



Australian Government

ICTCYS614 Analyse cyber security insider risks and threats and devise recommendations

Release: 1

ICTCYS614 Analyse cyber security insider risks and threats and devise recommendations

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 analyse intentional and unintentional cyber security insider risks and threats, devise recommendations to minimise those risks and threats, and recommend organisational training responses to them.

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 analysing 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. Determine cyber security insider risks and threats in organisation or workplace context	1.1 Obtain work details and scope from required personnel and arrange for access to required technology in compliance with organisational security arrangements and required legislation, codes, regulations and standards 1.2 Evaluate and apply privacy requirements according to organisational policies and procedures 1.3 Identify systems of critical nature to business and key data logs for detection of cyber security insider risk and threat activity 1.4 Determine high-risk data using organisational risk framework 1.5 Monitor organisational behaviour patterns to identify cyber

ELEMENT	PERFORMANCE CRITERIA
	security insider risks and threats
2. Complete model-based analysis of cyber security insider risks and threats	2.1 Identify model required to analyse cyber security insider risks and threats 2.2 Analyse sensors and data logs and perform risk assessment to identify high-risk users and behaviours 2.3 Perform a model-based analysis of cyber security insider risks and threats
3. Devise and distribute recommendations arising from analysis	3.1 Prioritise risks and threats based on analysis according to organisational policies and procedures 3.2 Develop recommendations to minimise or eliminate insider risks and threats based on analysis findings 3.3 Seek and integrate feedback of required personnel on draft recommendations 3.4 Distribute information and documentation to required personnel according to legislative requirements and organisational policies and procedures
4. Review organisational training response to cyber security insider risks and threats	4.1 Review identified cyber security insider risks and threats to identify training requirements 4.2 Develop recommendations for training to address cyber security insider risks and threats 4.3 Seek feedback on training recommendations from required personnel 4.4 Finalise and distribute training recommendations according to 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
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 ICTCYS614 Analyse cyber security insider risks and threats and devise recommendations

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:

- perform one model-based analysis of cyber security insider risks and threats within an organisation or workplace context.

In the course of the above, the candidate must:

- document analysis findings that identify at least two intentional and two unintentional cyber security insider risks and threats
- devise and distribute recommendations that minimise workplace vulnerability
- recommend organisational training response relating to the findings of the above cyber security insider risk and threat analysis.

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 and standards relating to analysing cyber security insider risks and threats
- organisational policies and procedures, including:
 - data loss mitigation controls
 - risk framework
 - security arrangements
 - security control standards
- 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 organisational behavioural patterns that indicate cyber security insider risks and threats
- key features of different data classifications, including:
 - classified
 - confidential
 - private
 - protected
 - public
 - secret
 - sensitive
 - strictly for internal use
 - top secret
- key data loss mitigation controls
- key types of model-based insider risk and threat analysis and tools
- sensitive locations containing data logs and sensors at risk of cyber security insider risks and threats
- strategies for minimising and eliminating cyber security insider risks and threats in an organisation
- procedures for assessing risks, including for identifying different types of high-risk users
- technology protocols used for user identification.

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:

- legislative, regulatory and contractual requirements and organisational policies and procedures applicable to cyber security insider risks and threats, including organisational security procedures
- organisational framework to guide analysis of high-risk sensitive data
- 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>