Australian Government

Assessment Requirements for BSBXCS406 Develop cyber security insider threat and risk response plans

Release: 1

Assessment Requirements for BSBXCS406 Develop cyber security insider threat and risk response plans

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:

- develop at least one cyber security insider threat and risk response plan for an organisation or work area that effectively prevents and mitigates insider threats and risks.

In the course of the above, the candidate must:

- assess the organisation's mission, culture, values, and threats and tailor the risk response to this context
- conduct primary and secondary research on best practice for risk response plans.

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:

- employee risk profiles, including:
  - types of risks and threats employees pose
  - likelihood of threats occurring
  - level of disruption and cost associated with employee risk
  - effectiveness of controls in place to manage risk
- definition of cyber security insider threat
- organisational security policies and procedures regarding cyber security insider threat prevention
- methods to evaluate effectiveness of policies and procedures, including:
  - qualitative, including observing behaviour
  - quantitative, including number of breaches per year

- risks related to different positions and duties within organisation described in performance evidence
- technology used within roles and organisation exposed to insider threats and risks, including:
  - hardware, including computers, smart devices and surveillance cameras
  - software
- tools for cyber security threat detection, prevention, mitigation and analysis
- legal and regulatory requirements relating to cyber security insider threat and risk response plans
- organisational policies and procedures relating to cyber security insider threat and risk response plans
- organisational format and features expected of cyber security insider threat and risk response plan.

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 its components
- system, network and application infrastructure
- internet connection that supports the requirements set out in the performance evidence
- organisational security procedures
- legislative requirements regarding organisational security.

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