Australian Government

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

Release: 1

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. 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