



Australian Government
Australian Signals Directorate

cyber.gov.au

ASD Essentials series

Glossary

Essentials

Glossary

actions	A technology-agnostic description of a technical or procedural control that supports the achievement of a cyber security principle.
action sequencing	The recommended order in which domains should be addressed when applying the framework
attack surface	The systems, services, interfaces and access pathways that could be targeted or exploited by a malicious actor.
baseline (behavioural)	A baseline of user activity, such as typical login patterns, resource access habits and anomalous actions.
baseline configuration	A documented configuration standard that has been formally reviewed and approved by an appropriate authority within the organisation.
boundary services (domain)	Systems positioned at network boundaries that broker connectivity between internal and external environments, including internet services and edge devices.
break-glass account	An emergency account reserved for exceptional situations where normal access methods are unavailable.
business systems (domain)	Supporting enterprise functions that collectively enable organisational operations.
cloud service provider (CSP)	An organisation that delivers cloud services and is responsible for operating elements of those services under a shared responsibility model.
compensating control	An alternative control that delivers the same intended security outcome as a primary action, where that action cannot be applied.
configuration drift	A change in the actual configuration of a system away from its approved baseline
control plane or management plane	The interfaces and services used to configure, manage and administer cloud services, including administration portals, management APIs, automation interfaces and policy configuration layers
critical processes and services (domain)	Core processes and services that are essential to delivering primary organisational outcomes or contributing to personnel health and safety.

cross-cutting (technology)	A solution, capability or control that applies across multiple domains rather than being specific to one.
customer responsibility	A cyber security responsibility implemented and operated by the customer.
cyber security principle	An enduring cyber security objective drawn from the ASD information security manual.
cyber threat	Any circumstance or event with the potential to harm systems.
domain	Groupings of business functions and assets that share similar risks.
endpoint (technology)	A device used by personnel to access organisational systems and data.
federation (Identity)	A trust relationship between identity systems that allows authentication and authorisation in one system to be recognised by another
governance and culture (domain)	The policies, risk management processes, roles, responsibilities and security culture that underpin the cyber security program.
identity Services (domain)	Identity, credential and access management services including identity providers, directories, authentication and authorisation enforcement capabilities and credential stores.
independent OT authentication	Authentication services operated independently within the OT environment to reduce reliance on non-OT and external systems.
indicators of Good Practice	A set of statements used to inform expert judgement about whether an action should be rated not effective, partially effective or effective.
integrations and connectors	Interfaces and components that enable data exchange or functionality between cloud services and external systems, including APIs, third-party applications, plug-ins and automated workflows.
internet-facing (technology)	A system, service or component that is reachable from the public internet, either directly or through controlled ingress mechanisms, interfaces or integrations.
legacy (technology)	Any technology that is no longer supported by the manufacturer, developer or vendor
MITRE ATT&CK	A public knowledge base of adversary tactics and techniques based on observed real-world behaviour, maintained by the not-for-profit organisation MITRE

lateral movement	The activity by which an adversary moves from a point of compromise to other systems within an environment.
offline licensing	A licensing approach that allows systems to operate offline or in air-gapped environments, or to continue operating when disconnected from external networks or vendor services.
operational technology (OT)	Operational technology (OT) includes a broad set of technologies that covers process automation, instrumentation, cyber-physical operations, and industrial control systems (ICS).
OT self-reliance	The capability to operate critical services using localised, independent facility capabilities solely within the OT environment.
platform-as-a-service (PaaS)	A cloud service model in which the provider operates the underlying infrastructure, platform and runtime capabilities, while the customer deploys and manages applications, data and service configurations.
principle-focus approach	A method of implementing the framework in which the organisation selects a cyber security principle and applies it across multiple domains.
privileged environments (domain)	Systems and services that support privileged activities, management services, control planes and high-impact administrative functions.
provider-inherited responsibility	A cyber security responsibility implemented and operated by the cloud service provider that the customer verifies through assurance.
provider-supplied capability	A security capability supplied by the cloud service provider that the customer must enable, configure and operate.
priority phases	A sequencing tier that groups domains to assist in prioritisation
non-person identity	A digital identity used by an application, workload, service, device or automated process rather than an individual.
residual risk (cyber)	The cyber security risk that remains after controls have been applied.
risk appetite	The level of cyber security risk an organisation is willing to accept in pursuit of its objectives.
risk assessment (cyber)	The process of identifying cyber security risks, analysing their likelihood and consequence, and evaluating them against the organisation's risk appetite.

risk management (cyber)	The coordinated set of activities through which an organisation identifies, assesses, treats and monitors cyber security risks.
risk profile	A combined picture of cyber security risks an organisation is exposed to at a given point in time.
sessions and tokens	Mechanisms used to maintain authenticated access to cloud services after a user, application or non-person identity has successfully authenticated.
shared responsibility model	A model that defines how cyber security responsibilities are allocated between a cloud service provider and its customer.
software-as-a-service (SaaS)	A cloud service model in which the provider operates the application, platform and underlying infrastructure, while the customer manages its users, data, access, integrations and service configurations.
Domain-focus approach	A method of implementing the framework in which the organisation selects a single domain and applies all applicable principles before moving to the next.
techniques (MITRE ATT&CK)	A representation of how an adversary achieves a tactical goal by performing an action
technology-agnostic	A description of what must be done without mandating a specific vendor, product or architecture
tenant	A logically separated instance or administrative boundary of a cloud service that contains an organisation's users, data, configurations and integrations.
threat Intelligence (cyber)	Information about cyber threats, threat actors and adversary techniques that have been collected, analysed and contextualised to support decision making.
threat modelling	A structured activity to identify the threats relevant to a system, function, or organisation.
user devices (domain)	Endpoints used by personnel to access organisational systems, cloud services and data, including desktops and laptops.
visibility and response (domain)	The procedures and capabilities to detect, analyse and respond to cyber security events and incidents.
vital OT	Vital OT are the subset of critical systems that are unacceptable to have offline for an extended period, from the perspective of the safe provision of a minimum viable product.

**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>

