



Australian Government

BSBXCS403 Contribute to cyber security threat assessments

Release: 1

BSBXCS403 Contribute to cyber security threat assessments

Modification History

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

Application

This unit describes the skills and knowledge required to support maintaining a cyber secure network through identifying cyber security threats for an organisation.

It applies to those working in a broad range of industries who as part of their job role contribute to assessments of level of risk relating to real and potential cyber security breaches.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Digital Competence – Cyber Security

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Contribute to reviewing workplace cyber security threats	1.1 Identify relevant organisational data security/protection policies and procedures 1.2 Contribute to organisation-wide cyber security audits 1.3 Contribute to identifying threats to workplace security of cyber security threats
2. Assist in assessing risks and potential business impact of cyber security threats	2.1 Assist in assessing cyber security risks and their likelihood, consequences and suggested mitigation strategies 2.2 Assist in reviewing industry level threats and best practice cyber security strategies 2.3 Assign risk levels for identified cyber risks based on measurement scale

ELEMENT	PERFORMANCE CRITERIA
	2.4 Contribute to identifying impact of risks
3. Finalise cyber security threat assessment	3.1 Document impact findings that include recommendations for required responses to control risks 3.2 Support the communication of cyber security threat assessment outcomes and recommendations to required personnel 3.3 Seek feedback as required on assessment findings 3.4 Assist in integrating feedback to finalise threat assessment 3.5 Distribute or store final threat assessment according to organisational policies and procedures

Foundation Skills

This section describes those language, literacy, numeracy and employment skills that are essential to performance but not explicit in the performance criteria.

Skill	Description
Learning	Modifies behaviour following exposure to new information
Numeracy	- Interprets mathematical data - Completes at times complex calculations and records mathematical data
Oral communication	- Asks open and closed probing questions and actively listens to clarify consultations - Communicate findings of assessment of business impact to required personnel
Reading	Recognises and interprets information from relevant sources to determine organisational expectations
Writing	- Uses clear, specific and industry-related terminology relating to cyber security - Produces written reports on business impact of assessed threat
Teamwork	Works collaboratively with interdisciplinary teams to ensure procedures are implemented
Technology	Uses appropriate technology platforms to assist with cyber security threat assessments

Unit Mapping Information

No equivalent unit. New unit.

Links

Companion Volume Implementation Guide is found on VETNet: -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for BSBXCS403 Contribute to cyber security threat assessments

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:

- provide non-technical support to a cyber security threat assessment in a work area by describing three threats
- communicate and distribute findings of the identified threats.

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 contributing to cyber security threat assessments, including:
 - data protection
 - implications of Notifiable Data Breach legislation on an organisation and other associated Australian privacy laws
 - established international legislation
- potential organisational impact of cyber attacks
- online risks affecting organisation's operations
- common procedures for cyber threat rating and modelling
- strategies, techniques and tools that improve an organisation's cyber security and audit processes
- organisational policies and procedures for information security, including:
 - confidentiality, integrity, and availability
 - communicating threat assessment findings.

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>