



Australian Government

ICTCLD511 Protect cloud infrastructure and data

Release: 1

ICTCLD511 Protect cloud infrastructure and data

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.

Application

This unit describes the skills and knowledge required to protect networks and resources, and compute both at rest and in transit data in cloud environments.

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>
1. Review cloud usage and risks	1.1 Confirm work brief and tasks according to organisational policies and procedures 1.2 Locate sensitive and regulated data identified in work brief 1.3 Assess data sensitivity and potential risk to organisation 1.4 Review existing data processing services and assess potential risk to organisation 1.5 Review data processing service configuration and identify opportunities to improve security and reduce risk to organisation

ELEMENT	PERFORMANCE CRITERIA
	1.6 Document findings according to organisational policies and procedures, and prioritise recommendations.
2. Implement resource protection controls	2.1 Confirm work brief for network security controls 2.2 Access cloud platform and implement change to environment 2.3 Test security controls and confirm resources are being protected as expected 2.4 Confirm functionality of network resources and rectify any issues 2.5 Document configuration changes according to organisational policies and procedures
3. Implement data encryption at rest	3.1 Confirm work brief for data encryption controls 3.2 Generate and secure encryption key in cloud platform according to organisational policies and procedures 3.3 Encrypt sensitive data with encryption key 3.4 Where practical, demonstrate that data is unreadable without access and use of encryption key 3.5 Demonstrate that encryption key is only accessible by required personnel and services in cloud environment 3.6 Document configuration changes according to organisational policies and procedures
4. Implement data protection controls	4.1 Confirm work brief related to data protection controls 4.2 Identify cloud-based data loss protection (DLP) service 4.3 Enable and configure DLP across organisation's storage and identify sensitive information 4.4 Review DLP reports, document findings and recommend system improvements 4.5 Document configuration changes according to organisational policies and procedures
5. Recommend updates to organisational policies and procedures	5.1 Summarise required changes for organisational policies and procedures 5.2 Present summary to required personnel 5.3 Obtain approval from 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	Organises, evaluates and critiques ideas and information from a range of complex texts
Writing	Prepares technical documentation detailing analysis, work performed and results using succinct language and logical structure
Planning and organising	- Identifies key factors that impact on decisions and their outcomes, drawing on experience, competing priorities, and decision-making strategies - Plans strategic priorities and outcomes in a flexible, efficient and effective context and diverse environment exposed to competing demands
Self-management	Develops and implements strategies that confirm that organisational policies and procedures and regulatory requirements are being met
Technology	Demonstrates skills that reflect sophisticated knowledge of principles, concepts, language and practices associated with cloud computing and cloud-based threats

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 ICTCLD511 Protect cloud infrastructure and data

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:

- configure at least three network controls to protect a web-based application running in a cloud environment, which must include at least one of the following types of controls:
 - web application firewall
 - content delivery network
 - load balancer
 - network access control lists
 - host-based firewalls
- generate and securely manage at least one encryption key used to encrypt data at rest in the cloud
- implement at least one data loss prevention (DLP) system to identify and provide visibility to sensitive data

In the course of the above, the candidate must:

- use cloud management console, cloud software development kits and command line tools
- collect and analyse cloud data and adjust resources as required
- consider procedural improvements to produce repeatable and automated deployments by reducing 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:

- functions and features of GRC measures
- methods to create and defend network layers between resources, including:
 - distributed denial of service (DDoS) protection
 - content distribution networks (CDNs)
- types of network security controls to manage inbound and outbound network traffic and service endpoints
- functions and features of firewalls
- common processes to harden virtual machine images and containers prior to deployment
- common processes to manage vulnerabilities of live resources through patching and configuration rules
- common patterns and services to minimise interactive access to compute resources, including bastion hosts
- common types and key characteristics of sensitive and regulated data
- functions and capabilities of data loss protection (DLP) systems
- methods to implement attribute-based access controls (ABACs) for different data classifications
- data retention policies and how they can be implemented
- methods for managing encryption keys generated by cloud providers
- storage services that support encryption at rest and how this can be monitored and enforced
- services for tracking and auditing access to sensitive data and encryption keys
- secure certificate management and deployment on external network resources, including CDNs, load balancers and application programming interface (API) gateways
- methods to configure networks and application to enforce data encryption in transit
- methods to conduct risk assessments and compliance assessments
- 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 and data that must be protected
- required software and hardware to configure cloud systems
- 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>