



Australian Government
Australian Signals Directorate

cyber.gov.au

ASD Essentials for cloud



Essentials

Table of contents

- Introduction** 3
 - Cloud environments covered in this chapter 3
 - ASD Essentials framework structure 3
 - More about the Essentials 4
 - Cloud service models 5
 - Shared responsibility 6
- Cloud chapter elements** 7
 - Domains 7
 - Priority phases 9
- ASD Essentials for cloud matrix**10
 - Matrix structure and use10
 - Capability domains 11

Introduction

The Australian Signals Directorate (ASD) provides cyber security advice and services to government, critical infrastructure, industry, small business and individuals. Part of that function is publishing prioritised, practical guidance that helps organisations direct their finite resources to the mitigations that matter most. This guidance is designed to help these organisations protect cloud environments from sophisticated cyber threats.

Cloud environments covered in this chapter

The ASD Essentials for cloud chapter provides guidance for organisations whose technology environment is delivered entirely through software-as-a-service (SaaS) and platform-as-a-service (PaaS).

A growing number of organisations consume their technology entirely as commercial services, operating no infrastructure or platforms of their own. For them, some of the enterprise IT guidance describes work the provider now performs and cannot be implemented or evidenced by a SaaS or PaaS consumer, including: running and hardening servers, operating networks and maintaining platform runtimes.

This chapter expresses actions and priority phases in practical terms for organisations that primarily rely upon SaaS and PaaS. It focuses effort on the areas that determine a consumer's security posture including identity, data, configuration, applications, integrations and provider assurance.

ASD Essentials framework structure

Every ASD Essentials series chapter uses the same three layers:

- **Principles** describe the security outcomes an organisation aims to achieve.
- **Actions** describe what must be done to achieve them.
- **Domains** describe where that work applies.

The three layers answer a sequence of implementation questions, as shown in Figure 1.

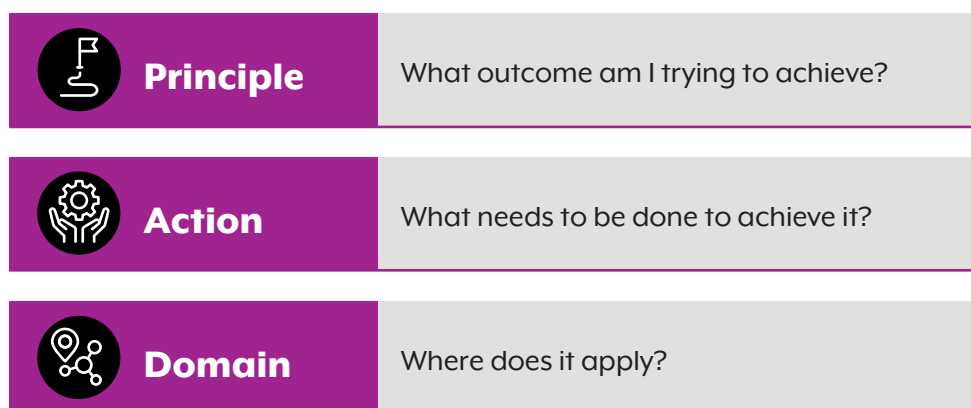


Figure 1. How the ASD Essentials framework layers work

To implement an Essentials series chapter, an organisation works through each **action** in the **domains** to which the action applies. The remaining content supports this implementation.

More about the Essentials

The ASD Essentials series includes the following suite of publications and guidance:

- Overview publications
- ASD Essentials series chapters
- Supplemental publications

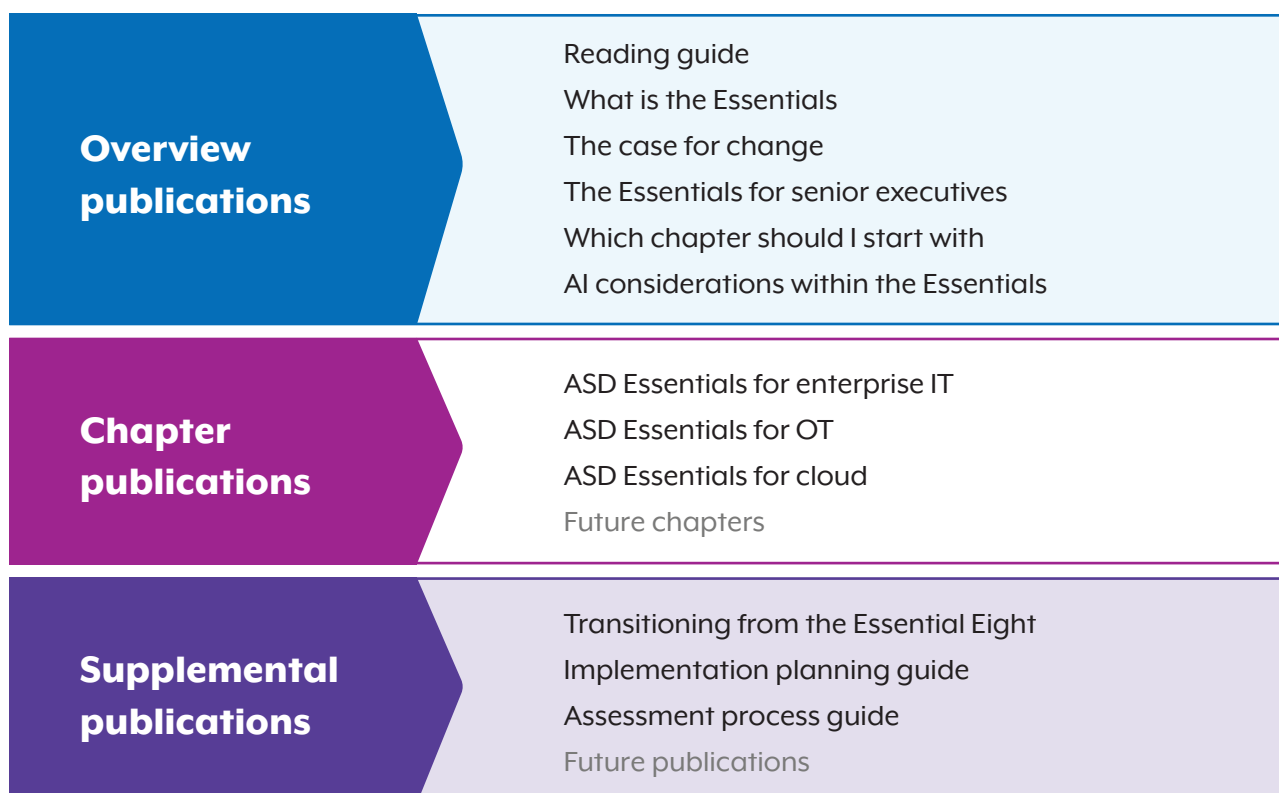


Figure 2. The Essential series

Small and medium sized businesses that do not operate at enterprise scale can still use this guidance where relevant. The security outcomes described by the principles within the Essential series are equally important for smaller organisations. What differs is how those outcomes are achieved and how much responsibility sits with service providers and vendors.

ASD publishes tailored cyber security guidance for small businesses, home offices and individuals at cyber.gov.au

Cloud service models

This publication covers two service models, and the responsibilities differ meaningfully between them.

Software-as-a-service (SaaS) organisations consume finished applications. The provider operates everything beneath the service, and the organisation's responsibilities concentrate on identity, data, tenant configuration, the integrations it connects and provider assurance. Examples include a small Commonwealth entity or statutory body whose entire corporate environment runs on a cloud productivity and collaboration suite, a line-of-business records or case-management system, and a handful of connected SaaS applications; or a service-delivery organisation that operates no servers and administers everything through provider consoles.

Platform-as-a-service (PaaS) organisations build and run their own applications on a provider-operated platform. The provider maintains the platform, runtimes and underlying infrastructure, but the organisation writes the code, selects the dependencies, deploys the workloads and configures the network and access boundaries around them. Examples include an entity delivering a public-facing digital service on a managed application platform and managed database; or a team building internal applications on serverless and container platform services without operating the servers beneath.

The distinction matters because PaaS consumers retain responsibilities that SaaS consumers do not, including securing what they build, patching what they deploy and segmenting the environments they configure. The matrix at Annex A records this explicitly, marking each action against both service models.

Service model boundaries

Few environments map perfectly to a single service model. Some SaaS services now expose customer-configurable capabilities, including low-code or custom application development, scripting and automation or private networking. These capabilities begin to resemble platform services. Where an organisation makes significant use of such capabilities, it should apply the PaaS-marked actions to those services, even where the service is procured as SaaS. Similarly, an organisation using PaaS services that expose direct control over compute or networking is approaching the boundary with IaaS and should consider whether the Essentials for enterprise IT better reflects the responsibilities it holds. Service model boundaries are a matter of degree, and organisations should make a considered judgement about what they actually operate rather than what the procurement label says.

Shared responsibility

When operating within SaaS and PaaS environments organisations share responsibility with the cloud service provider (CSP). Organisations need to understand what security responsibilities they retain, and which responsibilities are delivered by the CSP and require oversight and assurance.

Review ASD's advice on shared responsibility within [Cloud shared responsibility model: Guidance for individuals and small and medium businesses](#).

Each action in the matrix at Annex A carries a marker showing where responsibility for implementing the action typically sits:

- **(C) Customer** – The customer organisation both delivers and operates the controls that implement the action.
- **(S) Supplied** – The provider supplies the required capability, but the customer organisation must enable, configure, operate and monitor it. Each of these instances requires agreement between all parties to understand what the provider is responsible to supply.
- **(P) Provider** – The provider implements the action, and the organisation's task is to verify it through assurance evidence.

These markers guide how each action is implemented and assessed.

For customer actions, the organisation is assessed on the control because it implements it.

For supplied actions, the provider's capability is assumed, and the assessment focuses on the customer's side. This should consider whether the capability has been enabled, configured to the organisation's context, and operated consistently. A capability that exists but has been left at an insecure default, or applied inconsistently, is not yet effective.

For provider actions, the organisation does not implement the control but remains accountable for confirming it is in place. This should draw on current independent assurance recorded against the shared responsibility register, such as an IRAP assessment scoped to the service, features, regions and support arrangements consumed.

The markers reflect the most common consumption pattern and are indicative rather than determinative. An organisation's specific responsibilities may vary depending on the service model, provider arrangements, service tier and configuration choices. This variation is common in PaaS environments where customers often have greater responsibility, of the application security, identity and access management, data protection and platform configurations, compared to a typical SaaS service. Organisations should confirm and document the actual division of responsibility for each service they rely on rather than assuming these markers necessarily apply to those services in every case.

Cloud chapter elements

Domains

The chapter defines eight domains. Six **technical domains** group systems, services and assets that share similar cyber security risks.

Non-production environments, including development, testing and staging, are in scope. Assign them to domains on the same basis as any other asset, according to their function, connectivity, data, privileges and potential impact on production.

Some non-production environments can reach production or change what runs in it. Where an environment holds production trust, administrative access, or the ability to modify or deploy to production, organisations should protect it to the same level as the production environment it can affect.

Two **capability domains** – **Governance and culture**, and **Visibility and response** – apply across all technical domains. Table 1 describes each domain and the cyber security risk it addresses.

Table 1: Domains and risk context

Domain	Description	Risk Context
Governance and culture	Policies, risk management processes, roles and security culture that underpin cyber security program.	Unclear ownership and accountability can lead to inconsistent security decisions and outcomes degrading over time.
Visibility and response	Procedures and capabilities for detecting, analysing and responding to cyber security events and incidents.	Limited visibility and response can delay the detection, analysis and containment of intrusions.
Boundary services	Systems and services that broker connectivity and data flows between SaaS and PaaS services and external or cross-domain environments, including integrations, APIs, gateways, internet-facing services and remote access.	Boundary services expose cloud services, APIs and integrations to external environments, making them frequent targets for scanning, exploitation and initial access.
Identity services	Identity, credential and access management services such as identity providers, authentication and authorisation enforcement solutions or credential stores.	Compromise of identity services can enable an adversary to gain persistent or privileged access to cloud services and organisational data.

Domain	Description	Risk Context
Critical processes and services	Core processes and services that are critical to delivering primary organisational outcomes.	Compromise or loss of these systems can disrupt the organisation's ability to deliver critical outcomes or services.
Privileged environments	Systems and services that support privileged activities, management services and high-impact administrative functions. Including SaaS administration interfaces, PaaS management and deployment services and cloud control-plane capabilities used to configure, monitor and manage services.	Compromise of privileged systems can give an adversary extensive control over systems, services and security controls.
Business systems	SaaS and PaaS services that support enterprise functions and collectively enable organisational operations, including business applications, workflow platforms, data services and custom applications hosted on managed platform services.	Business systems support day-to-day operations and can provide malicious actors with pathways to high-value services, identities and data.
User devices	Endpoints used by the workforce to access SaaS and PaaS services, including desktops, laptops and mobile devices.	User devices are widely distributed and frequently provide malicious actors with an initial foothold into more critical systems.

Priority phases

In each chapter, the domains are grouped into **priority phases**. The phases set out the order in which ASD recommends the domains be addressed. This reflects where ASD assesses that effort delivers the greatest and most rapid reduction in risk.

Priority phases are a sequencing mechanism, not a rating. They do not represent assurance over the effectiveness of controls, compliance against a standard or an organisation's cyber security maturity against a particular class of adversary. The recommended sequence is designed to support organisations to progress through each phase, scaling and hardening their environments as they go, reducing the organisations' overall cyber security risk.

The two capability domains (**Governance and culture**, and **Visibility and response**) apply across all phases and expand as implementation progresses.

ASD recommends implementing the technical domains in the sequence shown to focus cyber security effort where it provides the greatest benefit against current adversary tradecraft.

Refer to the *Implementation planning guide* for detailed planning advice.

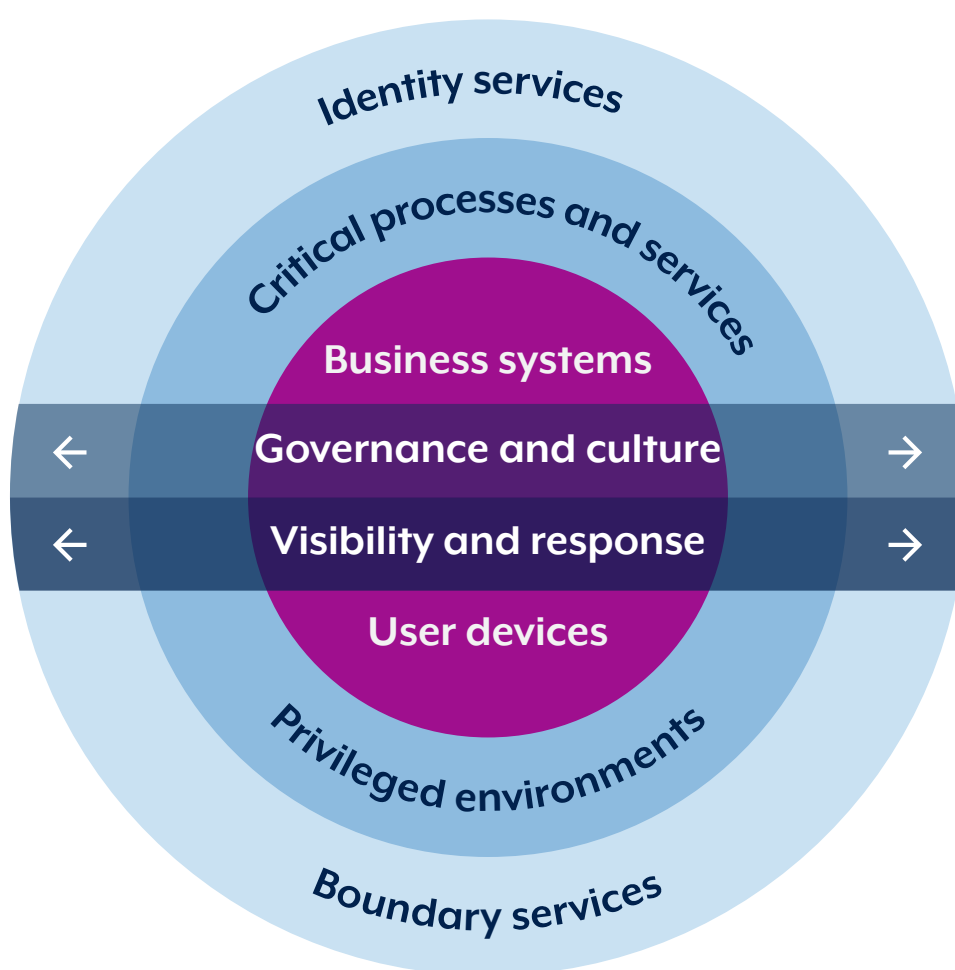


Figure 3. ASD Essentials for cloud priority phases

ASD Essentials for cloud matrix

Matrix structure and use

Each principle states a cyber security objective drawn from ASD's *Information Security Manual* (ISM). Principles align with the corresponding ISM principle identifier, such as GOV-01. These identifiers are provided for traceability and do not indicate an implementation order.

Actions describe what organisations must do to achieve each principle in technology-agnostic terms. Organisations implement these actions through controls that are appropriate to their IT environment, risk profile and regulatory obligations. Relevant controls can be found in the ISM and other ASD guidance on [cyber.gov.au](https://www.cyber.gov.au).

For guidance on applying these principles and actions to artificial intelligence (AI), refer to *AI considerations within the Essentials*.

Where applicable, the technical domain matrix maps actions to the MITRE ATT&CK techniques they are intended to address.

The matrices are organised by capability and technical domains:

- **Matrix 1** and **2** cover the two capability domains.
- **Matrix 3** maps actions across the six technical domains.

For definitions of shared responsibility markers (C) Customer, (S) Supplied and (P) Provider, refer to section Shared responsibility.

Capability domains

Governance and culture

Matrix 1: Governance and culture capability domain

Principle	PaaS Shared Responsibility	SaaS Shared Responsibility	Action
GOV-01 - Executive cyber security accountability	C	C	Formally define and establish executive and board-level accountabilities for cyber security, including setting, monitoring and adjusting organisational risk appetite, and review these accountabilities at a defined cadence.
GOV-08 - Executive artificial intelligence accountability	C	C	Establish and maintain executive accountability for the use, governance and risk management of artificial intelligence within the organisation.
	C	C	Require executive or delegate approval before enabling material SaaS or PaaS AI functions, including review of accessible data, permissions, retention, logging, agents and connectors.
GOV-04 - Cyber security resourcing	C	C	Assign sufficient cyber security personnel and resources with the required skills to operate, monitor, maintain and manage the lifecycle of controls across cloud services, and define cyber security responsibilities within role descriptions.
	C	C	Periodically review cyber security resourcing against cyber threat trends, cyber security incident outcomes and organisational changes.
GOV-09 Security risk management responsibilities	C	C	Adoption of high-risk SaaS or PaaS services that store sensitive data or support critical business functions requires executive approval.
	C	C	SaaS or PaaS platforms that organisations configure, monitor, assure or operate, express security requirements as a condition of use.

Principle	PaaS Shared Responsibility	SaaS Shared Responsibility	Action
	S	S	Shared responsibility arrangements for cloud services are understood, documented and incorporated into security risk management activities
GOV-03 - Security risk management assurance	C	C	Establish and maintain an approved risk management methodology and plan that is used to assess and treat cyber security and shared responsibility risks
GOV-11 - Supplier cyber security assurance	C	C	Select and engage suppliers of software, hardware and services on the basis of a cyber supply chain risk assessment proportionate to the risk the supplier introduces, and retain appropriate assurance evidence to support the decision
	C	C	Maintain current, appropriately scoped assurance that suppliers continue to meet their cyber security commitments, and act when assurance lapses, excludes a service or feature in use, or the supplier's risk changes.
	C	C	Maintain a register of inherited and retained security responsibilities per provider, and review it as services change
	C	C	Establish policies that meet your data sensitivity and sovereignty requirements
	C	C	Establish policies that restricts software on cloud services to reputable suppliers
GOV-14 - Legacy system management	C	C	Establish and maintain a process for identifying, assessing and treating cyber security risks associated with legacy systems and unsupported technologies through compensating controls, enhanced monitoring and assurance until the systems can be removed or replaced.
PRO-14 - Cyber security awareness training	C	C	Update and provide cyber security awareness training on a regular basis to reflect current threats and operational considerations.
PRO-06 – Vulnerability management	C	C	Prioritise cloud services that maximise provider-managed security responsibilities and minimise customer-managed components, where this is consistent with organisational, security and business requirements.

Visibility and response

Matrix 2: Visibility and response capability domain

Principle	PaaS Shared Responsibility	SaaS Shared Responsibility	Action
IDE-01 - Asset identification	C	S	Use an approved asset inventory mechanism that supports automated discovery to detect new and changed non-physical assets including short-lived containers and virtual machines.
	C	S	Identify sanctioned and unsanctioned services, tenants and integrations and promptly bring them under organisational governance.
IDE-04 - Security risk identification	C	C	Identify relevant weaknesses, malicious actor techniques and cyber threat behaviours when undertaking risk assessments and review these inputs on a continuous basis
PRO-13 - Identity, credential and access management	S	S	Regularly scan codebases, configuration files, file shares and user collaboration platforms to identify unsecured keys, secrets credentials and tokens
DET-01 - Centralised event logging	S	S	Establish a centralised event log storage capability that protects logs from unauthorised access, modification or deletion
DET-02 - Cyber security event detection	S	P	Ensure detection logic identifies unauthorised changes, anomalous authentication activity and anomalous control-plane activity, including consent grants, federation changes and privilege elevations
	S	P	Baseline resource utilisation to monitor for and detect anomalous activity
DET-03 - Cyber security incident identification	S	S	Triage alerts and events in a timely manner to determine whether cyber security incident thresholds have been met
	S	S	Use available indicators from all connected sources, rather than isolated signals, when performing cyber security incident identification activities
DET-05 - Detection capability efficacy	C	C	Review detection coverage periodically to identify gaps arising from new cloud services, integrations or architectural changes

Principle	PaaS Shared Responsibility	SaaS Shared Responsibility	Action
RES-05 - Cyber security incident coordination	C	C	Integrate external coordination obligations and requirements into incident response activities, including provider notifications arrangements, escalation contacts and the division of investigative responsibilities under shared responsibility
RES-03 - Cyber security incident response	C	C	Use documented, tested and approved incident response procedures when responding to cyber security incidents, covering tenant and identity-provider compromise, provider-side incidents, token and session revocation, removal of unauthorised consent grants and validation of a trusted state before resuming operations
RES-04 - Cyber security incident insights	C	C	Perform post-cyber security incident reviews to identify the security gaps that enabled each stage of the cyber security incident.
	C	C	Evaluate monitoring coverage and cyber security incident response procedures following cyber security incidents.

Technical domains

Matrix 3: Technical domains

Principle	Cloud actions	PaaS shared responsibility	SaaS shared responsibility	MITRE ATT&CK	Identity services	Boundary services	Critical processes and services	Privileged environments	Business systems	User devices
IDE-01 - Asset identification	Maintain current records of identities, non-person identities, integrations, data and cloud regions, using automated discovery where available to detect new and changed assets.	C	C	Cloud Service Dashboard Cloud Service Discovery Unused/Unsupported Cloud Regions	✓	✓	✓	✓	✓	✓
PRO-01 – Secure system lifecycle	Develop and use a controlled process to onboard, configure and exit services, verifying data retrieval, deletion and access revocation.	S	S	Valid Accounts Trusted Relationship	✓	✓	✓	✓	✓	✓

Principle	Cloud actions	PaaS shared responsibility	SaaS shared responsibility	MITRE ATT&CK	Identity services	Boundary services	Critical processes and services	Privileged environments	Business systems	User devices
	Harden development pipelines and their credentials, restricting who can approve and deploy changes to production.	S	P	Supply Chain Compromise Valid Accounts Account Manipulation	✓		✓	✓	✓	
	Identify and remediate vulnerable third-party libraries and dependencies before deployment and on an ongoing basis.	C	P	Supply Chain Compromise Exploit Public-Facing Application		✓	✓		✓	
PRO-16 – Cyber supply chain security	Assess and approve applications, integrations and consent grants before permitting access, and review them on a regular basis.	C	C	Trusted Relationship Account Manipulation Valid Accounts Steal Application Access Token	✓	✓	✓	✓	✓	✓
	Assess the integrity and authenticity of images, components and artefacts before they are deployed into services, and verify provenance where suitable supplier evidence is available.	S	P	Supply Chain Compromise Server Software Component Command and Scripting Interpreter Implant Internal Image	✓	✓	✓	✓	✓	
	Use vendor advisories and threat intelligence to maintain awareness of supplier, product and component exposure to compromise, and act within timeframes proportionate to the risk.	S	S	Supply Chain Compromise Server Software Component Trusted Relationship	✓	✓	✓	✓	✓	✓
	Identify and mitigate single points of dependency created by OAuth and federated identity providers.	C	C	Trusted Relationship Steal Application Access Token Forge Web Credentials	✓		✓	✓	✓	

Principle	Cloud actions	PaaS shared responsibility	SaaS shared responsibility	MITRE ATT&CK	Identity services	Boundary services	Critical processes and services	Privileged environments	Business systems	User devices
PRO-13 Identity, credential and access management	Identify and disable or remove default and unused accounts on a regular basis, permitting exceptions only where the account is documented, justified, hardened and monitored. Govern emergency access accounts separately, minimise their number, securely protect their credentials, monitor their use and test them regularly.	S	S	Valid Accounts Brute Force	✓	✓	✓	✓	✓	✓
	Monitor services for supply chain compromise, including provider advisories and changes to security commitments, and respond in a timely manner.	S	S	Supply Chain Compromise Server Software Component	✓	✓	✓	✓	✓	✓
	Store credentials, keys, secrets and tokens in approved secure access controlled repositories, and rotate, expire or replace non-person credentials with managed or federated workload identities where supported..	S	S	Unsecured Credentials Credentials from Password Stores Steal Application Access Token Steal or Forge Authentication Certificates	✓					
	Use phishing-resistant MFA for users authenticating to systems.	S	S	Valid Accounts Brute Force Phishing Adversary-in-the-Middle	✓	✓	✓	✓	✓	✓
	Non-person identities are authorised, assigned an owner and constrained to their intended context, with use bound to trusted workload, issuer or service conditions and activity recorded.	S	S	Valid Accounts Steal Application Access Token	✓	✓	✓	✓	✓	

Principle	Cloud actions	PaaS shared responsibility	SaaS shared responsibility	MITRE ATT&CK	Identity services	Boundary services	Critical processes and services	Privileged environments	Business systems	User devices
	Disable legacy authentication protocols or, where this is not feasible, restrict and monitor their use, apply compensating controls and establish a time-bound decommissioning plan.	S	S	Brute Force Valid Accounts Account Manipulation	✓	✓	✓	✓	✓	✓
	Ensure that user and non-person credentials are unique per system or account, particularly in high-privilege contexts.	C	C	Brute Force Valid Accounts	✓	✓	✓	✓	✓	✓
PRO-12 – Least privilege access	Periodically review and update access privileges in alignment with current roles, duties and business requirements.	S	S	Account Manipulation Valid Accounts	✓	✓	✓	✓	✓	
	Restrict permissions to create, modify, or delete accounts and roles, or to access privileged functions or applications, to authorised administrative roles.	S	S	Create Account Account Manipulation Permission Groups Discovery Account Discovery Account Access Removal	✓	✓	✓	✓	✓	
	Provision user, administrative and non-person accounts with only the minimum access and privileges required to perform defined operational functions.	S	S	Create Account Account Manipulation Valid Accounts	✓	✓	✓	✓	✓	
PRO-05 – Secure administration	Ensure administrative activities against cloud management planes are performed only from managed, compliant, hardened devices.	C	C	Valid Accounts Steal Web Session Cookie Steal Application Access Token	✓	✓	✓	✓		

Principle	Cloud actions	PaaS shared responsibility	SaaS shared responsibility	MITRE ATT&CK	Identity services	Boundary services	Critical processes and services	Privileged environments	Business systems	User devices
	Enforce explicit privilege activation before privileged actions are permitted, with approved and time-bound elevation limited to the functions required, and monitor privileged sessions and test response arrangements.	S	S	OS Credential Dumping Valid Accounts Account Manipulation Steal Web Session Cookie Steal Application Access Token Adversary-in-the-Middle	✓	✓	✓	✓		
	Record all administrative or management actions that modify cloud services, configurations or controls with the details of the identity, timestamp and target.	S	S	Impair Defenses Modify Authentication Process Create Account Account Manipulation	✓	✓	✓	✓	✓	
PRO-04 – Secure configuration management	Define approved configuration baselines for cloud services and tenant-level settings, informed by vendor and industry hardening guidance, that disable or remove unnecessary services, insecure settings and unsupported or weak protocols.	S	P	Exploitation of Public-Facing Application External Remote Services Valid Accounts Server Software Component	✓	✓	✓	✓	✓	✓
	Deploy approved configuration baselines across cloud services, preferring policy-as-code and preventative guardrails that block non-compliant configurations at deployment.	P	P	Exploit Public-Facing Application External Remote Services Valid Accounts Account Manipulation Create Account	✓	✓	✓	✓	✓	✓

Principle	Cloud actions	PaaS shared responsibility	SaaS shared responsibility	MITRE ATT&CK	Identity services	Boundary services	Critical processes and services	Privileged environments	Business systems	User devices
	Detect and respond to configuration drift from approved configuration baselines using scheduled technical assessments and, where supported, automated monitoring, based on system criticality and change rate.	S	P	Impair Defenses Modify Cloud Compute Infrastructure Modify Cloud Resource Hierarchy Account Manipulation Create Account Modify Authentication Process External Remote Services	✓	✓	✓	✓	✓	✓
PRO-06 – Vulnerability management	Identify, prioritise and remediate vulnerabilities in customer-introduced applications, integrations and extensions within risk-based timeframes.	C	C	Exploit Public-Facing Application Exploitation for Privilege Escalation	✓	✓	✓	✓	✓	✓
	Apply security patches or updates to customer-managed components within defined risk-based timeframes, or automatically where impact is low.	C	C	Exploit Public-Facing Application Exploitation for Privilege Escalation	✓	✓	✓	✓	✓	
	Remediate or mitigate vulnerabilities exceeding defined risk thresholds within defined risk-based timeframes based on exploitation, exposure, criticality, impact and compensating controls and verify treatment effectiveness.	S	P	Exploit Public-Facing Application Exploitation for Privilege Escalation	✓	✓	✓	✓	✓	
	Test security patches and updates before deployment and maintain tested rollback or recovery procedures to manage adverse operational impacts.	C	P	Exploit Public-Facing Application Exploitation for Privilege Escalation	✓	✓	✓	✓	✓	

Principle	Cloud actions	PaaS shared responsibility	SaaS shared responsibility	MITRE ATT&CK	Identity services	Boundary services	Critical processes and services	Privileged environments	Business systems	User devices
PRO-07 – Trustworthy software	Restrict administrative and management tooling to approved software sets and executed only from authorised privileged systems.	C	C	Impair Defenses Command and Scripting Interpreter Masquerading Remote Access Tools	✓	✓	✓	✓	✓	✓
	Regularly review proposed and approved software and application integrations in the organisational environment	C	C	Supply Chain Compromise Trusted Relationship		✓	✓	✓	✓	
PRO-08 – Cryptographic protection	Permit only supported, verified and organisation-authorised software to execute, with exceptions minimised risk-accepted, time-bound, monitored and regularly reviewed.	S	S	Supply Chain Compromise Implant Internal Image Masquerading User Execution	✓	✓	✓	✓	✓	
	Ensure data in transit and at rest is protected using best practice cryptographic algorithms and protocols, with weak or deprecated options disabled.	S	S	Network Sniffing Adversary-in-the-Middle Data from Cloud Storage	✓	✓	✓	✓		
	Manage cryptographic keys securely throughout their lifecycle, including generation, validation, storage, rotations and revocation.	S	P	Unsecured Credentials Steal or Forge Authentication Certificates Steal Application Access Token	✓	✓	✓	✓		
	Retain customer control over the keys protecting the organisations most sensitive data, including the ability to revoke provider access.	S	S	Data from Cloud Storage	✓	✓	✓	✓		

Principle	Cloud actions	PaaS shared responsibility	SaaS shared responsibility	MITRE ATT&CK	Identity services	Boundary services	Critical processes and services	Privileged environments	Business systems	User devices
PRO-10 – Regular and proven backups	Back up settings, identities, policies, integrations, tenant configurations, and other important data to immutable storage on a defined schedule, implementing customer-controlled backup where provider arrangements are insufficient.	S	S	Data Destruction Data Encrypted for Impact Inhibit System Recovery Data Manipulation	✓	✓	✓	✓	✓	
	Isolate backup repositories from production cloud environments through separate accounts, subscriptions or tenants with independent access controls, preventing unauthorised modification or deletion.	C	C	Data Encrypted for Impact Data Destruction Inhibit System Recovery Data Manipulation	✓	✓	✓	✓	✓	✓
	Conduct regular testing of backup data and restoration procedures to ensure that backups are reliable and capable of meeting defined recovery time objectives and recovery point objectives.	C	C	Data Encrypted for Impact Data Destruction Inhibit System Recovery Data Manipulation	✓	✓	✓	✓	✓	
	Establish recovery arrangements with the service provider, covering data loss, malicious deletion and tenant misconfiguration.	S	S	Data Encrypted for Impact Data Destruction Inhibit System Recovery Data Manipulation	✓	✓	✓	✓	✓	
	Vital cloud capabilities that require absolute availability for mission critical objectives are able to be quickly rebuilt on another provider if organisational needs demand.	S	S	Data Destruction Inhibit System Recovery Service Stop			✓	✓		

Principle	Cloud actions	PaaS shared responsibility	SaaS shared responsibility	MITRE ATT&CK	Identity services	Boundary services	Critical processes and services	Privileged environments	Business systems	User devices
PRO-18 – Network segmentation and segregation	Isolate workloads within network zones and limit lateral movement to explicitly approved pathways and service trust.	C	P	Remote Services Exploitation of Remote Services Lateral Tool Transfer Network Service Discovery Use Alternate Authentication Material	✓	✓	✓	✓		
PRO-09 – Content filtering	Block outbound network connections to known malicious or untrusted destinations.	S	P	Exfiltration Over C2 Channel Exfiltration Over Alternative Protocol Proxy Exfiltration Over Web Service Application Layer Protocol		✓	✓	✓	✓	✓
	Inspect and control outbound flows from cloud services to detect unauthorised transfer of sensitive or high-value data.			Exfiltration Over C2 Channel Exfiltration Over Alternative Protocol Proxy	✓		✓	✓	✓	✓
	Inspect inbound content from external or untrusted sources to prevent delivery of malicious or unsafe content.	S	P	Phishing Ingress Tool Transfer User Execution		✓	✓		✓	
PRO-14 – Cyber security awareness training	Ensure all personnel receive cyber security awareness training, that is tailored to how they will interact with organisational systems in their assigned roles, before being granted access to organisational systems and data.	C	C	Phishing Valid Accounts User Execution	✓	✓	✓	✓	✓	✓

Principle	Cloud actions	PaaS shared responsibility	SaaS shared responsibility	MITRE ATT&CK	Identity services	Boundary services	Critical processes and services	Privileged environments	Business systems	User devices
DET-01 – Centralised event logging	Enable provider audit logging at sufficient tiers and retention, and forward security-relevant logs and configuration changes to a central capability.	S	S	Disable or Modify Tools Account Manipulation Create Account Modify Cloud Resource Hierarchy Modify Authentication Process Modify Cloud Compute Infrastructure	✓	✓	✓	✓	✓	✓
DET-04 – Baseline high-risk access activities	Continuously monitor and analyse activity against established baselines to detect anomalous use of legitimate identities, services and software.	P	P	Valid Accounts Account Manipulation Use Alternate Authentication Material Remote Access Tools	✓	✓	✓	✓	✓	✓
DET-02 – Cyber security event detection	Ensure event logs are normalised, time-synchronised and enriched to support correlation across cloud services and environments.	S	P		✓	✓	✓	✓	✓	✓

**For more information, or to report a
cyber security incident, contact us:**

cyber.gov.au

1300 CYBER1 (1300 292 371)

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms, the entity's logo, third party content, and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license

<https://creativecommons.org/licenses/by/4.0/>

For the avoidance of doubt, this means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license

<https://creativecommons.org/licenses/by/4.0/legalcode.en>

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website

<https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines>

