



Australian Government

**Assessment Requirements for BSBXCS306
Apply own techniques to prevent cyber
security insider threats**

Release: 1

Assessment Requirements for BSBXCS306 Apply own techniques to prevent cyber security insider threats

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:

- apply techniques to prevent at least two potential cyber security insider threats in own work area, using different techniques with each threat.

In the course of the above, the candidate must:

- adhere to organisational security procedures regarding cyber security insider threat prevention.

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 cyber security insider threat
- organisational security procedures for preventing cyber security insider threats
- types of cyber security insider threats and risks, including malicious and accidental actions
- opportunities for insider threats, including:
 - simple passwords
 - orphaned accounts
- human resource policies that support prevention of cyber security insider threats, including:
 - general data protection policies
 - incident response policies
 - third-party access policies
 - account management policies
 - user monitoring policies

- password management policies
- techniques to reduce cyber security insider threats, including:
 - organisation-wide participation in cyber security insider threat awareness programs
 - limiting user permissions and access to applications, systems, and data
 - firewalls and demilitarised zone networks
 - software monitoring
- good practice examples of organisational learning and development programs regarding insider threat prevention.

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
- 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>