



Australian Government

BSBXCS405 Contribute to cyber security incident responses

Release: 1

BSBXCS405 Contribute to cyber security incident responses

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 assist in responding to and containing cyber security incidents.

It applies to those working in a broad range of industries and job roles who work alongside technical experts to develop cyber security risk-management 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. Confirm cyber security incident and contribute to its containment	1.1 Confirm nature and location of cyber security incident according to organisational policies and procedures 1.2 Estimate risk, likelihood and potential consequence of incident according to organisational response procedures 1.3 Assist in ensuring that cyber incident is contained according to legislative requirements and organisational cyber security incident response plan 1.4 Assist in confirming no further risks according to legislative requirements and organisational response procedures
2. Communicate information on cyber security incident	2.1 Escalate cyber security incident with required workplace personnel according to organisational policies and procedures

ELEMENT	PERFORMANCE CRITERIA
	2.2 Consult with required internal and external stakeholders on communication needs relating to cyber security incident 2.3 Assist in alerting required external parties according to legislative requirements and organisational procedures
3. Contribute to post-incident activities	3.1 Support post-breach review and reporting 3.2 Assist in identifying lessons learnt from incident response and recommended changes to cyber security response plan 3.3 Assist in updating cyber security response plan to reflect review outcomes according to organisational policies and procedures 3.4 Communicate lessons learnt and recommendations to required personnel

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 - Understands developments within cyber security protection and is able to advise on which options are appropriate
Numeracy	- Interprets mathematical data - Completes at times complex calculations and records mathematical data
Oral communication	- Asks open and closed probe questions and actively listens to clarify consult with business and ICT technicians - Communicate findings of assessment of business impact to required personnel
Reading	Recognises and interprets information from relevant sources to determine organisational expectations and legal requirements
Writing	- Uses clear, specific and industry-related terminology relating to cyber security - Produce written reports on business impact of assessed threat
Planning and organising	Manages cyber security incident response plan including protection strategies through to responding to breaches
Technology	Uses appropriate technology platforms to assist with cyber security

Skill	Description
	incident responses

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>