Australian Government

Department of Education, Employment and Workplace Relations

ICANWK403A Manage network and data integrity

Release: 1

ICANWK403A Manage network and data integrity

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 and network technicians, responsible for implementing and managing the organisational disaster recovery and asset protection policy and procedures.

The role involves leading the development of asset protection processes, determining threats and implementing controls to mitigate risk.

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. Ensure compliance with company network and security policies	1.1 Review company ***security policies*** 1.2 Audit and record security access 1.3 Ensure user accounts are controlled 1.4 Ensure secure file and resource access
2. Conduct audit on system assets	2.1 Use appropriate ***tools*** and techniques to conduct audit on system hardware and software ***assets*** 2.2 Develop a system to record assets 2.3 Use system to develop reports on assets for management
3. Implement an antivirus solution	3.1 Research appropriate ***antivirus*** and anti-malware solutions 3.2 Implement antivirus or anti-malware solution 3.3 Test antivirus and anti-malware solution functionality
4. Implement systems to protect assets from threats	4.1 Determine ***environmental threats*** to data 4.2 Document systems to protect from environmental threat 4.3 Implement system to protect data from environmental threat
5. Develop a backup solution	5.1 Determine appropriate ***backup type*** to meet systems needs 5.2 Investigate current backup media options 5.3 Implement a backup solution 5.4 Demonstrate functionality of backup solution 5.5 Demonstrate restore of data from backup media 5.6 Implement a real time backup and data ***sync solution***
6. Monitor network performance	6.1 Determine available ***network*** performance ***monitoring tools*** 6.2 Implement network performance monitoring tools to monitor network 6.3 Produce report on network performance

Required Skills and Knowledge

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

Required skills

- communication skills to:
  - convey and clarify information
  - liaise with clients
- initiative and enterprise skills to apply precautions and required action to minimise, control or eliminate hazards that may exist during work activities
- literacy skills to:
  - develop and document network and data integrity processes
  - interpret and prepare technical documentation
  - record asset audit information
- planning skills to develop methods for maintaining network and data integrity
- problem-solving skills to:
  - apply solutions in networks, including systems management processes
  - deploy rapid solutions to problems involving management of network assets
- technical skills to apply current best practice to methodologies and technologies.

Required knowledge

- broad knowledge related to:
  - auditing and control of user access
  - asset tracking and auditing
  - backup, restore and rollback procedures
  - current antivirus solutions and techniques
  - system and network monitoring tools and related functions
- detailed knowledge of:
  - client organisation structure and business functionality
  - tools and applications required to manage network and data integrity
  - network management and disaster recovery processes.

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 user access control issues • use appropriate tools to conduct audit on system assets • implement and test antivirus solution • employ systems to negate environmental threats • demonstrate features of data backup, restore and system roll back • perform network monitoring using a variety of current standard tools • add network controls according to network and data integrity policies.
Context of and specific resources for assessment	Assessment must ensure access to: • site or prototype where network and data integrity strategies may be implemented and managed • use of network support tools currently used in industry • organisation's security policies, manufacturer recommendations and network and data integrity protection 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 policies related to:
	  • access control
	  • asset auditing
	  • antivirus protection
	  • fallback and backup strategies
	  • environmental and physical threats
	  • system monitoring
	• direct observation of candidate demonstrating management of

	disaster recovery and related strategies in a range of situations • review of documentation prepared by candidate to manage network and data integrity.
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 policies should include:	• data security • physical security • remote access • user logon.

Tools should include:	• hardware and software audit tools:
	  • MSINFO32
	  • DXdiag
	  • Microsoft Software Inventory Analyzer (MSIA)
	• E-Z Audit
	• hardware and software logs.

Assets may include:	• company information and branding • computers • data • personal information • servers.
Antivirus may include:	• AVG • EICAR (test virus string) • McAfee • Microsoft Security Essentials • Norton Antivirus or Endpoint • Trendmicro.
Environmental threats may include:	• earthquake • fire • flood • power failure, spike or surge • theft.
Backup type must include:	• copy • differential • folder and drive synchronisation • full and normal incremental • RAID.
Sync solution may include:	• Folder Sync • Shadowprotect

	• Yadis.
Network may include:	• internet • LAN • WAN • WLANs.
Monitoring tools may include:	• Microsoft server performance monitor • Windows network monitor • Windows performance monitor • Windows resource monitor • Windows task manager • Wireshark.

Unit Sector(s)

Networking