



Australian Government

BSBXCS409 Plan and implement organisational cyber security insider threat prevention strategies

Release: 1

BSBXCS409 Plan and implement organisational cyber security insider threat prevention strategies

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 plan and implement cyber security insider threat prevention strategies. This includes assessing different insider threat prevention strategies and providing training and support to staff to transition to new strategies.

The unit applies to individuals in specialist positions who use various systems and strategies to actively encourage teams and employees in an organisation to use insider threat prevention strategies.

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 implement cyber security insider threat prevention strategies	1.1 Research cyber security insider threat strategies in industry and organisation-specific context 1.2 Determine potential threat sources within organisation 1.3 Identify previous and current insider threat prevention strategies in the organisation
2. Select strategies for insider threat prevention	2.1 Consult with employees and relevant information technology personnel on success of current and previous insider threat prevention strategies

	2.2 Consult with required personnel to identify requirements of insider threat prevention strategies according to organisational and budgetary requirements 2.3 Identify insider threat strategies suited to organisational context and needs
3. Implement cyber security insider threat prevention strategies	3.1 Implement software and practices that comply with organisational and legislative requirements 3.2 Communicate strategies to required stakeholders and seek active participation of staff 3.3 Assist in implementing training processes and support for staff in transition to new strategies
4. Evaluate effectiveness of strategy and update and review as required	4.1 Interview employees to determine receptiveness towards strategies 4.2 Gather data on frequency of incidents following implementation of strategies 4.3 Modify strategies to meet changing needs according to organisational requirements 4.4 Monitor staff training needs and train new staff on strategies

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
Numeracy	- Interprets data from a range of sources to determine success of prevention plan - Uses mathematical skills to interpret budgets, timelines and overall success of strategy
Oral communication	- Participates in verbal exchanges using appropriate style, tone and vocabulary for audience, context and purpose - Uses listening and questioning techniques to elicit key information and confirm understanding - Presents at times complex information adjusting presentation style and vocabulary to suit the audience
Reading	Extracts, analyses and evaluates information from complex texts, including organisational policies and procedures
Writing	Gathers and uses information and ideas from a range of sources to create texts to meet organisational requirements
Planning and organising	Uses logical planning processes to identify and plan ongoing improvements

Teamwork	• Works collaboratively with colleagues and stakeholders to develop threat prevention strategies
Technology	• Uses required technology to plan and implement threat prevention strategies

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 BSBXCS409 Plan and implement organisational cyber security insider threat prevention strategies

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:

- plan and implement at least one cyber security insider threat prevention strategy that includes:
 - objectives
 - methods
 - budget
 - responsibilities of key individuals.

In the course of the above, the candidate must:

- identify and report opportunities for further improvement.

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 policies in relation to cyber security, including:
 - general data protection policies
 - incident response policies
 - third-party access policies
 - account management policies
 - user monitoring policies
 - password management policies
- sources of potential cyber security threats in organisation
- resourcing needed to respond to insider threat, including:
 - administrative resources

- technical resources
- financial resources
- knowledge of roles and responsibilities of key people in insider threat response teams, including:
 - response team lead
 - information technology specialists
 - human resources
 - legal
 - compliance
 - risk
 - communications
- legislative requirements relating to cyber security threats
- key features and functions of software used to mitigate insider threats
- staff training methods in relation to implementing insider threat prevention strategy
- key features of insider threat prevention strategies, including:
 - managing user access to sensitive resources
 - monitoring user activity in a network
 - analysing user behaviour
- methods to evaluate effectiveness of insider threat prevention strategies, including:
 - data analysis of cyber breaches
 - interviewing employees.

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
- legislative requirements regarding organisational security
- real life case studies of failures and successes of insider threat prevention strategies
- workplace documentation, resources required to plan and implement insider threat prevention strategies.

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>