



Australian Government

ICTCLD509 Manage cloud identity and access

Release: 1

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.

Application

This unit describes the skills and knowledge required to securely authenticate and maintain cloud-based identity and access management (IAM) systems in organisations. It includes developing, implementing and evaluating secure cloud computing solutions.

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 across cloud environments.

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. Prepare to manage cloud identity and access	1.1 Confirm work brief and tasks according to organisational policies and procedures 1.2 Identify required protocols, platforms and networks in cloud-based infrastructure and confirm interoperability with organisational systems 1.3 Review password and multi-factor authentication requirements 1.4 Discuss limitations of existing cloud-based IAM configuration with required personnel

ELEMENT	PERFORMANCE CRITERIA
	1.5 Confirm new IAM entities that will be required to complete work brief 1.6 Identify required protocols, platforms and networks in cloud-based infrastructure and confirm interoperability with organisational systems
2. Create and secure new IAM users	2.1 Authenticate cloud-based IAM service used by organisation according to work brief 2.2 Modify password policy and enforce password complexity and expiry according to work brief 2.2 Define updated security policies and roles according to work brief 2.3 Create user accounts and associate with required permissions following organisational naming conventions 2.4 Securely share user access credentials with organisational staff 2.5 Enforce multi-factor authentication according to work brief 2.6 Confirm that required staff can access specified account and reset credentials according to organisational processes and procedures
3. Configure machine resource permissions	3.1 Identify cloud-based machine resources requiring IAM permissions according to work brief 3.2 Define and confirm required security policies meet organisational needs 3.3 Check that machine resources have required permissions 3.4 Apply permissions to identified machine resources according to work brief 3.5 Confirm that machine can be accessed by other resources and services as per work brief 3.6 Document changes according to organisational policies and procedures
4. Periodically review IAM configuration	4.1 Track members, activities and permissions in centralised location 4.2 Review activity and recommend permission changes 4.3 Delete permissions and entities that are no longer required 4.4 Document changes according to organisational policies and procedures

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 documentation 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
Self-management	Develops and implements strategies that confirm that organisational policies and procedures are being met

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 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>