



Australian Government

Department of Education, Employment and Workplace Relations

ICANWK614A Manage IT security

Release: 1

ICANWK614A Manage IT security

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 manage data security, enterprise continuity, incidents, networks and telecommunications security, system and application security.

Application of the Unit

Experienced security technical specialists, security analysts and security consultants apply the skills and knowledge in this unit.

Those with managerial responsibility undertake this role.

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. Manage enterprise security parameters	1.1 Determine and evaluate parameters that affect enterprise security to establish benchmark 1.2 Review security classification and data management policies and guidance for relevance and update if required 1.3 Plan and coordinate an effective enterprise continuity of operations (COOP) program and organisational structure for critical business continuity 1.4 Develop a plan to address factors to manage the risks of the enterprise 1.5 Integrate and evaluate risk management concepts into operational activities with related contingency planning activities using an enterprise COOP performance measurement program 1.6 Evaluate and assess security incidents to establish an effective incident-management program for the enterprise 1.7 Manage the coordination between related security teams for effective incident management processes and procedures
2. Manage networks and telecommunications security	2.1 Develop a network security and telecommunications program in line with enterprise policy and security goals 2.2 Manage the necessary resources to integrate network security and telecommunications program activities with technical support, security administration and incident response activities in a secure network 2.3 Establish effective communications protocols between the network security and telecommunications team and related security teams to manage the risks 2.4 Establish a performance measurement program to evaluate the security effectiveness of the integrated network security and telecommunications network 2.5 Ensure enterprise compliance with applicable network-based documents and that network-based audits and management reviews are conducted to implement process improvement
3. Implement and document enhancements	3.1 Implement appropriate changes and improvement actions as required and evaluate effectiveness of enhancements 3.2 Produce and table documentation for audit tracking

Required Skills and Knowledge

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

Required skills

- communication skills to:
 - negotiate with stakeholders and team members using a range of communication styles to suit different audiences and purposes
 - respond to diversity, including gender and disability
- literacy skills to:
 - access and prepare information electronically or in hard copy
 - write recommendations and prepare reports requiring precision of expression
- numeracy skills to manage finances
- planning and organisational skills to:
 - lead and mentor people to achieve project outcomes
 - maintain commitment of stakeholders and project teams
- problem-solving skills to apply ethical decision making when problem solving
- safety awareness skills to apply workplace safety procedures in line with requirements
- technical skills to:
 - apply risk management techniques, including risk sharing and transfer
 - use management tools applicable to complex activities.

Required knowledge

- business and commercial issues related to the management of IT security
- COOP
- cost schedule control systems to handle potential budget blow-outs
- critical analysis in a management context
- legislation, organisational or jurisdictional policy and procedures that may impact on management:
 - budgetary framework
 - codes of ethics and conduct
 - equal employment opportunity, equity and diversity principles
 - financial management requirements
 - governance requirements
 - human resources
 - OHS and environment requirements
 - procurement guidelines
 - public relations
 - quality standards
 - risk management
- management specifications and objectives
- management systems
- management tools and techniques suited to a range of complex projects activities

- organisational and political context
- systems development life cycle (SDLC).

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: • direct contingency planning, operations and programs to manage risk • establish the IT system and application security engineering program • manage the necessary resources to establish and maintain an effective network security and telecommunications program • specify policy and coordinate review.
Context of and specific resources for assessment	Assessment must ensure access to: • IT business specifications • IT security assurance specifications • management-related scenarios • a security environment, including the threats to security that are, or are held to be, present in the environment • information on the security environment, including: • laws or legislation • existing organisational security policies • organisational expertise • use of risk analysis tools and methodologies currently used in industry • 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: • direct observation of candidate managing networks and telecommunications security • direct observation of candidate managing IT security incidents • verbal or written questioning to assess candidate's knowledge of organisational policy and procedures that impact on IT security • review of documentation prepared by candidate, including contingency planning and programs to manage risk.

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.

Parameters may include:	• applications security • data security • enterprise continuity • incidents • system security.
Continuity of operations may include:	• COOP plan execution • COOP plan revision and updating • COOP program implementation • identification of functional requirements: • mission impact analysis • mitigation strategies and plan • risk assessment • plan design and development • project initiation • training, testing and drills.
Factors may include:	• business continuity and recovery • contingency planning • contingency planning and programs • disaster recovery • emergency delegations of authority • orders of succession for key positions • scope of the enterprise COOP program • security incidence • staffing model.
Security incidents may include:	• event causing interruption to reduction in quality of service • failure or error in IT infrastructure • illegal data harvesting • illegal downloads • malware: • adware • computer viruses • phishing • spyware

	• trojans • worms • security breach • service not available • system down • tampering.
Incident-management program may include:	• ensuring that the best possible levels of service quality and availability are maintained • establishing effective and responsive response team • evaluation of security incidents • improvement of incident management processes and procedures • minimisation of the impact on business operations • restoration of normal service operation as quickly as possible • sourcing effective security tools.
Related security teams may include:	• incident response team • security administration: • external stakeholders: • law enforcement agencies • public relations professionals • vendors • internal stakeholders: • finance • HR • legal department • procurement • technical support.
Resources may include:	• equipment • financial • network security and telecommunications personnel • training.
Applicable network-based documents may include:	• directives • laws • policies • procedures • regulations • standards.
Documentation may include:	• applicable network-based documents • audits and management reviews • communications protocols • contingency plans and activities

	• evaluation reports • incident management program, processes and procedures • management reports • network security and telecommunications program • performance measurement program • reviews and improvements records • security classification and data management policies • security incidence records.
--	---

Unit Sector(s)

Networking