Australian Government

Department of Education, Employment and Workplace Relations

ICANWK511A Manage network security

Release: 1

ICANWK511A Manage network security

Modification History

Release	Comments
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to implement and manage security functions throughout a network.

Application of the Unit

This unit applies to middle managers, such as information security managers, network engineers or security analysts, responsible for implementing and managing the organisational security management system.

They provide technical advice, guidance and leadership in resolution of specified problems and the role may involve responsibility for others. The role also involves leading development of strategic reviews, determining security threats and implementing controls to mitigate risk. Related tasks include network security planning, implementation, cost-analysis and budgeting.

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
Elements describe the essential outcomes of a unit of competency.	*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.*

Elements and Performance Criteria

1. Define a process for designing security	1.1 Define planning phase for ***network*** security design 1.2 Define building phase for network security design 1.3 Define managing phase for network security design
2. Identify threats to network security	2.1 Determine why ***attacks*** occur 2.2 Determine who the attack may come from 2.3 Analyse common types of network ***vulnerabilities*** 2.4 Determine how attacks occur 2.5 Design a threat model to categorise treats
3. Analyse security risks	3.1 Determine elements of risk management 3.2 Determine ***assets*** that require protection 3.3 Categorise assets and calculate their value to the organisation 3.4 Create a risk management plan
4. Create a security design	4.1 Determine attacker scenarios and threats 4.2 Design ***security*** measures for ***network components*** 4.3 Obtain feedback and adjust if required 4.4 Develop security policies
5. Design and implement responses to security incidents	5.1 Design auditing and incident response procedure 5.2 Document security incidents 5.3 Implement configurations aligned with incident response procedure design 5.4 Test and sign off

Required Skills and Knowledge

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

Required skills

- analytical skills to:
  - analyse network information
  - plan approaches to technical problems or management requirements
- communication skills to:
  - convey and clarify complex information
  - liaise with clients
- literacy skills to interpret and prepare technical documentation, including recording security incidents and developing security policies
- planning skills to plan control methods for managing system security
- problem-solving skills to:
  - apply solutions in complex networks, including systems processes
  - deploy rapid deployment of solutions to problems involving failure and security incidents
- technical skills to apply best practice to systems security methodologies and technologies.

Required knowledge

- detailed knowledge of:
  - auditing and penetration testing techniques
  - logging analysis techniques
  - organisational network infrastructure
  - related weaknesses of installed network infrastructure
  - security technologies
- broad knowledge of:
  - capabilities of software and hardware solutions
  - emerging security issues
  - general features of emerging security policies, with depth in security procedures
  - network management and security process controls
- network security implementation risk management plans and procedures.

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: • identify threats to security • develop risk management plan • design network security policies • analyse and plan solutions to compromised networks and design incident response • evaluate security information and use it to plan suitable control methods and countermeasures • add network controls, according to system security policies, procedures and risk management plan.
Context of and specific resources for assessment	Assessment must ensure access to: • site or prototype where network security may be implemented and managed • network support tools currently used in industry • organisational security policies, manufacturer recommendations and security standards • 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: • verbal or written questioning to assess candidate's knowledge of emerging security issues, security features of hardware and software, limitations in vendor solutions, operating systems and software • direct observation of candidate demonstrating management of network security in a range of complex security situations • review of documentation prepared by candidate to manage network security.
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 may include:	• data • internet • local area networks (LANs) • large and small LANs • virtual private networks (VPNs) • wide area networks (WANs) • wireless LANs (WLANs).
Attacks and vulnerabilities may include:	• authorisations • brute force and dictionary attacks • denial of service and by-pass • eavesdropping • hackers • internal threats • intruder detection • manipulation • penetration • social engineering, including impersonation • spoofing • viruses using logging.
Assets may include:	• data • hardware • personal information • product and branding information.
Security may include:	• AAA • authentication process, Kerberos and challenge handshake authentication protocol (CHAP) • Diameter and remote authentication dial-in user service (RADIUS) • folder and file security • IPSec • lightweight extensible authentication protocol (LEAP) • personal knowledge management (PKM) • smart cards • secure socket layer (SSL)

	• tokens • VPN • wired equivalent privacy (WEP) • wi-fi protected access (WPA) or WPA2.

Network components may include:	• servers
	• workstations
	• accounts
	• authentication
	• data
	• data transmission
	• network perimeters:
	  • part of router configuration or proxy server
	  • products:
	  • Cisco Centri, PIX
	  • ClearOS
	  • IPcop
	  • Linux iptables
	  • MS ISA server
	  • SmoothWall
	  • Untangle.

Unit Sector(s)

Networking