



Australian Government

ICTNWK520 Design ICT system security controls

Release: 1

ICTNWK520 Design ICT system security controls

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 design the security controls that ensure an information and communications technology (ICT) system is both physically and legally secure.

It applies to individuals in a range of ICT areas who are required to guarantee the security of ICT systems.

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. Review organisational security policy and procedures	1.1 Review business environment to identify existing requirements 1.2 Determine organisational goals for legal and security requirements 1.3 Verify security needs in a policy document 1.4 Determine legislative impact on business domain 1.5 Gather and document objective evidence on current security threats 1.6 Identify options for using internal and external expertise 1.7 Establish and document a standard methodology for

ELEMENT	PERFORMANCE CRITERIA
	performing security tests
2. Develop security plan	2.1 Investigate theoretical attacks and threats on the business 2.2 Evaluate risks and threats associated with the investigation 2.3 Prioritise assessment results and write security policy 2.4 Document information related to attacks, threats, risks and controls in a security plan 2.5 Review the security strategy with security approved key stakeholders 2.6 Integrate approved changes into business plan and ensure compliance with statutory requirements
3. Design controls to be incorporated into system	3.1 Implement controls in a procedurally organised manner to ensure minimum risk of security breach in line with organisational guidelines 3.2 Monitor each phase of the implementation to determine the impact on the business 3.3 Take corrective action on system implementation breakdown 3.4 Record implementation process 3.5 Evaluate corrective actions for risk 3.6 Plan risk assessment review process 3.7 Take action to ensure confidentiality throughout all phases of design

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
Reading	1.1, 1.2, 1.5, 3.1	Recognises and interprets legislative, organisational and technical material to determine job requirements
Writing	1.3, 1.5, 1.7, 2.3, 2.4, 2.6, 3.4	Develops a broad range of business reports for a specific audience, using clear and detailed language to convey explicit information, requirements and

		recommendations
Oral Communication	2.5	• Uses appropriate, detailed and clear language to address personnel and disseminate information in a group environment • Uses listening and questioning skills to confirm understanding for requirements, and participates in a verbal exchange of ideas/solutions
Navigate the world of work	1.2, 1.4, 2.6	• Keeps abreast of legislative or regulatory requirements relevant to own role and considers implications of any changes when planning and undertaking work
Get the work done	1.5, 1.6, 2.1-2.3, 3.1-3.3, 3.5-3.7	• Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world • Is acutely aware of the importance of understanding, monitoring and controlling access to digitally stored and transmitted information • May operate from a broad conceptual plan, developing the operational detail in stages, regularly reviewing priorities and performance during implementation, and identifying and addressing issues • Monitors outcomes of decisions, considering results from a range of perspectives and identifying key concepts and principles that may be adaptable in the future

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTNWK520 Design ICT system security controls	ICANWK520A Design IT system security controls	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 ICTNWK520 Design ICT system security controls

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:

- review organisational security policies and procedures
- establish realistic security procedures
- design security plan and controls for a system
- develop a security control strategy
- oversee the implementation and evaluation of the strategy.

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:

- describe communications security, including human organisational interactions
- describe how to conduct an information security risk assessment
- identify and summarise internet security technologies and processes, including:
 - firewalls
 - physical security
 - security testing methods for performing security tests
 - wireless security
 - security threats
 - the impact of security policies, plans and strategies
 - general features of specific security technology
 - risk assessment
- describe current industry accepted security processes, including general features and capabilities of software and hardware solutions

- outline the legal and ethical standards expected when considering security controls, including:
 - ethics in information and communications technology (ICT)
 - privacy issues
 - legislation
- summarise the need for developing organisational guidelines, processes, policies and procedures.

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 security assurance specifications
- probability, frequency and severity of direct and indirect harm, loss or misuse of the ICT system
- risk analysis tools and methodologies
- an ICT environment in which there are security risks
- legislation, regulations and standards relating to security
- existing organisational security policies
- organisational expertise.

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>