Australian Government

Department of Education, Employment and Workplace Relations

ICANWK520A Design IT system security controls

Release: 1

ICANWK520A Design IT system security controls

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 design the security controls that ensure an IT system is secure, both physically and legally. It involves developing the organisational policy and procedures for information security, process security, internet technology security, communications security, wireless security and overall physical security.

Application of the Unit

This unit applies to individuals in a range of information and communications technology (ICT) areas who are required to guarantee the security of IT systems.

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. Review organisational security policy and procedures	1.1 Review business environment to identify existing ***requirements***
	1.2 Determine organisational goals for legal and security requirements
	1.3 Verify security needs in a policy document
	1.4 Determine legislative impact on business domain
	1.5 Gather and document objective evidence on current ***security threats***
	1.6 Identify options for using internal and external expertise
	1.7 Establish and document a standard methodology for performing security tests
2. Develop security plan	2.1 Investigate theoretical attacks and threats on the business
	2.2 Evaluate risks and threats associated with the investigation
	2.3 Prioritise assessment results and write ***security policy***
	2.4 Document information related to attacks, threats, risks and controls in a ***security plan***
	2.5 Review the ***security strategy*** with security-approved key ***stakeholders***
	2.6 Integrate approved changes into business plan and ensure compliance with statutory requirements
3. Design controls to be incorporated into system	3.1 Implement controls in a procedurally organised manner to ensure minimum risk of security breach in line with ***organisational guidelines***
	3.2 Monitor each phase of the implementation to determine the impact on the business
	3.3 Take corrective action on system implementation breakdown
	3.4 Record implementation process
	3.5 Evaluate corrective actions for risk
	3.6 Plan ***risk assessment*** review process
	3.7 Take action to ensure confidentiality throughout all phases of design

Required Skills and Knowledge

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

Required skills

- analytical skills to undertake risk assessment of data-gathering techniques
- communication skills to manage group facilitation and presentation related to transferring and collecting information
- literacy skills to produce business reports
- planning and organisational skills to provide accurate and concise insights to possible security threats for all levels of staff, both technical and managerial
- problem-solving skills to identify and remedy evolving and complex security threat scenarios.

Required knowledge

- detailed knowledge of:
  - communications security, including human organisational interactions
  - how to conduct an information security risk assessment
  - internet technology security, including firewalls
  - physical security
  - security testing methods for performing security tests
  - wireless security
- overview knowledge of:
  - current industry-accepted security processes, including general features and capabilities of software and hardware solutions
  - ethics in IT
  - general features of specific security technology
  - privacy issues and legislation
  - process security for policy 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: • confirm sufficient knowledge of security products and organisational security policy • establish realistic ground rules for security product procedures • design security controls for a system • incorporate these into a security strategy.
Context of and specific resources for assessment	Assessment must ensure access to: • IT security assurance specifications • probability, frequency and severity of direct and indirect harm, loss or misuse of the IT system • risk analysis tools and methodologies • risks to the mission or business resulting from IT-related risks • security environment, which also includes the threats to security that are, or are held to be, present in the environment • security environment relating to laws and legislation, existing organisational security policies and organisational expertise • 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:
	• verbal or written questioning to assess knowledge of:
	  • layered security
	  • risk management
	  • security issues
	  • statutory requirements
	• review of documented security, including:
	  • policy
	  • plan
	  • strategy.

Guidance information	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where

for assessment	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.

Requirements may relate to:	• application • business • network • people in the organisation • system.
Security threats may include:	• by-pass actions • data tampering and manipulation • eavesdropping • impersonation • keyboard logging • local applications or local area network (LAN) connections • penetration • weaknesses in internet networks.

Security policy may relate to:	• audits and alerts
	• privacy
	• standards, including:
	  • archival
	  • backup
	  • network
	• theft
	• viruses.

Security plan may include:	• logical controls • physical controls • social controls.

Security strategy:	• may include:
	  • authentication
	  • authorisation and integrity
	  • privacy
	• usually forms part of the overall objectives of the organisation.

Stakeholders may include:	• development team • project team • sponsor

	• user.
Organisational guidelines may include:	• communication methods • content of emails • dispute resolution • document procedures • downloading information and accessing particular websites • financial control mechanisms • opening mail with attachments • personal use of emails and internet access • templates • virus risk.
Risk assessment may include:	• developing risk plans • developing scenarios • evaluating threats • following up • gathering information • identifying counter measures • identifying threats • ranking risk • reporting.

Unit Sector(s)

Networking