



Australian Government

ICTCYS610 Protect critical infrastructure for organisations

Release: 1

ICTCYS610 Protect critical infrastructure for organisations

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Application

This unit describes the skills and knowledge required to analyse an organisation's critical cyber operations and develop and implement a critical protections strategy that addresses the needs of the organisation.

It applies to those who work as senior network and server administrators, cyber security analysts, security engineers, network engineers other cyber security related roles and are responsible for cyber security activities, including researching, developing and implementing protection strategies.

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

Unit Sector

Cyber security

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. Research critical infrastructure need for an organisation	1.1 Research organisation's need for critical infrastructure protection and document findings according to organisational requirements 1.2 Analyse organisation's existing critical infrastructure protection plan 1.3 Determine effectiveness and alignment of existing plan to organisational requirements 1.4 Identify operational systems, critical assets, segmentation and legislative requirements 1.5 Determine level of protection, vulnerability, risk and

ELEMENT	PERFORMANCE CRITERIA
	mitigation according to organisational requirements
2. Develop protection strategy	2.1 Consolidate research findings and map critical processes according to organisational requirements 2.2 Develop and document critical infrastructure protection plan according to organisational policies and procedures 2.3 Submit protection plan to required personnel and seek and respond to feedback
3. Implement protection strategy	3.1 Backup data according to organisational policies and procedures 3.2 Secure devices according to protection plan and technical requirements 3.3 Implement network segmentation according to protection plan and technical requirements 3.4 Apply software patches according to technical requirements 3.5 Implement additional protection plan requirements and asset management processes
4. Test implementation outcomes	4.1 Test deployment of protection plan according to organisational policies and procedures 4.2 Obtain and analyse results according to organisational policies and procedures 4.3 Determine and document additional protection methods for critical infrastructure protection 4.4 Submit documentation to required personnel and seek and respond to feedback

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
Reading	Identifies technical, manufacturer and organisational from documentation to determine and confirm job requirements
Writing	Prepares complex workplace documentation detailing processes and outcomes using required structure, layout and required language
Planning and organising	Develops the operational detail in stages, regularly reviewing priorities and performance during strategy development and implementation, and identifies and addresses issues challenges as

SKILL	DESCRIPTION
	they arise
Problem solving	Identifies context to recognise anomalies and subtle deviations to normal expectations, focusing attention and remedying problems as they arise
Self-management	Takes full responsibility for identifying and considering organisational protocols and requirements
Technology	Identifies principles, concepts, language and practices associated with the digital and cyber world

Unit Mapping Information

No equivalent unit. New unit.

Links

Companion Volume Implementation Guide is found on VETNet -

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

Assessment Requirements for ICTCYS610 Protect critical infrastructure for organisations

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Performance Evidence

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

- research, develop, implement and test an organisation's critical protection infrastructure plan.

In the course of the above, the candidate must:

- analyse operating environment
- document processes and outcomes.

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including knowledge of:

- critical infrastructure sectors and assets
- cyber security methodologies required to protect infrastructure for organisations
- legislative requirements applicable to researching, analysing and developing critical infrastructure protection policies.

Assessment Conditions

Skills in this unit must be demonstrated in a workplace or simulated environment where the conditions are typical of those in a working environment in this industry.

This includes access to:

- required hardware, software and components
- organisational operating environments, networks and systems
- organisational style guides required for presenting documented processes, procedures and findings.

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

Links

Companion Volume Implementation Guide is found on VETNet -

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