



Australian Government
Australian Signals Directorate

cyber.gov.au

Asset scoping guide for enterprise IT



Essentials

Table of contents

- Purpose 3
 - Boundary services 3
 - Identity services 4
 - Critical processes and services 5
 - Privileged environments 6
 - Business systems 8
 - User devices 9

Purpose

This annex provides supplementary guidance to support asset scoping for the six technical domains in *ASD Essentials for enterprise IT*. It complements the *Implementation planning guide* by providing additional context for each domain, example assets and questions organisations can use when scoping their enterprise IT environment.

The *ASD Essentials for enterprise IT* has eight domains. Two of them, governance and culture and visibility and response, describe organisational capabilities rather than assets and systems, so they are not scoped using this annex.

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

Organisation 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.

Boundary services

What this domain involves

Boundary services include assets at network boundaries that broker connectivity and data flows between environments of different trust levels. They can include internet-facing services, cross-domain gateways, interagency connections, cloud service boundaries and operational technology (OT) boundaries.

Because these assets sit at trust boundaries and can provide pathways into an organisation's environment, they are commonly targeted by external malicious actors.

Consequence of compromise

Malicious actors routinely scan for and exploit vulnerabilities in internet-facing services to gain initial access. Common targets include email gateways, virtual private network (VPN) concentrators, web applications and remote access portals.

Compromise of a boundary service can enable access to internal networks, data interception, disruption of customer or partner facing services, and the staging of attacks against third parties.

Scoping questions to consider	Example assets
• Is the system directly reachable from the public Internet? • Is any part of the system reachable without connecting to an internal network or VPN? • Could compromise of the system allow a malicious actor to pivot into internal networks or sensitive environments from outside the organisation? • Is the system placed in a demilitarized zone (DMZ) or other exposed network segment? • Does the system provide a boundary or bridging point between external users and internal environment?	• VPN concentrators • remote access solutions • enterprise routers and switches that facilitate traffic between the internet to internal networks • web servers and web applications • application programming interface (API) endpoints • email gateways • network and web application firewalls

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 include corporate identity, credential and access management services such as directories, authentication and authorisation services, federation platforms and credential stores.

These services support authentication, authorisation, identity lifecycle management and the enforcement of access control policies across the enterprise IT environment.

A system is in scope for this domain where its identity functions have effect beyond the systems itself. Many **critical processes and services** and **business systems** manage their own accounts, permissions and roles, and that alone does not make them identity services. A system is an **identity service** where compromise of its identity functions would give a malicious actor access to other systems, for example because it authenticates users to those systems, issues tokens they accept, or feeds accounts and entitlements into services that do.

Consequence of compromise

Compromise of identity services can enable broad, cascading access across the IT environment. A malicious actor who gains control of directory services, federation platforms or credential stores may be able to impersonate users, escalate privileges and move laterally while bypassing controls that rely on identity as a trust signal.

Identity services can be compromised at multiple stages of an attack, from initial credential theft through to the establishment of persistent access that survives changes to individual accounts or credentials.

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 or deactivate user accounts that are used beyond the systems 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 act as a trust anchor or central point of control for access across the enterprise? • Is the system responsible for issuing or validating security tokens, such as OAuth tokens, Security Assertion Markup Language (SAML) tokens or JSON Web Tokens (JWTs)? • Does the system operate as an identity provider (IdP) for single sign-on (SSO) authentication? • Does the system store, issue or broker credentials, keys or secrets used by people or by other systems? • Does the system enforce enterprise access policies, such as conditional access, password policies or privilege requirements? • Could compromise of the system allow a malicious actor to create, modify or delete accounts, elevate privileges, or manipulate group memberships or role assignments in other systems?	• Identity, credential and access management (IAM) solutions, such as Microsoft Active Directory Domain Services (AD DS) and Microsoft Entra ID • Federation services • Certificate services • Credential stores, including enterprise password managers and secrets vaults • Systems that provision accounts or entitlements into other systems, such as a human resource system that drives joiner, mover and leaver processes

Assets commonly shared with other domains

- A human resources system that feeds accounts into the directory is an **identity service** for that function, and remains a **business system** for its own entitlements and data.
- An enterprise password manager holding credentials for critical systems is also a **critical process and service**.
- A privileged access management platform is also part of a **privileged environment**.

Critical processes and services

What this domain involves

Critical processes and services include the core processes and services that are essential to delivering primary organisational outcomes or contributing to personnel health and safety.

Compromise of assets in this domain can directly affect an organisation's ability to achieve mission or business outcomes.

Consequence of compromise

Malicious actors targeting this domain may seek to disrupt services through ransomware or destructive attacks, or steal high-value information for intelligence, competitive advantage or extortion.

The operational importance of these assets and the potential consequences of their compromise can make them attractive targets for capable and deliberate malicious actors.

Scoping questions to consider	Example assets
• Is the system directly linked to the organisation's primary mission or core business functions? • Would the organisation be unable to deliver essential services if the system became unavailable? • Would the system becoming unavailable have significant consequential impacts on other parts of the organisation? • Would compromise of the system result in significant regulatory, legal or reputational consequences? • Is the data stored or processed by the system unique, sensitive, irreplaceable or extremely costly to reconstruct? • Has the system previously been identified as high risk or mission critical? • Do multiple other systems depend on the system functioning correctly? • Would the system, or the data it contains, be an attractive target for a malicious actor?	• Data stores containing intellectual property • Data stores containing customer data, personally identifiable information or other sensitive personal information • Financial or payment services and capabilities • Key business applications and services • Email systems and other key communication platforms • Backup and disaster recovery systems • Code repositories containing critical application code and data • Enterprise password managers

Assets commonly shared with other domains

Backup and disaster recovery systems are also part of a **privileged environment** where they are administered through dedicated management tooling.

Email systems are also **boundary services** at the gateway, and **business systems** in the collaboration functions they provide. Data stores are in scope for this domain based on the sensitivity or irreplaceability of the data they hold, and remain business systems where they also support day to day operations

Privileged environments

What this domain involves

Privileged environments include the systems, services, infrastructure, tooling, accounts and controls that support privileged activities, management services and high-impact administrative functions.

This includes the environments from which administrative actions are performed, platforms that broker and control privileged access, and mechanisms that govern how elevated permissions are granted, used and recorded.

Privileged accounts exist on systems throughout the environment. The presence of a privileged accounts on a system does not place that system in this domain. This domain covers the systems and tooling used to perform, broker and control privileged activity. Actions relating to accounts, credentials and access privileges apply across every domain in which those accounts exist, not only to this domain.

Consequence of compromise

Malicious actors who obtain privileged access can modify configurations, disable security controls, establish persistence and access data within the scope of those privileges.

Credential theft, token manipulation and exploitation of misconfigured delegation are common post-compromise techniques. Once privileged environments are compromised, malicious actors can operate with the authority of legitimate privileged users, making malicious activity more difficult to distinguish from authorised administration.

Scoping questions to consider	Example assets
• Does the system or service allow users to perform administrative actions or obtain permissions beyond those available to standard users? • Does the system or service manage or control core infrastructure services, such as directory services, identity platforms, network controllers or hypervisors? • Does the system or service provide direct or indirect administrative access to critical assets or operational environments? • Does the system or service provide an administrative entry point into sensitive or high-value systems? • Is the system or service regularly used by administrators, engineers or other privileged users rather than standard users? • Would losing control of the system or service significantly affect the organisation's security posture or operational integrity? • Is the system or service a dependency for identity, access control or administrative functions? • Could compromise of the system or service provide a malicious actor with broad or elevated control of other assets?	• Secure admin workstations (SAWs) and privileged access workstations (PAWs) • Privileged identity management (PIM) solutions • Privileged access management (PAM) solutions • Jump servers • Cloud management platforms • Administrative tooling, such as database administration clients, directory management tools and hypervisor management consoles • Configuration and endpoint management platforms used to administer the device fleet

Assets commonly shared with other domains

- A privileged access management platform is also an **identity service**.
- A remote access solution used for administration is also a **boundary service**.
- An endpoint management platform is also a business system where it supports day to day operations.

Business systems

What this domain involves

Business systems are supporting enterprise functions that collectively enable day-to-day organisational operations. Individual systems may not meet the threshold for critical processes and services, but their disruption or collective compromise can degrade the organisation's ability to operate effectively.

Consequence of compromise

Compromised business systems can provide pathways for malicious actors to move laterally towards more sensitive or critical systems.

Disruption across multiple business systems can also affect an organisation's ability to coordinate, communicate and perform administrative or logistical activities.

Scoping questions to consider	Example assets
• Is the system relied on to remain highly available to minimise impacts on upstream or downstream operations? • Does a third-party supplier have obligations or expectations relating to the availability of the system? • Does the system integrate with other core business systems? • Would disruption or compromise of the system degrade organisational effectiveness, communication or coordination? • Could compromise of the system introduce or increase supply chain risk? • Does the system hold accounts, roles or entitlements that govern what users can do within it?	• Corporate management systems • Cloud applications • IT service management (ITSM) systems • Office productivity applications • Collaboration and messaging tools

Assets commonly shared with other domains

- A business system that becomes essentials to delivering a primary organisational outcome is also a critical process and service
- A business system that provisions accounts of entitlements into other systems is also an identity service
- A business systems reachable from the internet is also a boundary service

User devices

What this domain involves

User devices are endpoints issued to the workforce, including desktop computers, laptops, virtual desktops and enterprise-managed mobile devices.

Their widespread use and exposure to user-initiated activity make them common entry points for malicious actors seeking access to an organisation's environment.

This domain is scoped by how a device is used rather than by the kind of device it is. A workstation used for standard user activity is a user device. A workstation used to perform administrative work is part of a privileged environment, and where it used for both, it belongs to both.

Consequence of compromise

User devices are common vectors for phishing, social engineering and drive-by compromise. A compromised user device can provide a malicious actor with a foothold from which to move laterally through the environment.

User devices are also common points at which content from external or untrusted sources is received, opened and processed, and common points from which organisational data can leave the environment, including through malicious exfiltration, accidental exposure or the use of unsanctioned applications. The volume and diversity of user devices can make security controls more difficult to apply consistently.

Scoping questions to consider	Example assets
• Is the device used by standard users to access organisational systems or data? • Do users use the device or system to perform day-to-day work, such as accessing email, collaboration tools or business applications? • Could compromise of the device allow a malicious actor to capture user credentials, access internal networks or systems, or exfiltrate organisational data?	• Desktop computers and laptops • Virtual desktops used for standard user access • Enterprise-managed mobile devices, such as mobile phones and tablets

**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>

