Australian Government

Assessment Requirements for ICTCYS614 Analyse cyber security insider risks and threats and devise recommendations

Release: 1

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