



**Australian Government**

# **ICTCLD512 Respond to cloud security incidents**

**Release: 1**

# ICTCLD512 Respond to cloud security incidents

## Modification History

| Release   | Comments                                                                                                                                                                                |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Release 1 | This version first released with the Information and Communications Technology Training Package Version 8.0.<br><br>Newly created unit of competency to address in-demand skills needs. |

## Application

This unit describes the skills and knowledge required to respond to a range of security incidents in cloud-based environments. It includes defining response objectives and simulating security incidents.

The unit applies to individuals who may work in roles such as security engineers, cloud developers and architects, and information security officers. It also includes individuals responsible for managing operational concerns, including automation and maintaining cloud resources.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

## Unit Sector

Cloud computing

## 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> |

| ELEMENT                                                        | PERFORMANCE CRITERIA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Prepare to respond to cloud security incident               | 1.1 Confirm work brief, risk framework and work tasks according to organisational policies and procedures<br>1.2 Identify organisational IT assets, host and network security, and related risk assessments<br>1.3 Identify domains exposed to potential security incident according to work brief<br>1.4 Confirm attack vector and impact of incident in consultation with required personnel<br>1.5 Create cloud incident plan according to work brief                                                                                                                          |
| 2. Detect and analyse cloud security incident                  | 2.1 Simulate security incident according to work brief<br>2.2 Confirm incident detection by monitoring systems<br>2.3 Record security incident information according to organisational policies and procedures<br>2.4 Review cloud incident findings according to organisational policies and procedures<br>2.5 Implement log capture and replication of relevant data to secure repository with appropriate retention policy<br>2.6 Determine functional impact, information impact and recoverability from incident<br>2.7 Notify required organisational personnel of incident |
| 3. Contain, eradicate and recover from cloud security incident | 3.1 Implement containment strategy to minimise impact according to cloud incident plan<br>3.2 Identify and document source and method of attack<br>3.3 Implement plan to eradicate security threat<br>3.4 Confirm recovery plan, impact to services and loss of data with required personnel<br>3.5 Implement recovery plan for resources and data<br>3.6 Build automated mechanisms for programmed cloud incident triage and response                                                                                                                                            |
| 4. Complete post-incident activities                           | 4.1 Conduct review of incident with required personnel<br>4.2 Identify and document opportunities for improving automated detection, containment, eradication and/or recovery for security incident<br>4.3 Update cloud incident response document and store in required location according to organisational policies and procedures<br>4.4 Recommend updates to organisational policies and procedures to reflect best practice cloud incident response methods<br>4.5 Present recommendations for improving organisational policies and procedures 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                                                                                                                                                                                                                                                                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reading                 | <ul style="list-style-type: none"><li>Organises, evaluates and critiques ideas and information from a range of complex texts</li></ul>                                                                                                                                                                                                              |
| Writing                 | <ul style="list-style-type: none"><li>Prepares technical documentation detailing analysis, work performed and results using succinct language and logical structure</li></ul>                                                                                                                                                                       |
| Planning and organising | <ul style="list-style-type: none"><li>Identifies key factors that impact on decisions and their outcomes, drawing on experience, competing priorities, and decision-making strategies</li><li>Plans strategic priorities and outcomes in a flexible, efficient and effective context and diverse environment exposed to competing demands</li></ul> |
| Self-management         | <ul style="list-style-type: none"><li>Develops and implements strategies that confirm that organisational policies and procedures and regulatory requirements are being met</li></ul>                                                                                                                                                               |
| Technology              | <ul style="list-style-type: none"><li>Demonstrates skills that reflect sophisticated knowledge of principles, concepts, language and practices associated with cloud computing and cloud-based threats</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=a53af4e4-b400-484e-b778-71c9e9d6aff2>

# Assessment Requirements for ICTCLD512 Respond to cloud security incidents

## Modification History

| Release   | Comments                                                                                                                                                                                |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Release 1 | This version first released with the Information and Communications Technology Training Package Version 8.0.<br><br>Newly created unit of competency to address in-demand skills needs. |

## 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:

- respond to at least three different cloud security incidents and update a cloud incident response document for at least one of those incidents.

In the course of the above, the candidate must:

- collect and analyse cloud and system data
- consider procedural improvements to produce repeatable and automated deployments and reduce manual processes
- report unusual cloud-based activities within required timeframes
- apply legislative requirements; governance, risk and compliance (GRC) measures; and organisational policies and procedures.

## 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:

- NIST 800-61 Computer Security Incident Handling Guide
- common causes and impacts of cloud incidents in organisations
- key components of cloud security incident response documentation
- common goals of responding to cloud incident response objectives in organisations, including:
  - recovering affected resources
  - preserving data for forensics
  - data attribution
- methods to prepare for cloud security incidents, including:

- identifying key personnel and supporting resources
- developing incident response plans
- granting provisional access
- using incident response tools
- best practices for regularly simulating security incidents to train staff, and improve configurations and operating procedures
- methods for automating containment of a cloud security incidents and/or affected resources
- functions and features of GRC measures
- types of evidence used in cloud incident investigations, including:
  - cloud service, network, operating system and application logs
  - storage snapshots
  - resource configuration changes
- methods to apply redeployment mechanisms in response to cloud security incidents
- techniques to automate triage and response mechanisms for cloud security incidents
- key information and data required to summarise cloud incident responses
- organisational policies and procedures, and legislative requirements relating to work tasks.

## 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:

- cloud infrastructure that has been exposed to at least three different types of incidents and requires protection controls
- software and hardware required to demonstrate the performance evidence
- opportunities for interaction with stakeholders
- work brief, resources, and organisational policies and procedures required to demonstrate the performance evidence.

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=a53af4e4-b400-484e-b778-71c9e9d6aff2>