



Australian Government

BSBXCS406 Develop cyber security insider threat and risk response plans

Release: 1

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.

Application

This unit describes the skills and knowledge required to develop cyber security insider threat and risk response plans to effectively prevent, detect and mitigate insider threats. This includes assessing current cyber security risks, evaluating existing procedures, and drafting a cyber security insider threat and risk response plan. An insider threat or risk refers to an intentional or unintentional act committed by individuals in an organisation that causes, or has the potential to cause, harm to an organisation's cyber security.

The unit applies to individuals who work in a broad range of industries who as part of their job role assist in preventing insider threat and risk, by supporting processes to develop response plans. Individuals in these job roles will demonstrate judgement and have limited responsibilities in changing contexts.

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 cyber security insider threat and risk response plan	1.1 Assess organisational cyber security risks and their causes 1.2 Evaluate impact and probability of assessed organisational cyber security risks 1.3 Prioritise organisational cyber security risks based on their impact and probability

2. Draft cyber security insider threat and risk response plan	2.1 Identify and document existing organisational policies and procedures for responding to cyber security insider threats and risks 2.2 Evaluate existing procedures to monitor employee adherence to risk minimising policies and procedures 2.3 Evaluate effectiveness of existing risk response policies and procedures based on prioritised risks 2.4 Research existing examples of best practice cyber security insider threat and risk response plans in different organisations 2.5 Develop draft of cyber security threat and risk response plan based on prioritised organisational risks according to legislative requirements
3. Review and finalise cyber security insider threat and risk response plan	3.1 Seek feedback on draft plan from required personnel according to organisational policies and procedures 3.2 Integrate feedback and finalise plan 3.3 Seek plan sign-off according to organisational policies and procedures 3.4 Distribute and store documented plan 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
Oral communication	Consults with stakeholders to inform decision making
Reading	Interprets information from relevant sources to inform plan
Writing	Uses clear and industry-specific terminology relating to cyber security in workplace documents
Teamwork	Works collaboratively with teams to develop risk response plans
Initiative and enterprise	Takes responsibility for identifying and complying with legislative requirements applicable to self and the organisation
Planning and organising	Maintains records and documentation relating to cyber security insider threat and risk response plans
Problem solving	Systematically gathers and analyses required information and evaluates options in order to identify opportunities for improvement
Technology	Uses appropriate technology platforms to assist with developing plan

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 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>