



Australian Government

ICTICT424 Address cyber security requirements

Release: 1

ICTICT424 Address cyber security requirements

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 4.0.

Application

This unit describes the skills and knowledge required to determine the cyber security requirements of an organisation and use a range of resources to protect valuable assets.

This unit applies to individuals who are required to participate in the identification and implementation of cyber security controls.

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

Unit Sector

General ICT

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. Analyse cyber security requirements	1.1 Identify and document valuable assets to create register of valuable assets 1.2 Perform threat and risk assessment on valuable assets register to identify and document cyber security requirements 1.3 Review current cyber security controls against the cyber security requirements to identify cyber security gaps
2. Select and implement cyber security controls	2.1 Identify cyber security controls which address cyber security gaps 2.2 Determine specific cyber security controls to address cyber security gaps against the organisation's risk appetite 2.3 Seek feedback from organisational representative and agree on

	cyber security controls to implement 2.4 Implement, test and document agreed cyber security controls to address cyber security gaps 2.5 Seek feedback from organisational representative to identify discrepancies between cyber security controls and cyber security requirements
3. Maintain and improve security controls	3.1 Determine currency of valuable assets register to identify new valuable assets and changed threats and risks 3.2 Identify, determine, and agree on cyber security controls to address new cyber security gaps 3.3 Implement and document new and modified cyber security controls to address cyber security gaps

Foundation Skills

This section describes those language, literacy, numeracy and employment skills that are essential to performance but not explicit in the performance criteria.

Skill	Description
Learning	Identifies, plans and implements strategies to manage gaps in cyber security knowledge
Reading	- Analyses and consolidates information and data from sources, against defined criteria and requirements, and checks for accuracy and completeness - Recognises and interprets textual information to determine specific information about security incidents
Writing	Develops material for a specific audience, using clear and detailed language in order to convey explicit information
Oral Communication	- Articulates information clearly, using specific and relevant language suitable to audience to convey recommendations and provide verbal reports - Uses listening and questioning techniques to confirm understanding
Numeracy	Extracts and evaluates the mathematical information embedded in a range of tasks and texts
Navigate the world of work	- Accepts responsibility and ownership for the task and makes decisions on completion parameters and the need for coordination with others - Takes personal responsibility for following explicit and implicit policies, procedures and legislative requirements
Interact with	Selects form, channel and mode of communication for a specific purpose relevant to own role

others	
Get the work done	- Plans strategic priorities and outcomes within a flexible, efficient and effective context, in a diverse environment exposed to competing demands - Gathers and analyses data, and seeks feedback, to improve plans and processes - Makes decisions in a complex and diverse environment, using input from a range of sources - Explores and incubates new ideas through unconstrained analysis and critical thinking, to develop and improve the organisation's controls

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTICT424 Address cyber security requirements	N/A	New unit	No equivalent unit

Links

Companion Volume Implementation Guides are available from VETNet - <https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for ICTICT424 Address cyber security requirements

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 4.0.

Performance Evidence

The candidate must demonstrate the ability to complete the tasks outlined in the elements and performance criteria of this unit; including evidence of the ability to:

- For two difference cyber security requirements:
 - analyse cyber security requirements to protect valuable assets
 - determine threats and risks based on current controls and requirements
 - identify and apply controls to protect valuable assets
 - identify improvements to cyber security controls
 -

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements and performance criteria of this unit. This includes:

- Common cyber security threats and risks
- Common cyber security controls, key features, and associated advantages and disadvantages
- Cyber security control implementation processes and procedures
- Industry standards relevant to cyber security
- Testing procedures and processes
- Legislative and regulatory requirements relevant to cyber security
- Approaches to performing cyber security threat and risk assessment
-

Assessment Conditions

Skills in this unit must be demonstrated in a workplace or simulated environment where the conditions are typical of those in an ICT working environment or workplace. This includes access to:

- Organisational representative

- Organisational cyber security requirements
- Specifications of existing cyber security controls
- Information on organisational assets, both valuable and non-valuable
- Software required for performing cyber security threat and risk assessments

Assessors of this unit must satisfy the assessor requirements in applicable vocational education and training legislation, frameworks and/or standards.

Links

Companion Volume Implementation Guides are available from VETNet -

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