



Australian Government

Assessment Requirements for BSBXCS302 Identify and report online security threats

Release: 1

Assessment Requirements for BSBXCS302 Identify and report online security threats

Modification History

Release	Comments
Release 1	This version first released with BSB Business Services Training Package 6.0.

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 and report three different online security threats in a work area.

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:

- legislative requirements relating to identifying and reporting online security threats, including:
 - data protection
 - implications of Notifiable Data Breach legislation on an organisation and other associated Australian privacy laws
 - established international legislation
- organisational policies and procedures relating to online information security breaches, including:
 - blocking and reporting potential security breaches
 - escalation routes for cyber security issues
- common types of online scams and security risks, including phishing scams
- common techniques of phishing and spear phishing used by attackers, including:
 - spam email and SMS text
 - social engineering, including telephone calls, social media and website requests for information
- basic principles of cyber security
- indicators of insecure connection to websites, in particular where data is being collected
- Australian government sources of information on current online security threats
- common online security threats to which individuals might be exposed to, including physical threats

- common procedures for:
 - mitigating online security threats
 - following organisational cyber security incident response plan
 - responding to cyber security breaches.

Assessment Conditions

Skills must be assessed in a workplace or simulated environment where conditions are typical of a work environment requiring cyber secure practices, processes and procedures.

Access is required to:

- information and data sources relating to cyber security
- device with active internet connection
- internet browser
- industry standards and organisational procedures required to demonstrate the performance evidence.

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=a53af4e4-b400-484e-b778-71c9e9d6aff2>