



Australian Government

Department of Education, Employment and Workplace Relations

ICANWK519A Design an IT security framework

Release: 1

ICANWK519A Design an IT security framework

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 evaluate IT security requirements for a new system and to plan for controls and contingencies.

Application of the Unit

This unit applies to individuals in senior roles in the networking area who are required to design security for new 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
<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. Research IT security requirements	1.1 Investigate and assemble statutory, commercial and application security requirements 1.2 Assess impact on the existing IT system 1.3 Identify additional IT security requirements 1.4 Document security requirements and forward to appropriate person for approval
2. Conduct risk analysis	2.1 Identify security threats and determine security specifications, taking into account the internal and external business environment 2.2 Develop controls and contingencies to alleviate security threats 2.3 Identify the costs associated with contingencies 2.4 Document and forward recommendations to appropriate person for approval
3. Develop IT security policy and operational procedures	3.1 Review feedback from appropriate person to determine how to manage security threats 3.2 Develop security policies based on the security strategy 3.3 Create and document work procedures based on the security policies 3.4 Document operating procedures and forward to appropriate person for approval 3.5 Take action to ensure confidentiality of client and user information 3.6 Apply statutory requirements to policy and procedures

Required Skills and Knowledge

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

Required skills

- analytical skills to:
 - analyse International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Australian Standards (AS) and other standards to establish and maintain a security framework
 - evaluate and present information across a range of technical and management functions
- communication skills to liaise with clients and users and articulate complex security scenarios in a clear and concise manner
- literacy skills to produce document procedures and recommendations
- numeracy skills to develop a broad plan, budget or strategy
- planning and organisational skills to:
 - contribute to the development of security policies, procedures and frameworks
 - facilitate presentations to groups
- research skills to:
 - identify the range of security risks
 - transfer and collect information.

Required knowledge

- detailed knowledge of:
 - accurate and in-depth knowledge of the client business domain
 - awareness of legislation relating to IT security
 - current industry-accepted hardware and software products, including broad knowledge of security features and capabilities
 - operating systems, including strengths and weaknesses over lifetime of product
 - sources of risk relating to IT security
- overview knowledge of privacy issues and legislation.

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: • explain legal obligations with respect to privacy and the specific application of security issues • design a security framework.
Context of and specific resources for assessment	Assessment must ensure access to: • information on the security environment, including: • laws or legislation • existing organisational security policies • organisational expertise • IT business specifications • IT security assurance specifications • possible security environment, which also includes the threats to security that are, or are held to be, present in the environment • risk analysis tools or methodologies 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 candidate's knowledge of: • security threats • current industry security trends • current legislation • review of candidate's documented security policies • evaluation of candidate's documented operating procedures.
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 requirements may include:	• customs • expertise • knowledge • laws • organisational security policies • security environment, which also includes: • authentication • encryption • hardware • passwords • policies • threats to security that are, or are held to be, present in the environment.
Appropriate person may include:	• authorised business representative • client • supervisor.
Security threats may include:	• data tampering and manipulation; impersonation, penetration and by-pass actions • eavesdropping • keyboard logging • local applications or LAN connections • weaknesses in internet networks.
Security policies may cover:	• theft • viruses • standards, including archival, backup and network • privacy • audits and alerts.
Security strategy may include:	• authentication • authorisation and integrity • privacy.
Client may include:	• employees • external organisations • individuals

	• internal departments.
User may include:	• department within the organisation • person within a department • third party.

Unit Sector(s)

Networking