



Australian Government

ICTNWK510 Develop, implement and evaluate system and application security

Release: 1

ICTNWK510 Develop, implement and evaluate system and application security

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Application

This unit describes the skills and knowledge required to develop, implement and evaluate information security in an information and communications technology (ICT) system or application during the system development life cycle (SDLC), prior to the operations and maintenance phase.

It applies to individuals with excellent information and communications technology (ICT) expertise who are working as network managers and are required to handle system and application security from the development phase through implementation to evaluation.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Networking

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Develop system and application security	1.1 Identify enterprise ICT system or application security policies 1.2 Identify security requirements for the ICT system or application 1.3 Write an ICT system or application security plan according to the enterprise and ICT system or application security policies 1.4 Identify standards against which to engineer the ICT system or application

ELEMENT	PERFORMANCE CRITERIA
	1.5 Identify criteria for performing risk based audits against the ICT 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 ICT system and application design specifications according to established requirements
2. Implement system and application security	2.1 Execute enterprise and ICT system or application security policies 2.2 Apply and verify compliance with identified standards against which to engineer the ICT 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 ICT 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 ICT system or application security controls addressed within the system 2.9 Practise secure coding
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 ICT security technologies to support secure engineering across the SDLC phases 3.3 Continually assess 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

Foundation Skills

This section describes language, literacy, numeracy and employment skills incorporated in the performance criteria that are required for competent performance.

Skill	Performance Criteria	Description
Learning	3.6	Builds on prior knowledge and experience to clarify, extend understanding and contribute to ongoing organisational improvement
Reading	1.1-1.4, 1.7, 2.2, 3.4, 3.7	Gathers, interprets and analyses technical and regulatory information to determine requirements according to client needs
Writing	1.3, 2.8, 3.7	Uses factual information and industry related terminology to produce workplace documents
Oral Communication	3.7	- Conveys information about performance measures clearly, using specific and relevant language suitable to audience - Uses listening and questioning techniques to confirm understanding
Navigate the world of work	1.1, 1.3, 1.7	Takes full responsibility for identifying and considering relevant policies and legislative requirements in the development of system security processes
Get the work done	1.5-1.7, 2.1, 2.3-2.7, 2.9, 3.1-3.5	- Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and reduce risks - Uses digital tools to access and organise complex data and analyse multiple sources of information for strategic purposes - Is acutely aware of the importance of understanding, monitoring and controlling access to digitally stored and transmitted information - Uses a combination of formal and logical planning processes and an increasingly intuitive understanding of context to identify relevant information and risks - Makes a range of critical decisions in relatively complex situations, taking a range of constraints into account

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTNWK510 Develop, implement and evaluate system and application security	ICANWK510A Develop, implement and evaluate system and application security	Updated to meet Standards for Training Packages	Equivalent unit

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for ICTNWK510 Develop, implement and evaluate system and application security

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Performance Evidence

Evidence of the ability to:

- create an information and communications technology (ICT) system or application security plan
- implement system and application security
- apply and verify compliance with the identified standards
- practise secure coding practices
- assess and evaluate system compliance.

Note: If a specific volume or frequency is not stated, then evidence must be provided at least once.

Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- summarise a range of programming languages, including those used by the organisation
- summarise best practice in application of language syntax rules
- explain data structures
- outline graphical user interfaces (GUIs)
- summarise small-size application development
- identify and summarise the legislation, regulations and codes of practice that impact on network security
- describe the risk assessment process required in evaluating system vulnerabilities, including:
 - risk mitigation
 - security control selection
 - implementation and evaluation process
 - software security standards compliance.

Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the network industry, and include access to:

- ICT 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
- ICT security assurance specifications
- application and system scenarios.

Assessors must satisfy NVR/AQTF assessor requirements.

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>