TECDT90344

# Implement cloud security

## Overview

This standard is about implementing cloud security.

Cloud security involves protecting data, applications and infrastructure within cloud environments against unauthorised access, data breaches and other security threats. This includes designing, implementing, and maintaining security measures and controls to safeguard cloud-based systems and data.

This standard is for those who need to implement cloud security as part of their duties.

## Performance criteria

*You must be able to:*

1. Engage with cloud architects to identify cloud security requirements in line with organisational risk mitigation strategies
2. Develop and implement cloud security policies and controls in line with organisational security requirements
3. Implement Identity and Access Management (IAM) policies for cloud environments in line with organisational procedures
4. Implement encryption methods to protect data in line with organisational procedures
5. Implement network security controls, including firewalls, intrusion detection/prevention systems, and secure network configurations in line with organisational requirements
6. Monitor network traffic to identify anomalies and events to facilitate analysis, threat mitigation and incident response in line with organisational procedures
7. Conduct routine vulnerability assessments and penetration testing of cloud infrastructure environments, to identify potential security weaknesses
8. Establish and maintain security incident response plans for cloud environments in line with organisational procedures
9. Produce cloud security reports and documentation to record security measures, incidents, and compliance status in line with organisational procedures

## Knowledge and understanding

*You need to know and understand:*

1. Cloud platforms and their built-in security features
2. The main features of secure cloud environments including cloud security architecture, security protocols and components
3. Security responsibilities of both cloud providers and organisations and the shared responsibility models for security risk management
4. Fundamentals of Identity and Access Management (IAM) for cloud environments encompassing authentication, authorisation and accounting mechanisms to control access
5. How to implement Role-based Access Control (RBAC) to enable minimal access privileges in cloud environments
6. How to deploy Multi-Factor Authentication (MFA) and Single Sign-On (SSO) solutions to improve access control mechanisms for cloud applications
7. Hoq to implement encryption methods to safeguard sensitive data in cloud environments
8. How to configure Virtual Private Clouds (VPCs), subnets and segmentation within cloud environments to improve security
9. Network Access Control Lists (NACLs) and security groups and how to apply them to secure cloud resources
10. How to implement and maintain Intrusion Detection and Prevention Systems (IDPS) in cloud environments
11. How to deploy Web Application Firewalls (WAF) and implement Application Programming Interface (API) security measures to protect cloud-based applications from web-based attacks
12. How to monitor cloud network traffic to detect anomalies and events
13. How to conduct vulnerability assessments and penetration for cloud-hosted applications and networks
14. How to undertake cloud security auditing to validate compliance requirements
15. Security Information and Event Management (SIEM) tools used for real-time threat detection in cloud environments
16. How to undertake security incident response in cloud environments
17. How to apply automation tools for security policy enforcement in cloud environments
18. How to identify and mitigate security risks associated with cloud engineering

practices

19. How to analyse cloud security issues to develop effective solutions
20. Security procedures used to escalate cloud security issues and events
21. How to develop cloud security reports for recording security issues and mitigations

TECDT90344

# Implement cloud security

| | |
|---|---|
| **Developed by** | ODAG |
| **Version Number** | 1 |
| **Date Approved** | 24 Apr 2024 |
| **Indicative Review Date** | 01 Apr 2027 |
| **Validity** | Current |
| **Status** | Original |
| **Originating Organisation** | ODAG |
| **Original URN** | TECDT90344 |
| **Relevant Occupations** | Information and Communication Technology Professionals |
| **Suite** | IT(Networking) |
| **Keywords** | Cloud security, cloud engineering, cloud infrastructure |