Australian Government

Assessment Requirements for BSBXCS409 Plan and implement organisational cyber security insider threat prevention strategies

Release: 1

Assessment Requirements for BSBXCS409 Plan and implement organisational cyber security insider threat prevention strategies

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:

- plan and implement at least one cyber security insider threat prevention strategy that includes:
  - objectives
  - methods
  - budget
  - responsibilities of key individuals.

In the course of the above, the candidate must:

- identify and report opportunities for further improvement.

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:

- human resource policies in relation to cyber security, including:
  - general data protection policies
  - incident response policies
  - third-party access policies
  - account management policies
  - user monitoring policies
  - password management policies
- sources of potential cyber security threats in organisation
- resourcing needed to respond to insider threat, including:

  - administrative resources
  - technical resources
  - financial resources
- knowledge of roles and responsibilities of key people in insider threat response teams, including:
  - response team lead
  - information technology specialists
  - human resources
  - legal
  - compliance
  - risk
  - communications
- legislative requirements relating to cyber security threats
- key features and functions of software used to mitigate insider threats
- staff training methods in relation to implementing insider threat prevention strategy
- key features of insider threat prevention strategies, including:
  - managing user access to sensitive resources
  - monitoring user activity in a network
  - analysing user behaviour
- methods to evaluate effectiveness of insider threat prevention strategies, including:
  - data analysis of cyber breaches
  - interviewing employees.

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
- legislative requirements regarding organisational security
- real life case studies of failures and successes of insider threat prevention strategies
- workplace documentation, resources required to plan and implement insider threat prevention strategies.

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