



Australian Government

ICTNWK614 Manage ICT security

Release: 1

ICTNWK614 Manage ICT 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 manage data security, enterprise continuity, incidents, networks and telecommunications security, and system and application security.

It applies to individuals with managerial responsibility and advanced information and communications technology (ICT) skills who are working as experienced security technical specialists, security analysts and security consultants.

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. 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 procedures 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

ELEMENT	PERFORMANCE CRITERIA
	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

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, 1.6, 2.1, 2.5	Identifies, analyses and evaluates complex text to determine regulatory and business requirements
Writing	1.2, 1.4, 1.6, 2.1,	Develops a broad range of operational material,

	2.3, 2.4, 3.2	including recommendations and reports for a specific audience, using clear and detailed language to convey explicit information, requirements and recommendations
Numeracy	2.2	• Uses mathematical formulas and calculations to estimate and plan project costs
Navigate the world of work	1.2, 2.3-2.5	• Develops and implements strategies that ensure organisational policies, procedures and regulatory requirements are being met • Monitors and reviews the organisation's policies, procedures and adherence to legislative requirements in order to implement and manage change
Interact with others	1.7, 2.2-2.5, 3.1	• Selects, implements and manipulates communications systems, processes and practices for maximum impact • Influences and fosters a collaborative culture, facilitating a sense of commitment and workplace cohesion • Understands diversity and seeks to integrate diversity into the work context, for managing change, making decisions and achieving shared outcomes
Get the work done	1.3-1.6, 2.1- 2.5, 3.1	• Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and understand the uses and potential of new technology • Is acutely aware of the importance of understanding, monitoring and controlling access to digitally stored and transmitted information • Uses a mix of intuitive and formal processes to identify key information and issues, evaluate alternative strategies, anticipate consequences and consider implementation issues and contingencies • When dealing with complex issues, may use intuition to identify the general problem area, switching to analytical processes to generate possible solutions, depending on differing operational contingencies, risk situations and environments • Monitors outcomes of decisions, considering results from a range of perspectives and identifying key concepts and principles that may be adaptable to future situations

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTNWK614 Manage ICT security	ICANWK614A Manage IT security	Updated to meet Standards for Training Packages. Minor change to competency title.	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 ICTNWK614 Manage ICT 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:

- direct contingency planning, operations and programs to manage risk
- establish the information and communications technology (ICT) 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.

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:

- explain business and commercial issues related to the management of ICT security
- explain continuity of operations (COOP)
- clarify critical analysis in a management context
- outline management specifications and objectives
- describe different management styles and systems
- explain systems development life cycle (SDLC).

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 networking industry, and include access to:

- ICT business specifications
- ICT 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.

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>