



Australian Government

Department of Education, Employment and Workplace Relations

ICANWK510A Develop, implement and evaluate system and application security

Release: 1

ICANWK510A Develop, implement and evaluate system and application 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 develop, implement and evaluate information security in an information technology (IT) system or application during the system development life cycle (SDLC) prior to the operations and maintenance phase.

Application of the Unit

This unit applies to network managers who are required to handle system and application security, from the development phase through implementation to evaluation.

The practice of these protocols ensures that the operation of IT systems and software does not present undue risk to the enterprise and its information assets. This objective is accomplished through risk assessment; risk mitigation; security control selection, implementation and evaluation; and software security standards compliance.

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. Develop system and application security	1.1 Specify enterprise and IT system or application security policies 1.2 Specify security requirements for the IT system or application 1.3 Author an IT system or application security plan according to the enterprise and IT system or application security policies 1.4 Identify standards against which to engineer the IT system or application 1.5 Specify criteria for performing risk-based audits against the IT system or application 1.6 Develop processes and procedures to mitigate the introduction of vulnerabilities during the engineering process 1.7 Integrate applicable information security requirements, controls, processes, and procedures into IT system and application design specifications according to established requirements
2. Implement system and application security	2.1 Execute enterprise and IT system or application security policies 2.2 Apply and verify compliance with identified standards against which to engineer the IT system or application 2.3 Perform processes and procedures to mitigate the introduction of vulnerabilities during the engineering process 2.4 Perform secure configuration management practices 2.5 Validate that the engineered IT system and application security controls meet the specified requirements 2.6 Re-engineer security controls to mitigate vulnerabilities identified during the operations phase 2.7 Ensure integration of information security practices throughout the SDLC process 2.8 Document IT system or application security controls addressed within the system 2.9 Practise secure coding practices
3. Evaluate system and application security	3.1 Review new and existing risk management technologies to achieve an optimal enterprise risk posture 3.2 Review new and existing IT security technologies to support secure engineering across the SDLC phases 3.3 Continually assess the effectiveness of the

	information-system controls based on risk-management practices and procedures 3.4 Assess and evaluate system compliance with corporate policies and architectures 3.5 Assess system maturation and readiness for promotion to the production stage 3.6 Collect lessons learned from integration of information security into the SDLC and use to identify improvement actions 3.7 Collect, analyse and report performance measures
--	---

Required Skills and Knowledge

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

Required skills

- analytical skills to translate requirements from problem space to machine space
- initiative and enterprise skills to write security plans
- literacy skills to write technical documentation
- planning and organisational skills to ensure that the plan is implemented
- problem-solving skills to ensure that security areas are covered
- technical skills to:
 - debug code
 - read and interpret program specifications
 - write code.

Required knowledge

- range of programming languages, including those used by the organisation
- best practice in application of language syntax rules
- data structures
- graphical user interface (GUI) interfaces
- small-size application development.

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: • author an IT system or application security plan • apply and verify compliance with the identified standards • practise secure coding practices • assess and evaluate system compliance.
Context of and specific resources for assessment	Assessment must ensure access to: • IT business specifications • information on the security environment, including laws and legislation, existing organisational security policies, organisational expertise and knowledge • possible security environment, which also includes the threats to security that are, or are held to be, present in the environment • risk analysis tools and methodologies • IT security assurance specifications • application and system scenarios • 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 security issues regarding the system or application and security standards • review of system or application security plan prepared by candidate • review of amended system or security plan after evaluation prepared by candidate • observation of candidate carrying out work to ensure the plan complies with security standards.
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.

<i>IT system or application</i> may include:	• applications • collection of programs • integrated suite of programs • operating system and system software • program.
<i>Vulnerabilities</i> may include:	• buffer overflows • errors in application or system • poor design • trapdoors • undefined or undocumented code • undefined variables • untested code.
<i>Established requirements</i> may include:	• laws • policies • regulations • standards.

Unit Sector(s)

Networking