intrusions or attempts 4.3 Carry out spot checks and audits to ensure that procedures are not being bypassed 4.4 Document newly discovered security threats, vulnerabilities and risks in a report for presentation to appropriate person to gain approval for changes to be made

Required Skills and Knowledge

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

Required skills

- analytical skills to:
 - analyse systems evaluation
 - review system security logs for breaches
- communication skills to liaise with clients
- literacy skills to write reports for evaluating system security status according to organisational security policies
- numeracy skills to undertake a cost-benefit comparison
- problem-solving skills to:
 - determine intrusion detection
 - troubleshoot and debug
- research skills to identify and analyse network security methodologies and technologies
- technical skills to:
 - develop enterprise policies strategies and procedures
 - implement local area network (LAN), wide area network (WAN), virtual private network (VPN) and wireless local area network (WLAN) solutions
 - implement security strategies and configure network security software and hardware
 - install hardware and software related to improving network security
 - undertake a network security risk assessment.

Required knowledge

- authentication issues
- overview knowledge of:
 - client business domain, including client organisation structure and business functionality
 - features and capabilities of networking technologies
 - privacy issues and privacy legislation
 - security information sources
 - risk analysis
- common VPN issues, including bandwidth and dynamic security environment
- configuring routers and switches
- current industry-accepted hardware and software security products, with broad knowledge of general features and capabilities
- function and operation of VPN concepts, including encryption, firewalls, packet tunnelling and authentication
- network protocols and operating systems
- organisational issues surrounding security
- security perimeters and their functions
- security protocols, standards and data encryption

- security threats, including eavesdropping, data interception, data corruption, data falsification
- types of VPNs, including site-to-site, user-to-site internet traffic and extranets
- systems and procedures related to:
 - audit and intrusion detection systems
 - auditing and penetration testing techniques
 - cryptography
 - LAN, WLAN and WAN
 - screened subnets
 - transmission control protocols or internet protocols (TCPs/IPs) and applications
 - use of virus detection software.

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: • assess and identify security threats, vulnerabilities and risks • determine appropriate countermeasure for threat, vulnerability or risk • implement countermeasure per threat or risk • install, configure and test network elements to ensure perimeter security • test and verify function and performance of selected security measures • monitor network for suspicious activity taking appropriate action where necessary • document newly discovered threats, vulnerabilities and risks, including change recommendations for approval.
Context of and specific resources for assessment	Assessment must ensure access to: • site where secure network installation may be conducted • network security documentation • equipment specifications • network components • hardware and software • firewalls (hardware and software) • live network • organisational guidelines • networked (LAN) computers • WAN service point of presence • 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: • documentation of current system security analysis that outlines required enterprise security requirements • identification of additional security threats and vulnerabilities

	• verbal or written questioning to assess candidate's knowledge of network security • direct observation of candidate performing tasks required to successfully install, configure and test a secure network • direct observation of candidate performing tasks required to successfully test function and performance of secure network • direct observation of candidate performing tasks required to successfully monitor and document newly discovered security threats, vulnerabilities and risks.
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.

System may include:	• applications • databases • gateways • operating systems • servers • WAN communication links • workstations.
Asset may include:	• data and information • intellectual property • physical assets.
Network may include:	• intranets • large and small LANs • internet • VPNs • WANs • WLANs.
Software may include:	• applications: • commercial • customised • in-house • packaged • encryption modules • operating systems • security: • antivirus • firewall • spyware • utilities: • audit • network monitoring.
Hardware may include:	• analog modems • digital subscriber line (DSL) modems • firewall devices

	• network cabling • wired and wireless networks • notebooks • personal computers • routers • servers • switches • workstations.
Security threats may include:	• by-pass • denial of service • eavesdropping • elevation of privilege • hacking • impersonation • manipulation • penetration • repudiation • viruses or malicious code.
Vulnerabilities may relate to:	• application bugs • communications devices • firmware flaws • firewall misconfigurations • operating system bugs • poor bandwidth control measures • transmitting data in plain text • unnecessary services and protocols • weak authentication techniques • weak permissions • weak physical security.
Commercial and business requirements may include:	• availability • backup and recovery of data • confidentiality • firewalls • hacking prevention • integrity • password logons • remote access to internal network.
Perimeter security may include:	• access control • auditing • authentication • authorisation

	• hardware or software firewalls • identification • network address translation (NAT) • surveillance.
Server may include:	• application • web • email • file and print • firewall • file transfer protocol (FTP) • proxy, cache • voice over internet protocol (VoIP).
Hardening techniques may include:	• demilitarised zones (DMZ) • encryption • intrusion detection system (IDS) • operating system patch application and management • rigid shared resource permissions • service pack application • strong firewall configurations, including unused port blocking • strong physical security • strong user authentication techniques • unused services and protocols disablement.
Data integrity may include:	• encryption • hash encoding • protocol control • VPN.
Document may include:	• audit trails • International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Australian Standards (AS) standards • naming standards • project management templates • report writing principles • security analysis report • version control.
Appropriate person may include:	• supervisor • authorised business representative • client.

Unit Sector(s)

Networking