ICTCYS614 Analyse insider cyber security threats

# Application

This unit describes the skills and knowledge required to analyse key behaviours of intentional and unintentional insider cyber security threats in high-risk situations, identify controls to minimise insider threats and support training personnel on insider threats to an organisation.

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 disciplines that are responsible for analysing cyber security 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** |
| *Elements describe the essential outcomes.* | *Performance criteria describe the performance needed to demonstrate achievement of the element.* |
| 1. Identify insider cyber security threats | 1.1 Analyse sensitive data in relation to insider cyber security threats and identify trends  1.2 Identify high-risk sensitive data in organisation or workplace context using organisational risk framework  1.3 Identify systems of critical nature to business and key log sources for detection of insider threat activity  1.4 Identify and apply privacy requirements according to organisational policy and procedures, and legislative requirements  1.5 Analyse and monitor insider threat behavioural patterns at all organisational levels and identify abnormal behaviour within an organisation |
| 2. Undertake threat model-based analysis of insider cyber security threat | 2.1 Identify threat model required to analyse insider cyber security threats  2.2 Analyse sensors and data logs and perform risk assessment to identify high-risk users and behaviours  2.3 Perform top-down, threat model-based analysis of insider cyber security threats |
| 3. Finalise analysis and distribute recommendations | 3.1 Document analysis findings of insider cyber security threats, sensitive data and high-risk users  3.2 Prioritise threats based on analysis according to organisational policies and procedures  3.3 Develop recommendations based on analysis findings  3.4 Communicate with personnel responsible for decision-making and gather feedback  3.5 Distribute relevant information and documentation to required personnel according to legislative requirements and organisational policies and procedures |
| 4. Support training of relevant personnel | 4.1 Identify training requirements regarding possible insider threat activities applicable to organisational policies and procedures  4.2 Develop training recommendations addressing insider threat detection  4.3 Seek feedback about the effectiveness of recommendations |

# 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 the target audience * Uses questioning and active listening techniques to confirm understanding of delivered message |
| Problem solving | * Uses 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 |
| Technology | * Demonstrates an understanding of digital principles, concepts, language and practices |

# 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 ICTCYS614 Analyse insider cyber security threats

**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 model-based analysis of insider cyber security threats on at least two occasions
* report on at least two intentional and two unintentional insider cyber security threats and distribute recommendations to minimise workplace vulnerability.

In the course of the above, the candidate must:

* adhere to legislative requirements and organisational policies and procedures.

# 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:

* classifications of data, including:
  + confidential
  + classified
  + private
  + protected
  + public
  + secret
  + sensitive
  + strictly for internal use
  + top secret
* conducting model-based cyber security analysis and threat analysis
* documentation processes that may be used in the process of identifying and analysing insider threats
* internet, technology and user identification protocols
* privacy standards and policies
* procedures for identifying high-risk users
* key data loss prevention controls
* key types of model-based cyber security analysis
* key types of threat analysis
* key security control standards relevant to organisation
* examples of intentional and unintentional insider cyber security threats
* strategies for minimising insider cyber security threats in an organisation
* organisational policies and procedures applicable to insider cyber security threat analysis
* relevant model-based analysis methods
* sensitive locations containing data, data logs and sensors at risk of insider cyber security threats
* types of insider threats, including:
  + careless employees
  + compromised employees
  + disgruntled employees
  + expired users with valid credentials
  + malicious insiders
  + misinformed users.

# 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:

* devices which contain sensitive data
* organisational framework to guide analysis of high-risk sensitive data
* legislative, regulatory and contractual requirements and organisational procedures and policies applicable to insider threats such as organisational security procedures.

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>

ICTCYS615 Detect and respond to insider cyber security threats

# Application

This unit describes the skills and knowledge required to detect and respond to intentional and unintentional insider cyber security 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 disciplines that are responsible for detecting and responding to cyber security 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** |
| *Elements describe the essential outcomes.* | *Performance criteria describe the performance needed to demonstrate achievement of the element.* |
| 1. Analyse organisation for vulnerabilities to insider threats | 1.1 Obtain work details and scope from relevant personnel and arrange for required technology access in compliance with organisational security arrangements, legislation, codes, regulations and standards  1.2 Analyse organisational structure, governance and historical data and identify at risk data and business process vulnerabilities  1.3 Analyse insider threat behavioural patterns and identify abnormal behaviour within an organisation  1.4 Identify privacy requirements according to organisational policy and procedures, and legislative requirements |
| 2. Determine and configure threat detection tool | 2.1 Identify sources of sensitive data and business risks that may be vulnerable to insider cyber security threats  2.2 Identify the nature of insider threat for each identified sensitive data location  2.3 Analyse strengths and limitations of threat detection tools  2.4 Select threat detection tool for identified insider threat  2.5 Configure chosen insider threat detection tools into organisation’s operations and infrastructure |
| 3. Detect and monitor insider cyber security threat | 3.1 Use insider threat detection tools  3.2 Monitor tool and locate the source of insider threat  3.3 Identify extent of insider threat and impact on organisation  3.4 Identify if further risks exist and maintain custody chain according to legislative requirements and organisational security procedures |
| 4. Respond to insider threat | 4.1 Discuss solutions to remove the threat and disable user access with relevant personnel, where required  4.2 Select required solution  4.3 Implement solution according to discussion with relevant personnel and organisation policies and procedures  4.4 Test solution and escalate to relevant personnel, where required according to organisational security procedures |
| 5. Report insider cyber security threat | 5.1 Evaluate actions taken and confirm threat was contained  5.2 Document exposed data and implemented solution according to organisational requirements  5.3 Gather feedback on threat detection and response from personnel involved in the incident  5.4 Submit documentation according to organisational policies, procedures and legislative requirements |

# 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 the target audience * Uses questioning and active listening techniques to confirm understanding of delivered message |
| Problem solving | * Uses 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 |
| Technology | * Demonstrates an understanding of digital principles, concepts, language and practices |

# 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 ICTCYS615 Detect and respond to insider cyber security threats

# 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:

* identify and configure at least three different tools and use each to detect a different insider cyber security threat.

In the course of the above, the candidate must:

* adhere to legislative requirements and organisational policies and procedures
* report and respond to at least three insider cyber security 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:

* classifications of data, including:
  + classified
  + confidential
  + private
  + protected
  + protected
  + public
  + secret
  + sensitive
  + strictly for internal use
  + top secret
* data logs, including the use of server, network and firewall information
* documentation processes that may be used in the process of responding insider threats
* insider threat detection methodologies and tools
* insider threat causes and sources
* internet, technology and user identification protocols
* privacy standards and policies
* key security control standards
* organisational policies and procedures applicable to insider threat response, including procedures for:
  + assessing impact and rectifying damage imposed by the insider threat
  + containing threats, including disabling user access
  + determining the nature of a detected threat
  + identifying the location of sensitive data
  + notifying and reporting a threat to required personnel
* prevention strategies and actions to contain insider threats, including data loss
* types of insider threats, including:
  + careless employees
  + compromised employees
  + disgruntled employees
  + expired users with valid credentials
  + malicious insiders
  + misinformed users.

# 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:

* threat detection tools required for configuration
* devices which contain sensitive data that may be targeted
* required hardware and software
* legislative, regulatory and contractual requirements and organisational procedures and policies applicable to insider threats such as organisational security procedures.

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

**ICTSS00117 Cyber Security Counter-Insider Threat Skill Set**

# Description

This skill set addresses the skills and knowledge to analyse, detect and respond to insider cyber security threats and expand capabilities for minimising vulnerability to various internal risks in an organisational context.

# Pathways Information

The units provide credit towards ICT60120 Advanced Diploma of Information Technology and other qualifications that allow for selection of these units.

# Licensing/Regulatory Information

No licensing, legislative or certification requirements apply to this skill set at the time of publication.

# Skill Set Requirements

ICTCYS601 Create cyber security standards for organisations

ICTCYS607 Acquire digital forensic data

ICTCYS614 Analyse insider cyber security threats

ICTCYS615 Detect and respond to insider security threats

# Target Group

The skill set is for individuals who work in information technology security roles, including cyber security analysts and specialists, cyber risk and assurance managers, and other related disciplines that are responsible for analysing, detecting and responding to cyber security threats.

# Suggested words for Statement of Attainment

These units of competency from the ICT Information and Communications Technology Training Package meet industry requirements for cyber security counter-insider threat prevention, detection and response in ICT contexts.