



Australian Government

BSBXCS408 Develop employee cyber security risk profiles

Release: 1

BSBXCS408 Develop employee cyber security risk profiles

Modification History

Release	Comments
Release 1	This version first released with the Business Services Training Package Version 8.0. Newly created unit.

Application

This unit describes the skills and knowledge required to contribute to business operations and risk mitigation by developing employee cyber security risk profiles. This includes identifying the organisational risk landscape, assessing compliant employee characteristics, and documenting employee risk characteristics.

The unit applies to individuals with specialist skills who contribute to employee cyber security risk mitigation in an organisation.

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. Prepare to develop employee risk profiles	1.1 Consult with key stakeholders on common employee cyber security risks faced by organisation 1.2 Assess probability and cost of employee cyber security risks faced by organisation 1.3 Identify and evaluate existing organisational strategies to mitigate risk for current and future employees 1.4 Identify relationship between frequency of employee cyber security risk events and existing organisational strategies to mitigate employee risk 1.5 Determine current level of workplace awareness regarding employee

	cyber security risk 1.6 Consult with key stakeholders to determine scope of employee cyber security risk management appropriate to organisation
2. Assess individual employee risk characteristics	2.1 Consult with key stakeholders to determine characteristics of an employee compliant with organisational policies and procedures 2.2 Consult with key stakeholders to determine high risk characteristics of employees in organisation 2.3 Identify and document high risk characteristics of employees and potential candidates, and of different demographics in organisation
3. Finalise employee cyber security risk profile	3.1 Assess organisational priorities in maintaining cyber security safety 3.2 Document employee and potential candidate cyber security risks in a risk profile against identified priorities according to organisational policies and procedures and legislative requirements 3.3 Update employee cyber security risk profile with new information as required and according to organisational policies and procedures and legislative requirements 3.4 Inform required personnel of key employee cyber security risks

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	Gathers and analyses information applicable to employees, risk, business and systems
Oral communication	Uses a range of questioning techniques and active listening to communicate effectively and clarify where necessary
Reading	Identifies and interprets information from relevant sources
Writing	Uses clear and industry-specific terminology relating to cyber security and employee risk profiles
Teamwork	Works collaboratively with colleagues and stakeholders to develop employee cyber security risk profiles
Technology	Uses appropriate technology platforms to assist with developing employee cyber security risk profiles

Unit Mapping Information

No equivalent unit. Newly created unit.

Links

Companion Volume Implementation Guide is found on VETNet - -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=11ef6853-ceed-4ba7-9d87-4da407e23c10>

Assessment Requirements for BSBXCS408 Develop employee cyber security risk profiles

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 a cyber security risk profile for at least three different employees
- update the cyber security risk profiles of at least three different employees based on newly identified organisational risks.

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 operations and recruitment strategies relevant to insider cyber security threats
- cost of employee risk profiling, including potentially breaching employee privacy
- benefits of employee risk profiling, including employee risk mitigation
- privileged access management systems
- organisational impacts of poor employee risk management and profiling
- legislative requirements relevant to employee risk mitigation
- organisational strategies that minimise employee risk, including:
 - organisation-wide participation in insider threat awareness programs
 - privileged access management systems
 - surveillance systems
- organisational factors relevant to employee risk mitigation, including:
 - policies and procedures
 - codes of conduct
 - organisational reputation and culture
- required communication methods, including:
 - producing documents in organisational databases

- reports
- oral communication
- procedures for developing employee risk profiles
- key employee privacy legislation

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 risk management 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>