



Australian Government

Department of Education, Employment and Workplace Relations

ICANWK607A Design and implement wireless network security

Release: 1

ICANWK607A Design and implement wireless 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 mitigate security threats to a wireless local area network (WLAN) by implementing security standards and policies.

Application of the Unit

This unit applies to protecting the wireless network from security threats by applying security policies and best practices to implement security standards and to configure wireless security components. Relevant job roles include advanced wireless help-desk support technician, wireless network support specialist and wireless network engineer.

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 to implement wireless network security	1.1 Research and evaluate organisational and regulatory security policies that have been used to benchmark acceptable network security standards 1.2 Assess customer requirements and needs against regulatory security compliance and OHS considerations 1.3 Produce a plan with security-solution documentation for future growth and security needs
2. Design, implement and test guest access services	2.1 Analyse and select the appropriate architecture for guest access services 2.2 Produce a map and set up guest access accounts 2.3 Configure WLAN controller authorisation 2.4 Configure the anchor and internal controllers 2.5 Troubleshoot guest access issues
3. Design, implement and test the security of wireless client devices	3.1 Design and configure authentication of clients and management frame protection on clients and controllers 3.2 Configure access control servers for integration with wireless network 3.3 Configure client and server-side digital certificate services 3.4 Troubleshoot secure wireless connectivity services
4. Design, implement and test the integration of wireless network with organisational network admission control systems	4.1 Analyse network admission control architectures to assess the feasibility of network integration 4.2 Analyse the high-level authentication process flow to ensure compatible integration 4.3 Configure and test the wireless controller for admission control 4.4 Troubleshoot integration issues of network with access control
5. Evaluate and plan secure wireless connectivity services	5.1 Configure the intrusion detection system (IDS) to monitor the network activities for malicious activities or policy violations 5.2 Analyse the report produced by the IDS to review threat-mitigation strategies 5.3 Update security solution plan to mitigate wireless vulnerabilities to ensure network integrity
6. Manage the requirements to integrate	6.1 Evaluate end-to-end security solutions and assess how they integrate with the planned wireless solutions

the WLAN with advanced security platforms	6.2 Analyse the <i>firewall configuration requirements</i> of WLANs to ensure compliance with organisational policies 6.3 Configure and test the WLAN controllers for wired and wireless intrusion prevention and detection system (IPDS) security protection
---	--

Required Skills and Knowledge

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

Required skills

- communication skills to liaise with internal and external personnel on technical, operational and business-related matters
- literacy skills to:
 - interpret technical documentation
 - write reports as required
- numeracy skills to:
 - evaluate performance and interoperability of network
 - interpret results
 - take test measurements
- planning and organisational skills to:
 - coordinate the process in liaison with others
 - plan, prioritise and monitor own work
- problem-solving and contingency-management skills to:
 - adapt configuration procedures to requirements of network
 - reconfigure depending on differing operational contingencies, risk situations and environments
 - troubleshoot and debug WLAN issues
- research skills to investigate appropriate hardware to meet requirements
- technical skills to:
 - select and configure networking devices and assess and implement security requirements
 - use networking tools.

Required knowledge

- configuration, verification and troubleshooting procedures to undertake:
 - router operation and routing
 - VLAN switching and inter-switching communications
- IOS and IP networking models
- intrusion prevention system (IPS) and IDS security protection
- threat mitigation strategies
- wireless:
 - current regulations, standards and certifications
 - deployment schemes
 - network security technology
 - network topologies, architectures and elements
 - networking protocols
- WLAN:

- advanced security platforms
- devices and their specification and use
- radio frequencies characteristics and their measuring techniques.

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: • conduct research and produce security solutions plan • evaluate, design and implement a WLAN site security plan • evaluate end-to-end security solutions and assess their integrate with the planned wireless solutions • use network tools to test wireless controllers and IPDS solutions.
Context of and specific resources for assessment	Assessment must ensure access to: • site or prototype where network installation may be conducted • hardware and software • organisational guidelines • live network • stand-alone and lightweight WLAN controllers and AP • hardware and software WLAN site survey tools • hardware and software IDS and IPS • 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 the candidate installing, configuring and testing a new or updated network • evaluation of documentation prepared by the candidate outlining testing procedures, test results, recommendation to network changes and completion records • verbal or written questioning of required knowledge.
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.

Security-solution documentation may include:	• equipment inventory • naming standards • project management templates and report writing • satisfaction reports • standards: • International Organization for Standardization (ISO) • International Electrotechnical Commission (IEC) • Australian Standards (AS) • version control.
Guest access services may include:	• anchor • bandwidth limiting • demilitarised zone or perimeter network (DMZ) • redundancy • scaling • VLAN-based • wired guest access.
Authorisation may include:	• authentication • email • external • internal • pass through.
Wireless network may include:	• cellular network • mobile services • paging network • wireless LAN (WLAN).
Architectures may include:	• agent versus agent • in-band • out-of-band.
Threat-mitigation strategies may include:	• client exclusions • custom signature • rogue reporting and location • signature • switch-port tracing.

<i>Wireless vulnerabilities</i> may include:	• anomalous behaviour attacks • client misconfiguration • denial of service (DoS) • eavesdropping • hijacking • radio frequency (RF) jamming • signature attacks • social engineering.
<i>Firewall configuration requirements</i> may include:	• access control list (ACL) • demilitarised zone (DMZ) • IP port pass-through.

Unit Sector(s)

Networking