



Australian Government
Australian Signals Directorate

cyber.gov.au

Asset scoping guide for cloud

The background of the lower half of the page is an abstract composition of overlapping, translucent purple and blue rectangular planes, creating a sense of depth and modernity.

Essentials

Contents

Purpose	3
Asset scoping	3
Governance and culture	3
Visibility and response	4
Boundary services	5
Identity services	6
Critical processes and services	8
Privileged environments	9
Business systems	10
User devices	11

Purpose

This publication provides supplementary guidance intended to complement the *ASD Essentials for cloud*. It includes further descriptions and context on the two capability domains and six technical domains outlined within the *ASD Essentials for cloud* chapter, as well as some prompting questions to assist organisations as they undertake their own scoping activities.

The questions and examples included below are prompts rather than an exhaustive list. An asset or function may be included in more than one domain, where it performs multiple roles or presents different consequences of compromise.

Asset scoping

The following sections describe each technical domain, the consequences of compromise and questions that can help organisations determine which assets are in scope.

Organisations should assess each asset against every domain description. An asset is in scope for each domain that describes it, and all actions applicable to those domains apply. Where the same actions applied to an asset through more than one domain, it is implemented once. Multi-domain memberships widen the set of actions that apply to an asset, it does not multiply the work for actions already in that set.

Governance and culture

What this domain involves

Governance and culture represent the administrative foundations that give the cyber security program its authority and longevity, including the policies, risk management processes, roles, responsibilities and security culture that underpin every other control. This domain is primarily people focused and process-driven rather than technology-driven.

Consequence of compromise

Weak governance and cyber security culture can result in inconsistent security decisions, unclear accountability, delayed remediation activity and reduced organisational ability to manage cyber security risk across cloud services over time. Deficiencies in this domain may undermine the effectiveness and sustainability of controls implemented across all other domains.

Scoping questions to consider	Example assets
• Does the organisation maintain approved policies and procedures for the use and security of SaaS and PaaS services? • Is there an approved register of SaaS and PaaS services used by the organisation? • Are SaaS and PaaS services subject to risk assessments and approvals before they are procured or on boarded? • Are roles and responsibilities for managing and securing SaaS and PaaS services, including shared responsibilities with cloud service providers, clearly defined? • Are security risks, exceptions, inherited responsibilities and remediation activities for SaaS and PaaS services recorded and regularly reviewed? • Do users and administrators receive security awareness and training relevant to their use of SaaS and PaaS?	• overarching organisational cyber security strategy documents, including cyber security policies and procedures for SaaS and PaaS services. • approved cloud service registers • cloud service provider risk assessments • cloud service procurement and onboarding procedures • cloud shared responsibility matrices • security awareness and training programs • employee codes of conduct • security roadmaps • risk registers for cloud services

Visibility and response

What this domain involves

Visibility and response represent the organisation's ability to detect, analyse and respond to cyber security events and incidents. This domain encompasses the procedures, platforms and capabilities that collect security telemetry then convert it into actionable insight to enable coordinated response and recovery activities when incidents occur.

Consequence of compromise

Without effective visibility, malicious actors can maintain persistence, escalate privileges within SaaS and PaaS services and cause impact without opposition. This can delay incident identification and response, prolong impacts, increase the resources required for resolution and cause greater organisational harm.

Scoping questions to consider	Example assets
• Does the service generate customer accessible audit logs for authentication events, user and non-person identity activity, administrative actions, consent grants, configuration and federation changes, data access and security events relevant to the service? • Can relevant SaaS and PaaS logs be accessed retained and exported for monitoring, correlation and investigation? • Are logs and alerts from the service integrated with the organisation's security monitoring capability, and can they be correlated with identity, endpoint and other cloud service telemetry? • Are suspicious activities within the service detected and investigated? • Are incident response plans and procedures documented for the SaaS or PaaS service? • Can the organisation revoke sessions, disable accounts, credentials or integrations, preserve relevant evidence and coordinate with the provider during an incident? • Are material security logs unbailable to the customer, restricted by service tier or retained for less than organisational requirements?	• SaaS application cloud services registers • incident response plans and procedures for SaaS and PaaS services • SaaS and PaaS audit logs and activity logging configurations • SaaS and PaaS security monitoring and alerting configurations • extended detection and response solutions incorporating SaaS and PaaS signals • security information and event management (SIEM) solutions integrating SaaS and PaaS telemetry • threat detection, investigation and response procedures for cloud services

Boundary services

What this domain involves

Boundary services represent the systems and services that control or broker connectivity, trust, control or data flows between SaaS and PaaS services and external or cross-domain environments, including internet facing services, APIs, gateways, federation relationships, cross-tenant connections and integrations. This domain is often the organisation's front door and the most visible target for external malicious actors.

Consequence of compromise

Malicious actors routinely scan internet-facing services, APIs and cloud service integrations to enable initial access. Web applications, application programming interface endpoints, SaaS and PaaS integrations and remote access portals are frequently targeted assets. A compromised boundary service can enable unauthorised access to cloud services, expose data, disrupt service disruption visible to customers and partners, or provide a staging point for attacks against connected third parties.

Scoping questions to consider	Example assets
• Is the system, or any of its interfaces (e.g., web portals, application programming interfaces (APIs) or webhooks), directly reachable from the public Internet? • Is any part of the system reachable by external users, services, tenants or third parties? • Would compromise of this system allow an attacker to gain access to connected SaaS or PaaS services or sensitive environments from outside of the organisation? • Does the system expose a public endpoint or externally accessible management interface? • Does the system serve as a boundary or bridging point between external users, identities, tenants or services and organisational SaaS or PaaS services? • Does the system use APIs, webhooks, connectors, gateways, federation or delegated administration to exchange data, trust or control with external parties or other cloud services?	• SaaS and PaaS application access portals • remote access services used to access SaaS and PaaS • SaaS and cloud email services and gateways • cross-organisation SaaS integrations and interagency cloud service integrations • API endpoints • SaaS and PaaS integrations and connectors • Integration-platform-as-a-service (iPaaS) solutions • API gateways and publishing platforms

Assets commonly shared with other domains

An asset that brokers external connectivity is often in scope for other domains as well, including the following examples:

- An internet-facing application that delivers a primary organisational outcome is also a **critical process and service**.
- A cloud service boundary that authenticates external users is also an **identity service**.
- A remote access solution used by administrators is also part of a **privileged environment**.

Identity services

What this domain involves

Identity services represent the functions responsible for authentication, authorisation, identity lifecycle management and access control policy enforcement. This domain is the trust anchor for every other technical domain. If malicious actors control identity, they typically control access to everything.

Consequence of compromise

Compromise of identity services enables broad, cascading access across SaaS and PaaS services. Malicious actors who gain control of identity providers, federation platforms or credential stores can impersonate any user, escalate to any privilege level and move between cloud services without triggering controls that rely on identity as a trust signal. Compromise of identity services can occur at multiple stages of an attack chain, from initial credential theft to the establishment of persistent attacker-controlled access that persists across SaaS sessions, tokens and federated access.

Scoping questions to consider	Example assets
• Does the system authenticate users to systems other than itself, including by verifying passwords, multi-factor authentication (MFA), certificates or tokens? • Does the system create, modify, disable or delete user accounts, service accounts, application identities or workload identities, that are used beyond the system itself? • Does the system manage user permissions, roles, or entitlements that take effect in other systems? • Does the system manage identity attributes, such as a user's name, job title or department, that other systems rely on? • Does the system serve as a trust anchor or central point of control for access across SaaS and PaaS services? • Is the system responsible for issuing, validating, exchanging or revoking authentication or authorisation artefacts, such as Open Authorization (OAuth) access or refresh tokens, OpenID connect identity tokens, Security Assertion Markup Language (SAML) tokens, JSON Web Tokens (JWT), certificates or session tokens? • Is the system an identity provider (IdP) for single sign-on (SSO), federation or cross-tenant authentication? • Does the system store, issue or broker credentials, keys or secrets used by people or by other systems? • Does the system enforce access policies (e.g. conditional access, authentication strength, password, session or privilege requirements)? • If this system were compromised, could an attacker leverage it to create, modify or delete accounts, elevate their privileges, or manipulate group memberships or role assignments in other systems? • Does the service maintain local, emergency or recovery accounts, application identities, workload identities, API keys, certificates or secrets outside the central identity provider?	• identity, credential and access management solutions • identity providers and single sign-on platforms • SaaS and PaaS identity and access management configurations • federation services • credential stores, including enterprise password managers and secrets vaults • authentication mechanisms • token and session management services • privileged access management (PAM) solutions • service identities and service accounts • systems that provision accounts or entitlements into other systems, such as a human resource system that drives joiner, mover and leaver processes

Critical processes and services

What this domain involves

Critical processes and services represent the process and services essential to delivering primary organisational outcomes or contributing to personnel health and safety. They include the cloud applications, platform services, workflows and data on which those outcomes depend. This is the domain where compromise is most likely to translate directly into mission or business objective failure.

Consequence of compromise

Malicious actors targeting this domain typically pursue disruption, unauthorised access and theft or manipulation. Because these services and data they process represent the high value targets, they attract capable and deliberate malicious actor activity.

Scoping questions to consider	Example assets
• Is the system directly tied to the organisation's primary mission or core business functions? • Would the organisation fail to deliver essential services if this system were unavailable? • If the system became unavailable, would consequential impacts occur within the organisation or for customers, partners or the community? • Would compromise of the system result in regulatory, legal, or reputational consequences? • Is the data unique, sensitive, irreplaceable, or extremely costly to reconstruct? • Has this system previously been identified as high risk or mission critical through a business impact assessment, risk assessment or equivalent process? • Do multiple other systems depend on this system, its data, identities, integrations, cloud region or provider features functioning correctly? • Would the system, or the data contained within it, represent a priority target for a malicious actor to gain access to? • Could loss of tenant configuration, automation, encryption keys, application code or provider recovery capability prevent restoration?	• intellectual property and proprietary data within business services • customer data, personally identifiable and sensitive personal information within SaaS and PaaS services • Financial, payment and revenue generating services and capabilities • key business applications and cloud services • email systems and other key communication platforms • SaaS and PaaS repositories and collaboration platforms containing critical business data • application data stores and service-managed data repositories • custom business applications, workflows and automation services hosted on PaaS platforms

Privileged environments

What this domain involves

Privileged environments represent the platforms, tooling, accounts and controls interfaces that enable and govern privileged activities and high-impact administrative functions. This domain encompasses the environments from which administrative actions are performed, the platforms and control planes that broker and enforce privileged access, and the policies and mechanisms that constrain how elevated permissions are granted, used and recorded.

Consequence of compromise

Malicious actors who obtain privileged access can modify configurations, weaken or disable controls, create persistence mechanisms and access or expose data within scope of those privileges. Techniques such as credential theft, token manipulation and exploitation of misconfigured delegation or control plane settings are standard components of post-compromise activity. Once privileged environments are compromised, malicious actors operate with the same authority as the organisation's own privileged users, enabling them to reshape SaaS and PaaS services, abuse integrations, establish persistence and undermine detection and recovery.

Scoping questions to consider	Example assets
• Does the service allow users to perform administrative actions or grant elevated permissions beyond normal user roles? • Does the service manage or control core cloud services (e.g., identity platforms, SaaS tenant settings, PaaS management planes, deployment services or security controls)? • Is the service an entry point into sensitive or high-value systems? • Does the service, identity, device or interface enable, broker or govern elevated control over cloud services, identities, configurations, data or security controls? • Would losing control of this system disrupt the organisation's security posture or operational integrity? • Is the service a dependency for identity, access control, deployments or administration functions? • Would compromise of the service provide an attacker with broad or unrestricted control? • Can an automation identity, deployment pipeline, integration, delegated administrator or management API perform privileged actions?	• secure administrative workstations and privileged access workstations • privileged identity management solutions • privileged access management solutions • SaaS administration portals and management consoles • PaaS management consoles and deployment interfaces • management APIs and automation interfaces • SaaS and PaaS tenant, subscription and account configuration settings • SaaS and PaaS control plane configurations and policy settings • identity federation and privileged role configuration • SaaS and PaaS integrations and connector configurations with elevated permissions • configuration and endpoint management platforms

Business systems

What this domain involves

Business systems represent supporting enterprise functions that enable day-to-day operations, but have not been classified as critical processes and services. Their individual or collective compromise can degrade organisational effectiveness and provide pathways to more sensitive services, identities and data.

Consequence of compromise

Malicious actors frequently use business systems as staging points to access additional cloud services, identities, data and business functions. The disruption or compromise of multiple business systems in parallel can render the organisation unable to perform coordination, communication and operational activities.

Scoping questions to consider	Example assets
• Is the system used to support routine business activities (e.g., productivity, communication, collaboration, service management, document storage, workflow or automation)? • Would loss of the service disrupt routine operations while allowing the organisation's primary outcomes to continue through alternative processes or within tolerable timeframes? • Does the system integrate with other core business systems? • Would the disruption or compromise of this system degrade organisational effectiveness or communication and co-ordination? • Does the system hold accounts, roles or entitlements that govern what users can do within it? • Does the service host customer developed applications, workflows, scripts or integrations or allow users to connect organisational data to external services?	• corporate management systems • SaaS business applications • PaaS hosted business applications and supporting services • IT service management (ITSM) and service management SaaS platforms • office productivity applications • collaboration and messaging SaaS platforms • SaaS and PaaS repositories and collaboration workspaces containing operational data • workflow, automation and low-code platforms supporting business operations

User devices

What this domain involves

User devices represent the endpoints issued to, or used by, the workforce to access SaaS and PaaS services, together with the endpoint applications and locally stored data that enable that access. This domain is highly distributed and exposed to user-initiated risk.

Consequence of compromise

User devices are a common vector through which phishing, social engineering and drive-by compromises reach organisations. A compromised user device can expose credentials, browser sessions or tokens used to access SaaS and PaaS services. User devices are a common point from which data leaves the organisation through exfiltration, accidental exposure or unsanctioned cloud services. Their volume and diversity make consistent security challenging.

User devices are also the most common point from which data leaves the organisation, whether through exfiltration, accidental exposure or unsanctioned SaaS cloud services. The volume and diversity of user devices make this domain the most challenging to secure consistently.

Scoping questions to consider	Example assets
• Is the device (e.g., desktop, laptop, mobile device, tablet or virtual desktop) used by standard users to access organisational SaaS or PaaS services or data? • Do users utilise web browsers or client applications on the device to perform daily work tasks, such as email, collaboration tools, or accessing SaaS business applications? • If a malicious actor gained access to the device, could it capture credentials, browser sessions or tokens, access SaaS or PaaS services, or exfiltrate organisational data? • Is the device unmanaged, personally owned or otherwise not fully controlled by the organisation or is its compliance or management status used as a condition of access? • Is the endpoint used for privileged administration?	• desktop computers and laptops used to access SaaS and PaaS services • virtual desktop environments used to access SaaS and PaaS services • enterprise managed mobile devices, such as mobile phones and tablets • unmanaged or bring your own devices (BYOD) accessing SaaS and PaaS services • web browsers, client applications and extensions used to access cloud services.

**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>

