



**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

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

## 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	<ul style="list-style-type: none"> <li>Interprets data from a range of sources to determine success of prevention plan</li> <li>Uses mathematical skills to interpret budgets, timelines and overall success of strategy</li> </ul>
Oral communication	<ul style="list-style-type: none"> <li>Participates in verbal exchanges using appropriate style, tone and vocabulary for audience, context and purpose</li> <li>Uses listening and questioning techniques to elicit key information and confirm understanding</li> <li>Presents at times complex information adjusting presentation style and vocabulary to suit the audience</li> </ul>
Reading	<ul style="list-style-type: none"> <li>Extracts, analyses and evaluates information from complex texts, including organisational policies and procedures</li> </ul>
Writing	<ul style="list-style-type: none"> <li>Gathers and uses information and ideas from a range of sources to create texts to meet organisational requirements</li> </ul>
Planning and organising	<ul style="list-style-type: none"> <li>Uses logical planning processes to identify and plan ongoing improvements</li> </ul>

---

Teamwork	<ul style="list-style-type: none"><li>• Works collaboratively with colleagues and stakeholders to develop threat prevention strategies</li></ul>
Technology	<ul style="list-style-type: none"><li>• Uses required technology to plan and implement threat prevention strategies</li></ul>

## 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>