



**Australian Government**

# **BSBXCS305 Identify and assess cyber security insider threats and risks**

**Release: 1**

# BSBXCS305 Identify and assess cyber security insider threats and risks

## Modification History

| Release   | Comments                                                                                                    |
|-----------|-------------------------------------------------------------------------------------------------------------|
| Release 1 | This version first released with the Business Services Training Package Version 8.0.<br>Newly created unit. |

## Application

This unit describes the skills and knowledge required to contribute to business operations by identifying and assessing cyber security insider threats and risks. This includes reviewing and applying organisational processes for identifying and documenting insider threats.

The unit covers insider threats and risks that relate to individuals in an organisation who commit an act, intentionally or unintentionally, that causes harm.

The unit applies to individuals who identify and communicate identified insider threats and risks to required management and information technology (IT) personnel.

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

## Unit Sector

Digital Competence - 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 identify insider threats and risks in workplace | 1.1 Identify common types of insider threats and risks<br>1.2 Determine organisational process for identifying and assessing insider threats and risks                                                                                  |
| 2. Identify and assess insider threats and risks              | 2.1 Review organisational processes and identify gaps that may allow for insider threats and risks to occur<br>2.2 Monitor work activities and identify digital and behavioural indicators of insider threats and risks in organisation |

|                                                                |                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                | 2.3 Analyse identified indicators and confirm existence of insider threats and risks<br>2.4 Identify potential impact and probability of identified threats and risks                                                                                   |
| 3. Complete identification and assessment of threats and risks | 3.1 Document identified insider threats and risks according to organisational policies and procedures<br>3.2 Communicate identified insider threats and risks to required management and information technology (IT) personnel within scope of own role |

## 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                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Oral communication | <ul style="list-style-type: none"><li>• Uses effective communication techniques to discuss insider threats and risks</li></ul>                                                                                                            |
| Reading            | <ul style="list-style-type: none"><li>• Interprets information in a range of formats when identifying insider threats and risks</li><li>• Reads and applies information of relevance when identifying insider threats and risks</li></ul> |
| Writing            | <ul style="list-style-type: none"><li>• Uses required and industry-specific terminology in identifying insider threats and risks</li></ul>                                                                                                |
| Technology         | <ul style="list-style-type: none"><li>• Uses required technological tools in identifying and assessing insider threats and risks</li></ul>                                                                                                |

## 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=11ef6853-ceed-4ba7-9d87-4da407e23c10>

# Assessment Requirements for BSBXCS305 Identify and assess cyber security insider threats and risks

## Modification History

| Release   | Comments                                                                                                        |
|-----------|-----------------------------------------------------------------------------------------------------------------|
| Release 1 | This version first released with the Business Services Training Package Version 8.0.<br><br>Newly created unit. |

## 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, assess and document at least:
  - three instances of malicious insider threats and risks
  - three instances of accidental insider threats and risks.

In the course of the above, the candidate must:

- identify common indicators of insider threats
- identify organisational risks associated with common insider threats
- identify scenarios where insider threats may occur
- adhere to relevant organisational security 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:

- definition of insider threat and risk
- difference between malicious and accidental insider threats and risks
- key components of organisational security procedures
- indicators of digital insider threats, including:
  - accessing sensitive data not associated with job function
  - using unauthorised storage devices
  - data hoarding
  - emailing data to those external to organisation
  - irresponsible social media use
- indicators of behavioural insider threats, including:

- frequently visiting workplace outside normal business hours or working extra hours
- violating corporate policies
- decline in work performance
- unpredictable behaviour or obvious signs of being disgruntled with organisation
- organisational policies and procedures relating to cyber security
- organisational impacts of insider threats and risks, including:
  - stolen and misused data
  - customer and client liability
  - reputational loss.

## 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:

- required hardware, software and their components
- system, network and application infrastructure
- internet connection that supports the requirements set out in the performance evidence
- organisational cyber security policies and 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=11ef6853-ceed-4ba7-9d87-4da407e23c10>