



Australian Government

ICTCYS612 Design and implement virtualised cyber security infrastructure for organisations

Release: 1

ICTCYS612 Design and implement virtualised cyber security 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 research, design, implement and test virtualised cyber security infrastructure in a small to medium sized organisation.

It applies to those who work in senior systems administrator roles including, network engineers and systems engineers, and are responsible for the design and implementation of virtualised cyber security infrastructures.

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. Prepare to design infrastructure	1.1 Analyse organisation's operations to determine cyber security needs 1.2 Research and identify industry standard network security options and security technologies 1.3 Determine data types, security levels, mission-critical network servers and secure boundary requirements
2. Design and plan infrastructure	2.1 Design and document infrastructure requirements according to organisational requirements 2.2 Determine and document implementation plan and timeframes 2.3 Obtain tools, network access and data according to

	organisational requirements 2.4 Plan and document network security monitoring strategy according to organisational requirements 2.5 Distribute documentation to required personnel and seek and respond to feedback
3. Implement infrastructure	3.1 Establish and create network boundaries according to infrastructure plan requirements 3.2 Implement network and server technologies according to infrastructure plan requirements 3.3 Implement user security technologies according to infrastructure plan requirements 3.4 Set security levels and user access according to organisational requirements 3.5 Establish network security monitoring strategy according to plan requirements
4. Test infrastructure	4.1 Test deployment of security infrastructure and its components according to technical specifications and infrastructure plan requirements 4.2 Obtain and analyse test results, logs and user feedback 4.3 Adjust implemented technologies according to organisational requirements and user 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
Learning	Monitors outcomes of decisions, considering results and identifying key concepts and principles that may be adaptable in the future
Oral communication	Uses listening and questioning techniques to articulate information and requirements using industry standard technical language intended for audience and environment
Reading	Interprets technical, manufacturer and organisational documentation to determine and confirm job requirements
Writing	Prepares complex workplace documentation detailing processes and findings using required structure, layout and required language
Planning and organising	Develops the operational detail of an activity in stages, regularly reviewing priorities and performance during implementation, and identifying and addressing issues

SKILL	DESCRIPTION
Problem solving	• Uses a developed understanding of context to recognise anomalies and subtle deviations to normal expectations, focusing attention and remedying problems as they arise
Self-management	• Takes responsibility for identifying and considering organisational protocols and requirements • Uses systematic processes, setting goals, gathering required information and identifying and evaluating options against agreed criteria
Technology	• Demonstrates an understanding of principles, concepts, language and practices associated with the digital 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 ICTCYS612 Design and implement virtualised cyber security 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:

- design and implement cyber security infrastructure and review results against organisational needs on at least two different occasions.

In the course of the above, the candidate must:

- identify an organisation's vulnerabilities, cyber security needs and data protection requirements
- document findings, plan and processes.

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:

- features and implementation methodologies of cyber security
- cyber security infrastructure features including:
 - application security
 - business continuity planning
 - disaster recovery planning
 - operational security (OPSEC)
 - threat vectors
- organisational business processes and applicable cyber security requirements design and implementation
- organisational procedures applicable to designing and implementing cybersecurity infrastructure, including:
 - documenting established requirements, risks and work performed
 - establishing requirements and features of cyber security infrastructure
 - establishing maintenance and alert processes

- testing methods and procedures
- security risks, and tolerance of risk in an organisation
- industry standard cyber security providers
- industry standards and regulations applicable to implementing cyber security infrastructure in an organisation
- organisation, infrastructure and cyber security requirements.

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:

- hardware, software and its components required in the design and implementation of cyber security infrastructure
- an organisation's operational details required for determining cyber security requirements
- application and user security technologies required for the design and implementation of cyber security infrastructure
- industry standard cyber security providers.

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>