Australian Government
Department of Education, Employment and Workplace Relations

ICANWK513A Manage system security

Release: 1

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

ICANWK513A Manage system security

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 on an operational system.

Application of the Unit

This unit applies to middle managers such as information security managers or security analysts, responsible for implementing and managing the organisation's security management system. They provide technical advice, guidance and leadership in resolution of specified problems and the role may involve responsibility for others.

The role also involves leading development of strategic reviews, and determining security threats and implementing controls to mitigate risk. Related tasks include planning and budgeting.

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. Analyse threats to system	1.1 Evaluate the organisation's ***system*** and verify that it meets enterprise guidelines and policies 1.2 Conduct risk analysis on system and document outcomes 1.3 Evaluate ***threats*** to the system and document findings 1.4 Compile and document human interactions with system
2. Determine risk category	2.1 Conduct a risk assessment on the system and categorise risks 2.2 Conduct a risk assessment on human operations and interactions with the system and categorise risks 2.3 Match risk plans to risk categories 2.4 Determine and plan resources by risk categories
3. Identify appropriate controls	3.1 Devise and put in place effective controls to manage risk 3.2 Design policies and procedures to cover user access of the system 3.3 Conduct training in the use of system-related policies and procedures 3.4 Monitor high-risk categories at specified periods 3.5 Categorise and record system breakdowns
4. Include controls in the system	4.1 Develop ***security plan*** and procedures to include in management system 4.2 Develop ***security*** recovery plan 4.3 Implement system controls to reduce risks in human interaction with the system
5. Monitor system tools and procedures	5.1 Review and monitor risks and controls using a management review process 5.2 Review risk analysis process based on security benchmarks from vendors, security specialists and organisational reviews 5.3 Plan to re-evaluate system and identify new threats and risks

Required Skills and Knowledge

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

Required skills

- analytical skills to evaluate system security
- communication skills to communicate clear concepts and solutions to complex issues
- literacy skills to write reports
- planning skills to:
  - develop a security plan
  - develop a security recovery plan
- problem-solving skills to:
  - manage unpredictable problems involving participation in group solutions and analysis
  - resolve issues for a mixed mode environment of people and systems processes
- research skills to identify, analyse and evaluate weaknesses and strengths of security systems
- technical skills to use systems security methodologies and technologies.

Required knowledge

- broad knowledge of general features of specific security technology
- risk analysis techniques, with broad knowledge of their general features, and depth in security procedures
- details of the client organisation
- systems management and process control in relation to security
- systems technologies, with broad knowledge of their general features and capabilities.

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: • implement and manage security functions on a system • conduct risk assessment • set up effective controls to manage risk • develop security plan and security recovery plan • monitor risks and controls • review risk-analysis process.
Context of and specific resources for assessment	Assessment must ensure access to: • site where system security may be implemented and managed • use of utility tools currently used in industry • organisational security policies • manufacturer recommendations • security standards • 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 security risks and options available in the operating environment • direct observation of candidate demonstrating management of system security in a range of complex situations • review of documentation prepared by candidate to manage system security.
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.

System may include:	• application service provider • applications • databases • gateways • internet service provider (ISP) • operating system • servers • wireless network access policies using mobile devices.
Threats may include:	• denial of service and by-pass • eavesdropping • hackers • impersonation • manipulation • penetration • viruses.
Security plan may include:	• alerts relating directly to the security objectives of the organisation • audits • privacy • standards: • archival • backup • network • theft • viruses.
Security may include:	• AAA • Diameter • IPSec • LEAP • PKM • smart cards • SSL • tokens • WEP

	• WPA.

Unit Sector(s)

Networking