



Australian Government

Assessment Requirements for ICTCLD509 Manage cloud identity and access

Release: 1

Assessment Requirements for ICTCLD509 Manage cloud identity and access

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:

- manage cloud identity and access for at least five different users.

In the course of the above, the candidate must:

- review cyber security requirements
- use cloud management consoles, software development kits and command line tools
- reduce unused privileges
- 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:

- features and functions of identity and access management (IAM) systems and GRC measures
- industry technology standards used in cloud computing solutions and services
- tools and functions of security layers and security-focused content in cloud services
- principle and implementation of least privilege
- differences in management of human and machine identities
- advantages of centralised identity providers in organisational environments
- applications of user authentication methods and technologies, including:
 - multi-factor authentication (MFA)
 - password-based authentication

- certificate-based authentication
- security assertion markup language (SAML)
- single sign-on (SSO)
- security benefits of using temporary rather than permanent credentials
- best practices for storage, rotation and audit of permanent credentials
- IAM and resource policy definitions for granting or removing permissions, including:
 - role-based access controls (RBACs)
 - attribute-based access controls (ABACs)
 - permission boundaries to delegate maximum set of permissions
 - cross-account, project, subscription, third-party and public access
- 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:

- IAM systems and user accounts that may be managed
- cloud-based applications, software and hardware
- work brief 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>