



Australian Government

Department of Education, Employment and Workplace Relations

ICAB5159C Build a security shield for a network

Release: 1

ICAB5159C Build a security shield for a network

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to build a security shield for a wireless local area network (WLAN) or local area network (LAN). The following unit is linked and forms an appropriate cluster: • ICAA5056B Prepare disaster recovery and contingency plans No licensing, legislative, regulatory or certification requirements apply to this unit at the time of publication.
------------------------	---

Application of the Unit

Application of the unit	
--------------------------------	--

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Prerequisite units		
	ICAS5192B	Configure an internet gateway

Employability Skills Information

Employability skills	This unit contains employability skills.
-----------------------------	--

Elements and Performance Criteria Pre-Content

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

ELEMENT	PERFORMANCE CRITERIA
1. Develop security framework	1.1. Determine level and nature of security required based on the current and future business requirements, the business strategic plan or client expectations 1.2. Identify and document security threats 1.3. Prepare plans and determine impact appraisal costs to manage sufficient protection of those assets identified as being at risk 1.4. Review firewall features and evaluate for security risks 1.5. Identify security perimeters within client/server system as required by developed security plan 1.6. Evaluate intrusion detection system (IDS) methods 1.7. Investigate framework for secure electronic communication infrastructure (SECI) and consider for use in an organisation that has valuable IP or organisational secrets 1.8. Investigate the use of a virtual private network (VPN) solution and determine where outside communication is used to link to the network as a normal business process 1.9. Determine hardware and software needs and prioritise according to security plan 1.10. Prepare cost-benefit analysis for proposed security shield according to business requirements 1.11. Finalise security framework components 1.12. Develop related policies and procedures and distribute to client as required according to business requirements
2. Implement security framework	2.1. Establish physical security perimeter through use of secure sites and components as required by enterprise security plan 2.2. Establish system security perimeter as required by security plan and chosen technology 2.3. Establish application security perimeter as required through server configuration 2.4. Establish data security perimeter through application access on the client/server system, wireless and use of VPN solution as required 2.5. Instruct client on the security shield and their

ELEMENT	PERFORMANCE CRITERIA
	responsibilities according to enterprise <i>security plan</i>
3. Test and validate security processes	3.1. Develop and execute a program of selective independent audits and penetration tests and record outcomes 3.2. Compare performance benchmarks against enterprise <i>security plan</i> 3.3. Implement audit and test programs and record, analyse and report results 3.4. Make changes to the security framework based on test results

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Ability to develop basic policies and procedures
- Ability to undertake a basic network security risk assessment
- Design, development and implementation of various VPN solutions
- Implementing LAN and WAN solutions
- Cost-benefit analysis

Required knowledge

- Security threats, including eavesdropping, data interception, data corruption, data falsification
- Authentication issues
- Organisational issues surrounding security
- Security perimeters and their functions
- Types of VPNs, including site-to-site, user-to-site internet traffic and extranets
- Function and operation of virtual private networking (VPN) concepts, including encryption, firewalls, packet tunnelling and authentication
- Common VPN issues, VoIP, wireless VoIP including quality of service (QoS) considerations, bandwidth, dynamic security environment
- Network protocols and operating systems
- Cryptographic check summing
- LAN, WLAN and WAN solutions
- TCP/IP protocols and applications

REQUIRED SKILLS AND KNOWLEDGE

- NGN data and voice integration, policing and shaping,
- Basic auditing and penetration testing techniques
- EDI security specifications, such as S/MIME and the use of XML/EDI
- Screened subnets
- Virus detection software
- Audit and intrusion detection systems
- Australian Computer Society Code of Ethics

Evidence Guide

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 following is essential:

- Assessment must confirm the ability to develop, implement and maintain a network security shield for VPNs, LANs and WLANs.

To demonstrate competency in this unit the following resources will be needed:

- Network technical requirements
- Network infrastructure, including servers and security hardware and software

Industry/vendor training may include CISCO, Microsoft, IBM, Redhat.

Context of and specific resources for assessment

The breadth, depth and complexity covering planning and initiation of alternative approaches to skills or knowledge applications across a broad range of technical and/or management requirements, evaluation and coordination would be characteristic.

The demonstration of competency may also require self-directed application of knowledge and skills, with substantial depth in some areas where judgement is required in planning and selecting appropriate equipment, services and techniques for self and others.

Assessment must ensure:

- Applications involve participation in development of strategic initiatives as well as personal responsibility and autonomy in performing complex technical operations or organising others. It may include participation in teams including teams concerned with planning and evaluation functions. Group or

EVIDENCE GUIDE	
	team coordination may also be involved.
Method of assessment	The purpose of this unit is to define the standard of performance to be achieved in the workplace. In undertaking training and assessment activities related to this unit, consideration should be given to the implementation of appropriate diversity and accessibility practices in order to accommodate people who may have special needs. Additional guidance on these and related matters is provided in ICA05 Section 1. - Competency in this unit should to be assessed using summative assessment to ensure consistency of performance in a range of contexts. This unit can be assessed either in the workplace or in a simulated environment. However, simulated activities must closely reflect the workplace to enable full demonstration of competency. - Assessment will usually include observation of real or simulated work processes and procedures and/or performance in a project context as well as questioning on underpinning knowledge and skills. The questioning of team members, supervisors, subordinates, peers and clients where appropriate may provide valuable input to the assessment process.
Guidance information for assessment	The interdependence of units for assessment purposes may vary with the particular project or scenario. Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, for example: - ICAA5056B Prepare disaster recovery and contingency plans An individual demonstrating this competency would be able to: - Demonstrate understanding of a broad knowledge base incorporating theoretical concepts, with substantial depth in some areas - Analyse and plan approaches to technical problems or management requirements

EVIDENCE GUIDE

	• Transfer and apply theoretical concepts and/or technical or creative skills to a range of situations • Evaluate information, using it to forecast for planning or research purposes • Take responsibility for own outputs in relation to broad quantity and quality parameters • Take some responsibility for the achievement of group outcomes • Maintain knowledge of industry products and services
--	--

Range Statement**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.

Business requirements may include but is not limited to:

- people and technology interaction
- storage and recovery of data
- access to internal network
- passwords/logons
- access control lists
- firewalls
- black-hat hacking/cracking
- confidentiality
- integrity
- availability
- the perceived value of information to competitors and the malicious nature of internet crackers
- an increase in internet usage

Client may include but is not limited to:

- internal departments
- external organisations
- individual people
- internal employees

RANGE STATEMENT	
<i>Security threats</i> may include:	• eavesdropping • manipulation • impersonation • penetration • denial of service and by-pass • hackers • viruses using logging • spoofing • associations
<i>Firewall</i> may include:	• hardware appliances • proxy servers • individual PC solution • varying functionality including network address translation (NAT)/IP masquerading, routing to specific machines
<i>System</i> may include but is not limited to:	• databases • applications • servers • operating systems • gateways • application service provider • ISP
<i>Security plan</i> may include:	• theft • viruses • standards (including archival, back-up, network) • privacy • audits • alerts • usually relates directly to the security objectives of the organisation
<i>Secure electronic communication infrastructure (SECI)</i> may include:	• strong authentication • WPA • AAA • strong encryption • remote access integration • secure tunnelling • IP routing • firewalls • scalability

RANGE STATEMENT	
	• redundancy
Network may include but is not limited to:	• large and small LANs • WLANs • national WANs • VPNs • the internet • the use of the PSTN for dial-up modems only • DSL connections • private lines • data • voice
Hardware may include but is not limited to:	• workstations • personal computers • modems and other connectivity devices • networks • remote sites • servers • DSL modems
Software may include but is not limited to:	• commercial software applications • organisation-specific software, packaged software, in-house or customised software
Policies may include:	• incident response procedures • network intrusion detection systems • forensic procedures • training • awareness raising policy
Server may include:	• Application/web servers • BEA Weblogic servers • IBM VisualAge and WebSphere • Novell NDS servers • Email servers • Voice servers • File and print servers • FTP servers • Firewall servers • Proxy/cache servers
Application	• May include but are not limited to commercial software applications; organisation-specific software; word processing, spreadsheet, database, graphic, communication packages

RANGE STATEMENT	
	and presentation functionalities. • May include presentation applications contained in Microsoft Office, Lotus Suite, Claris Works, Star Office or other similar applications.
<i>Security perimeter</i>	• physical security perimeter • system security perimeter • wireless security perimeter • application security perimeter • data and voice security perimeter

Unit Sector(s)

Unit sector	Build
--------------------	-------

Co-requisite units

Co-requisite units		

Competency field

Competency field	
-------------------------	--