



Australian Government

Assessment Requirements for ICTCYS615 Detect and respond to cyber security insider risks and threats

Release: 1

Assessment Requirements for ICTCYS615 Detect and respond to cyber security insider risks and threats

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 7.2.

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:

- detect and respond to at least three different insider cyber security risks and/or threats in an organisation or workplace context.

In the course of the above, the candidate must:

- select and configure a cyber security insider risk and threat detection tool suited to the detected risk or threat
- report on detected insider cyber security risks and threats.

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:

- key requirements of legislation, codes, regulations, standards and security arrangements relating to detecting and responding to cyber security insider risks and threats
- key security controls
- organisational policies and procedures applicable to cyber security insider risk and threat detection and response, including those for:
 - assessing impact and rectifying damage imposed by insider risks and threats
 - containing risks and threats, including disabling user access and maintaining custody chain
 - determining nature of detected risks and threats
 - determining user identification protocols
 - identifying location of sensitive data
 - reporting risks and threats to required personnel
- types of cyber security insider risks and threats, including:

- careless insiders
- compromised insiders
- expired users with valid credentials
- malicious insiders
- misinformed insiders
- key intentional and unintentional cyber security insider risks and threats
- key behavioural patterns that indicate cyber security insider risks and threats
- causes and sources of cyber security insider risks and threats
- strengths and limitations of cyber security insider risk and threat detection methodologies and tools
- key information in data logs, including server, network and firewall information
- key features of different data classifications, including:
 - classified
 - confidential
 - private
 - protected
 - public
 - secret
 - sensitive
 - strictly for internal use
 - top secret
- technology protocols used for user identification
- strategies for minimising and eliminating cyber security insider risks and threats in an organisation
- methods to configure cyber security insider risk and threat detection tools.

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:

- cyber security insider risk and threat detection tools required for configuration
- legislative, regulatory and contractual requirements and organisational policies and procedures applicable to cyber security insider risks and threats, including organisational security procedures
- required hardware and software.

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>