



Australian Government

ICTCYS602 Implement cyber security operations

Release: 1

ICTCYS602 Implement cyber security operations

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 research, implement and monitor cyber security operations.

It applies to those in cyber security roles including network and server administrators and cyber security architects working in security operations within an organisation.

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. Assess organisational cyber security operations	1.1 Identify existing organisational cyber security operations 1.2 Identify organisational cyber security requirements 1.3 Analyse effectiveness of organisations existing cyber operations against organisational requirements 1.4 Document findings of analysis according to organisational requirements
2. Determine and document organisational operations	2.1 Determine and document required updates to existing organisational operation 2.2 Determine and document service disruption and task requirements for implementing cyber operations 2.3 Distribute document to required personnel in preparation for required implementation

3. Implement organisational cyber security operations	3.1 Initiate implementation of cyber security operations according to task requirements 3.2 Implement required operational and analytical processes 3.3 Implement personnel requirements according to task requirements 3.4 Implement incident reporting and escalating procedures 3.5 Implement required hardware and software support requirements
4. Test and finalise	4.1 Test operational processes of cyber security operations and determine alignment to requirements 4.2 Analyse performance and document required operational changes 4.3 Update cyber security operations according to analysis results and determine required alignment to task requirements 4.4 Review final cyber security strategy and document and lodge document according to organisational procedures

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	Interprets information from technical, manufacturer and organisational documentation to determine and confirm job requirements
Writing	Prepares complex workplace documentation detailing analysis, findings and recommendations using required structure, layout and technical programming language
Planning and organising	Develops information security strategies using logical sequencing
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 ICTCYS602 Implement cyber security operations

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:

- plan, implement and test cyber security operations on at least one occasion.

In the course of the above, the candidate must:

- establish existing operational environment within organisation
- analyse effectiveness of existing operations.

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:

- inherent requirements of cyber security operations environment
- organisational procedures applicable to implementing cyber security operations, including:
- documentation processes
- establishing requirements and features of cyber security operations strategies
- testing methodologies.

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:

- software and its components applicable to implementing cyber security operations
- network security providers and solutions required to implement cyber security operations
- site server

- standards for Cyber security ISO/IEC 27000 series, Information security management systems standards
- application and user security technologies.

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>