Australian Government

Assessment Requirements for ICTCLD512 Respond to cloud security incidents

Release: 1

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. 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