Australian Government
Department of Education, Employment and Workplace Relations

ICAS5123C Manage network security

Release: 1

ISC INDUSTRY SKILLS COUNCILS
Creating Australia's Future

ICAS5123C Manage network security

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to implement and manage security functions throughout a network. 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		
	ICAS4124B	Monitor and administer network security

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. Identify threats to network	1.1. Conduct a network infrastructure analysis to understand network complexity 1.2. Determine risk category of each point on the ***network*** 1.3. Analyse approved ***user*** point of contact with ***network*** 1.4. Determine non-authorised ***user*** points of contact with the ***network*** 1.5. Conduct risk analysis on each identified category 1.6. Audit and document logs of current system
2. Determine risk of network failure	2.1. Undertake ***security*** analysis of risk data on each network category 2.2. Review log usage files 2.3. Analyse ***user*** points of contact with the network for weaknesses 2.4. Conduct ***threat assessment*** matrix on ***network*** 2.5. Design network ***security*** requirements that fit with organisational systems plans and procedures 2.6. Design audit trails that incorporate ***user*** tracking to determine risk
3. Plan suitable control methods for the network	3.1. Plan control methods for managing user access 3.2. Review controls over data input, output, files permissions, log-on and processing 3.3. Manage external and internal permission structures 3.4. Design automatic intrusion notification processes in line with systems management policy 3.5. Document controls for ***security*** and risk issues 3.6. Obtain approval from approved security senior management for the design of the control
4. Incorporate controls into the network	4.1. Add network controls to the ***network*** in line with system security polices and procedures 4.2. Document ***user*** access security provisions by user classification at program, record or field level, and include procedures for controlling the security provisions according to client requirements
5. Implement additional security facilities	5.1. Review external or intranet access, using appropriate software control mechanisms 5.2. Evaluate ***firewalls*** and record findings and preferences in rank order

ELEMENT	PERFORMANCE CRITERIA
	5.3. Investigate and consider use of a 'demilitarised zone' (DMZ) 5.4. Install and configure ***firewall*** in accordance with manufacturer recommendations and ***security*** standards 5.5. Make recommendations for additional ***equipment*** 5.6. Install approved ***equipment*** and configure to provide required levels of security

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE This section describes the skills and knowledge required for this unit.
Required skills
• Investigation skills for identifying, analysing and evaluating security systems logs for weaknesses, invalid users and intruders • Application of best practice in systems security methodologies and technologies • Problem solving skills for complex networks, including systems processes • Rapid deployment of solutions to problems involving failure • Ability to analyse network information and determine actions • Report writing skills • Questioning and active listening skills
Required knowledge
• Network management and security process controls • Specific and detailed knowledge of the organisation's network infrastructure • Security technologies and capabilities of software and hardware solutions, with substantial depth in some areas • Logging analysis techniques, with broad knowledge of general features, with depth in security procedures • Broad knowledge related to emerging security issues, with substantial depth in related weaknesses of installed network infrastructure

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 knowledge of emerging security issues, security features of hardware and software, limitations in vendor solutions, operating systems and software. • Assessment must confirm the ability to implement and manage security functions on a network. To demonstrate competency in this unit the following resources will be needed: • Live system • Network support tools
Context of and specific resources for assessment	Managing network security is a complex process involving internal and external threats and choices between a range of potential solutions. With many small to medium enterprises joining larger organisations in providing both domestic and global e-commerce facilities, it is increasingly important to provide secure networks. This can only be done with a comprehensive plan that takes into account the whole organisation system as well as the network. Analysis involves participation in development of network security planning and implementation. 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

EVIDENCE GUIDE	
	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 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.

EVIDENCE GUIDE	
	An individual demonstrating this competency would be able to: • Demonstrate understanding of security in relation to network solutions • Describe in detail issues related to security in some key areas • Analyse and plan to solve compromised networks • Determine network security requirements • Apply theoretical scenarios in line with security and technical issues • Demonstrate skills in a range of complex security situations • Evaluate security information and use it for planning purposes • Take responsibility for the achievement of security outcomes • Maintain knowledge of industry products and services Additionally, 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 • 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

Range Statement

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.	
Network may include but is not limited to:	• large and small LANs • WLANs • VPNs • WANs • the internet • the use of the PSTN for dial-up modems and DSL • private lines • data • voice
Demilitarised Zone (***DMZ***)	• May include a computer or small sub-network that sits between a trusted internal network , such as a corporate private LAN , and an untrusted external network, such as the public Internet. • Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.
User may include:	• a person within a department • a department within the organisation • a third party
Security may include but is not limited to:	• IPSec • SSL • PKM • LEAP • WEP • WPA • AAA • Diameter • tokens • smart cards
Threat assessment may include:	• eavesdropping • manipulation

RANGE STATEMENT	
	- impersonation - penetration - denial of service and by-pass - spoofing - authorisations - hackers - viruses using logging - intruder detection - other tools
Equipment may include but is not limited to:	- workstations - personal computers - modems or other connectivity devices - printers - hard drives - DSL modems - monitors - switches - hubs - personal digital assistant (PDA) - other peripheral devices
Firewalls may be part of router configuration or proxy server. Products include	- Cisco Centri - Smoothwall - IPcop - Check Point FireWall-1 - CyberwallPLUS - Linux - IPtables firewall - OpenBSD firewall

Unit Sector(s)

Unit sector	Support

Co-requisite units

Co-requisite units	

Co-requisite units		

Competency field

Competency field	