



Australian Government

ICTCYS615 Detect and respond to cyber security insider risks and threats

Release: 1

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.

Application

This unit describes the skills and knowledge required to detect and respond to intentional and unintentional cyber security insider risks and threats, including the configuration of tools.

The unit applies to those who work in information technology security roles, including cyber security analysts and specialists, cyber risk and assurance managers, and other related roles that are responsible for detecting and responding to cyber security insider risks and threats.

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 detect organisational cyber security insider risks and threats	1.1 Obtain work details from required personnel 1.2 Evaluate and apply privacy requirements according to organisational policies and procedures, legislation, codes, regulations, standards and security arrangements 1.3 Analyse type of behaviours that indicate cyber security insider risks and threats 1.4 Analyse sources of sensitive data and business processes that are vulnerable to cyber security insider risks and threats 1.5 Select required cyber security insider risk and threat detection tools according to organisational policies and procedures
2. Configure and monitor	2.1 Configure cyber security insider risk and threat detection tools

ELEMENT	PERFORMANCE CRITERIA
cyber security insider risk and threat detection tools	into organisation's operations and infrastructure 2.2 Use behavioural analysis and cyber security insider risk and threat detection tools 2.3 Monitor potential breaches identified by tool and abnormal outputs from behavioural analysis 2.4 Locate source of breaches and determine extent of cyber security insider risks, threats and their organisational impact 2.5 Maintain custody chain according to legislative requirements and organisational security procedures
3. Respond to cyber security insider risks and threats	3.1 Consult with required personnel to determine suitable course of action to mitigate identified risks and threats, and restrict user access where required 3.2 Implement determined course of action according to organisational policies and procedures 3.3 Test course of action according to organisational security procedures and escalate test findings to required personnel, where required
4. Finalise response to cyber security insider risks and threats	4.1 Evaluate course of action taken and confirm that risks and threats have been contained 4.2 Document exposed data and implemented course of action according to organisational requirements 4.3 Gather feedback on risk and threat detection and response process from personnel involved in the incident 4.4 Develop and submit report on threat detection and response according to legislative requirements and organisational policies and 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
Writing	Prepares complex workplace documentation detailing processes and outcomes using required structure, layout and applicable language
Oral communication	Presents information in a clear manner using language appropriate to target audience

SKILL	DESCRIPTION
Problem solving	• Uses understanding of context to recognise anomalies and subtle deviations to normal expectations
Self-management	• Takes responsibility for identifying and considering organisational policies, procedures, protocols and requirements
Technology	• Demonstrates an understanding of digital principles, concepts, language and practices

Unit Mapping Information

No equivalent unit. Newly created 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 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>