



Australian Government
Australian Signals Directorate

cyber.gov.au

ASD Essentials for enterprise IT



Essentials

Table of contents

Introduction	3
What is enterprise IT	3
ASD Essentials framework structure	3
More about the Essentials	4
Enterprise IT chapter elements	5
Domains	5
Priority phases	6
Priority phase 1: Boundary services and Identity services	6
Priority phase 2: Critical processes and services and Privileged environments	6
Priority phase 3: Business systems and User devices	7
ASD Essentials for enterprise IT matrix	8
Matrix structure and use	8
Capability domains	9
Governance and culture	9
Visibility and response	10
Technical 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 enterprise IT environments from sophisticated cyber threats.

What is enterprise IT

Enterprise IT refers to the IT environments operated by organisations whose scale, complexity, regulatory exposure or reliance on technology requires a structured and deliberate approach to the management of cyber security.

Enterprise IT environments typically include:

- multiple interconnected systems supporting different business functions
- identity and access arrangements that span a workforce and an extended user population
- dedicated cyber security and IT functions with defined roles
- formal governance over technology investment, risk and compliance.

ASD Essentials framework structure

Every ASD Essentials 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.

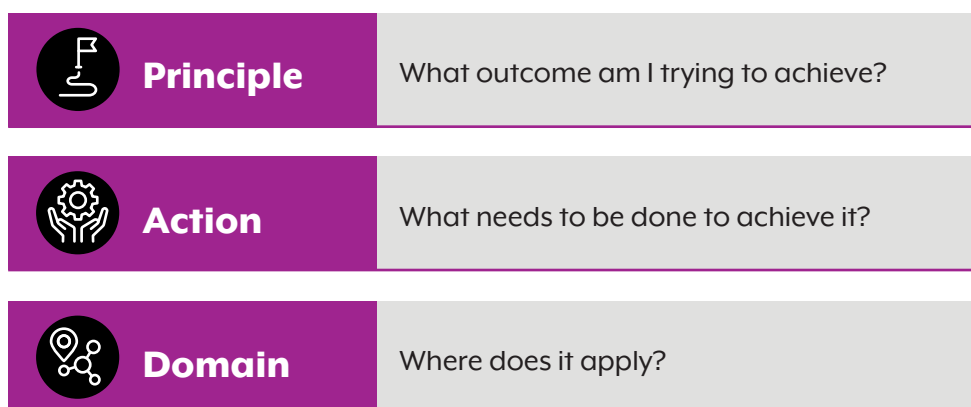


Figure 1. How the ASD Essentials framework layers work

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

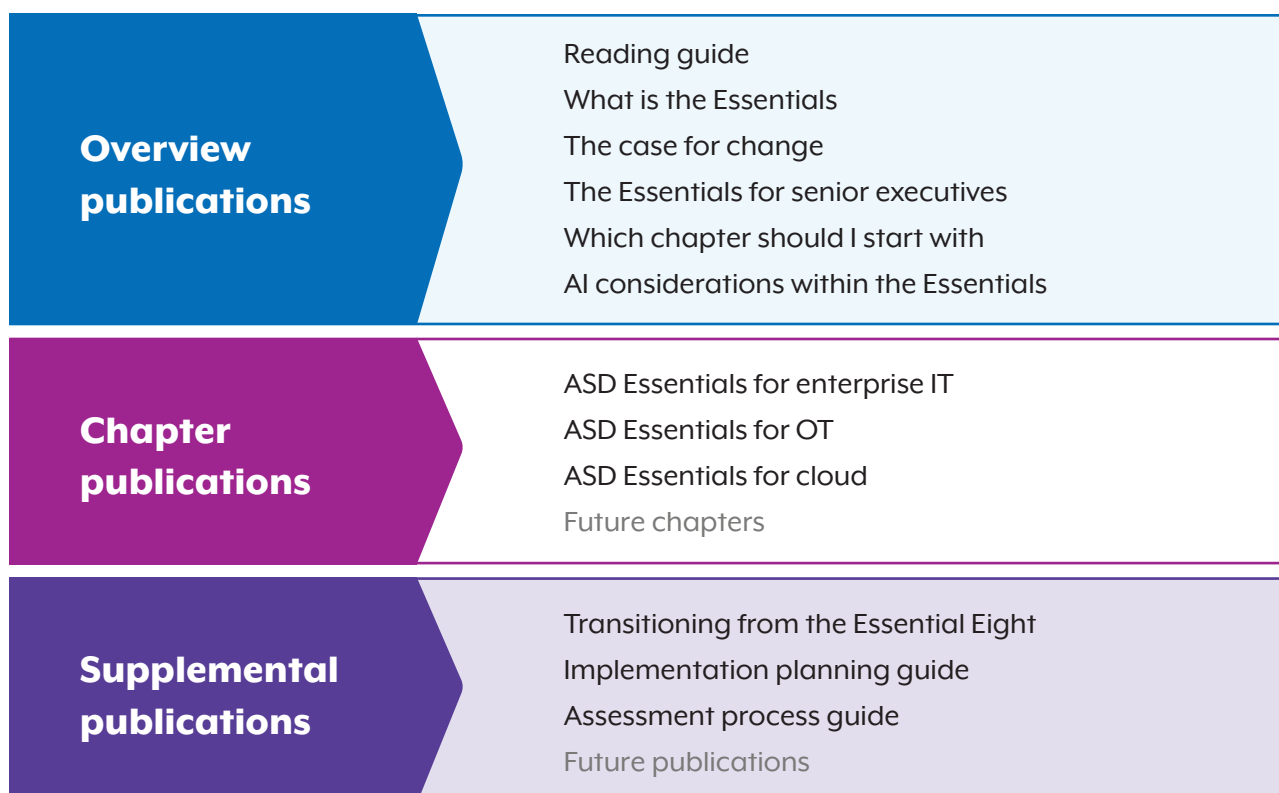


Figure 2. The Essentials series

Small and medium sized businesses that do not operate at the scale of enterprise IT can still use this guidance where relevant. For example, 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.

Enterprise IT 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	Assets at network boundaries that broker connectivity between environments of different trust levels, including internet-facing services and edge devices.	Internet-facing and boundary systems are routinely exposed to adversary scanning and exploitation making them common targets for initial access.
Identity services	Enterprise-wide identity, credential and access management services such as directories, authentication and authorisation services or credential stores.	Compromise of enterprise-wide identity services can enable an adversary to gain persistent or privileged access across the enterprise.

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.	Compromise of privileged systems can give an adversary extensive control over systems, services and security controls.
Business systems	Supporting enterprise functions that collectively enable organisational operations.	Compromise can disrupt day-to-day operations and provide pathways to more sensitive or critical systems.
User devices	Endpoints issued to the workforce, including desktops and laptops.	Widespread use and exposure make user devices common entry points for adversaries seeking access to the environment.

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 and reducing their overall cyber security risk.

The technical domains are grouped into the following priority phases.

Priority phase 1: Boundary services and Identity services

Boundary services and Identity services are prioritised because they are common pathways for adversaries seeking initial access to an organisation's environment. Weaknesses in these domains can enable unauthorised access and undermine security controls elsewhere in the environment. Addressing them together strengthens the protection of external access pathways and the identities used to access systems and services.

Priority phase 2: Critical processes and services and Privileged environments

Privileged environments can provide adversaries with elevated access following an intrusion. Critical processes and services are prioritised because their compromise or disruption could have significant consequences for an organisation. Addressing these domains together reduces the likelihood that an adversary can escalate access and affect systems and services that are critical to organisational outcomes.

Priority phase 3: Business systems and User devices

Business systems and User devices are widely distributed across enterprise IT environments and are common targets for adversaries. They are addressed after the earlier phases so organisations can build on the protections established for boundary, identity, privileged and critical environments. This sequencing helps reduce the likelihood that compromise of a business system or user device can spread across the organisation's environment.

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.

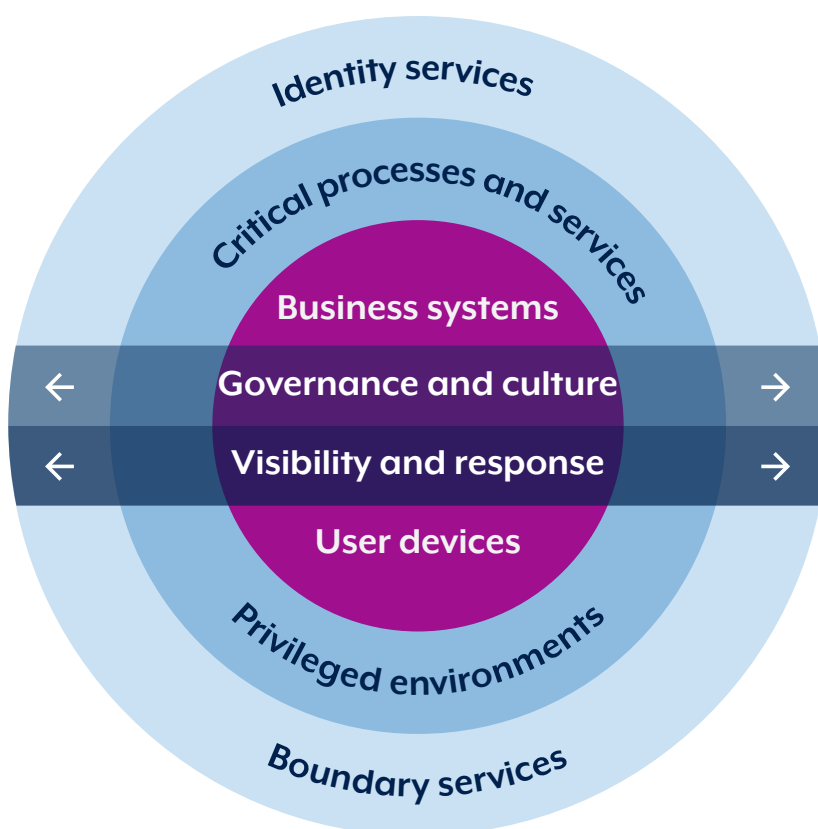


Figure 3. ASD Essentials for enterprise IT priority phases

ASD Essentials for enterprise IT 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 ASD 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.

Capability domains

Governance and culture

Matrix 1: Governance and culture capability domain

Principle	Action
GOV-01 - Executive cyber security accountability	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	Establish and maintain executive accountability for the use, governance and risk management of artificial intelligence within the organisation.
GOV-04 - Cyber security resourcing	Assign sufficient cyber security personnel and resources with the required skills to operate, monitor, maintain and manage the lifecycle of security controls and define cyber security responsibilities within role descriptions.
	Periodically review cyber security resourcing against cyber threat trends, cyber security incident outcomes and organisational changes.
GOV-03 - Security risk management assurance	Establish and maintain a risk management methodology and plan that is used to assess and treat cyber security risks.
GOV-11 - Supplier cyber security assurance	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.
	Maintain current assurance that suppliers continue to meet their cyber security commitments, and act when that assurance lapses or the supplier's risk changes.
GOV-14 - Legacy system management	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	Update and provide cyber security awareness training on a regular basis to reflect current threats and operational considerations.

Visibility and response

Matrix 2: Visibility and response capability domain

Principle	Action
IDE-01 - Asset identification	Use an approved asset inventory mechanism that supports automated discovery to detect new and changed physical and non-physical assets.
IDE-04 - Security risk identification	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	Identify unsecured keys, secrets and credentials by regularly scanning codebases, configuration files, file shares and user collaboration platforms.
DET-01 - Centralised event logging	Establish a centralised event log storage capability that protects logs from unauthorised access or modification.
DET-02 - Cyber security event detection	Ensure detection logic identifies unauthorised changes, anomalous authentication activity and suspicious software execution.
DET-03 - Cyber security incident identification	Triage alerts and events in a timely manner to determine whether cyber security incident thresholds have been met.
	Use indicators from across identities, applications, data and infrastructure activity rather than isolated signals when identifying cyber security incidents.
DET-05 - Detection capability efficacy	Review detection coverage periodically to identify gaps arising from new assets, services or architectural changes.
RES-05 - Cyber security incident coordination	Integrate external coordination obligations into cyber security incident response activities where required.
RES-03 - Cyber security incident response	Use documented, tested and approved cyber security incident response procedures when responding to cyber security incidents.
RES-04 - Cyber security incident insights	Perform post-cyber security incident reviews to identify the security gaps that enabled each stage of the cyber security incident.
	Evaluate the monitoring coverage and cyber security incident response procedures following cyber security incidents.

Technical domains

Matrix 3: Technical domains

Principle	Action	MITRE ATT&CK	Boundary services	Identity services	Critical processes and services	Privileged environments	Business systems	User devices
IDE-01 - Asset identification	Maintain current records of assets including infrastructure, operating systems, applications, identities, credentials and data.		✓	✓	✓	✓	✓	✓
PRO-01 - Secure system lifecycle	Design systems securely to provide visibility, enforce authorised access, protect data, minimise required and default privileges, limit exposed services and remove unnecessary functionality.	Exploit Public-Facing Application Valid Accounts Remote Services Exploitation for Privilege Escalation	✓	✓	✓	✓	✓	✓
	Secure build and deployment processes to enforce controls consistently across systems.		✓	✓	✓	✓	✓	✓
PRO-16 - Cyber supply chain security	Assess the integrity and authenticity of software, components and updates before use, and verify provenance where suitable supplier evidence is available.	Supply Chain Compromise Server Software Component	✓	✓	✓	✓	✓	✓
	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.	Supply Chain Compromise Server Software Component	✓	✓	✓	✓		

Principle	Action	MITRE ATT&CK	Boundary services	Identity 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 regularly, permitting exceptions only where the account is documented, justified, hardened and monitored.	Valid Accounts Brute Force	✓	✓	✓	✓	✓	✓
	Store authentication keys, secrets and tokens in approved secure repositories with access controls, including MFA.	Unsecured Credentials Credentials from Password Stores	✓	✓	✓	✓	✓	
	Use phishing-resistant MFA for users authenticating to systems, including from untrusted, external or high-risk locations.	Valid Accounts Account Manipulation Brute Force Remote Services Multi-Factor Authentication Request Generation Adversary-in-the-Middle	✓	✓	✓	✓	✓	✓
	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.	Brute Force Valid Accounts Adversary-in-the-Middle	✓	✓	✓	✓	✓	✓
	Ensure that user, machine, system and service account credentials are unique per system or account, particularly in high-privilege contexts.	Brute Force Valid Accounts	✓	✓	✓	✓	✓	✓

Principle	Action	MITRE ATT&CK	Boundary services	Identity services	Critical processes and services	Privileged environments	Business systems	User devices
PRO-12 - Least privilege access	Periodically review and update access privileges in alignment with current roles, duties and business requirements.	Account Manipulation	✓	✓	✓	✓	✓	✓
	Grant only authorised administrative roles permissions to create, modify or delete accounts and roles, and access privileged functions or applications.	Create Account Account Manipulation	✓	✓	✓	✓		
	Provision user, administrative and non-person accounts with only the minimum access and privileges required to perform defined operational functions.	Create Account Account Manipulation	✓	✓	✓	✓		
PRO-05 - Secure administration	Ensure administrative activities can only be performed from dedicated and hardened environments that are isolated from unprivileged user workloads.	Exploitation for Privilege Escalation OS Credential Dumping	✓	✓	✓	✓		
	Enforce explicit session establishment controls before privileged actions are permitted, including the use of time-bound privilege grants.	OS Credential Dumping Use Alternate Authentication Material Steal or Forge Kerberos Tickets	✓	✓	✓	✓		
	Record all administrative or management actions that modify systems, configurations or controls including the details of the user, timestamp and target.	Impair Defenses Modify Registry Create Account Account Manipulation Create or Modify System Process	✓	✓	✓	✓		

Principle	Action	MITRE ATT&CK	Boundary services	Identity services	Critical processes and services	Privileged environments	Business systems	User devices
PRO-04 - Secure configuration management	Define approved configuration baselines, informed by vendor and industry hardening guidance, that disable or remove unnecessary services, insecure settings, and unsupported or weak communication protocols.	Server Software Component Windows Management Instrumentation Network Service Discovery OS Credential Dumping	✓	✓	✓	✓	✓	✓
	Deploy approved configuration baselines on systems, including infrastructure, operating systems and applications.	Exploit Public-Facing Application External Remote Services User Execution Command and Scripting Interpreter	✓	✓	✓	✓	✓	✓
	Detect and respond to configuration drift using scheduled technical assessments and, where supported, automated monitoring, based on system criticality and change rate.	Impair Defenses Modify Registry	✓	✓	✓	✓	✓	✓
PRO-06 - Vulnerability management	Identify known software and configuration weaknesses of assets through continuous and repeatable assessment activities, including vulnerability scanning activities.	Exploit Public-Facing Application Exploitation for Privilege Escalation Exploitation of Remote Services Exploitation for Client Execution	✓	✓	✓	✓	✓	✓

Principle	Action	MITRE ATT&CK	Boundary services	Identity services	Critical processes and services	Privileged environments	Business systems	User devices
	Apply security patches or updates within defined riskbased timeframes or automatically where operational impact is low.	Exploit Public-Facing Application Exploitation for Privilege Escalation Exploitation of Remote Services Exploitation for Client Execution	✓	✓	✓	✓	✓	✓
	Remediate or mitigate vulnerabilities exceeding defined risk thresholds within defined timeframes based on exploitation, exposure, criticality, impact and compensating controls, and verify treatment effectiveness.	Exploit Public-Facing Application Exploitation for Privilege Escalation Exploitation of Remote Services Exploitation for Client Execution	✓	✓	✓	✓	✓	✓
PRO-07 - Trustworthy software	Permit only supported, verified and organisation- authorised software to execute on systems, with exceptions minimised, formally risk accepted, time-bound, monitored and regularly reviewed.	Impair Defenses User Execution Command and Scripting Interpreter Windows Management Instrumentation Process Injection System Binary Proxy Execution	✓	✓	✓	✓	✓	✓

Principle	Action	MITRE ATT&CK	Boundary services	Identity services	Critical processes and services	Privileged environments	Business systems	User devices
	Restrict administrative and management tooling to approved software sets and executed from only authorised, known locations.	Impair Defenses User Execution Command and Scripting Interpreter Windows Management Instrumentation Masquerading Process Injection System Binary Proxy Execution	✓	✓	✓	✓	✓	✓
PRO-10 - Regular and proven backups	Back up important data, applications and settings on a defined schedule to secure, resilient storage protected by encryption and immutable, offline, logically isolated or equivalent controls.	Data Encrypted for Impact Inhibit System Recovery	✓	✓	✓	✓	✓	
	Isolate backup repositories from general user environments and production workloads, ensuring they are separated from primary systems to prevent unauthorised access, modification or deletion.	Data Encrypted for Impact Data from Local System Inhibit System Recovery	✓	✓	✓	✓	✓	
	Conduct regular testing of backup and restoration procedures to ensure that backups are reliable and capable of meeting defined recovery time objectives and recovery point objectives.	Data Encrypted for Impact Inhibit System Recovery	✓	✓	✓	✓	✓	

Principle	Action	MITRE ATT&CK	Boundary services	Identity services	Critical processes and services	Privileged environments	Business systems	User devices
PRO-18 - Network segmentation and segregation	Isolate systems within network zones based on business criticality and trust level, and restrict and monitor inbound and outbound access to explicitly approved pathways and services.	Exploit Public-Facing Application External Remote Services	✓	✓	✓	✓	✓	
	Limit lateral movement between, and within, network segments to explicitly approved pathways and services, based on business requirements and trust levels.	Remote Services Lateral Tool Transfer	✓	✓	✓	✓	✓	
PRO-09 - Content filtering	Inspect outbound content flows to detect unauthorised transfer of sensitive or high-value data.	Exfiltration Over C2 Channel Exfiltration Over Alternative Protocol Proxy	✓	✓	✓	✓	✓	
	Block outbound network connections to known malicious or untrusted destinations.	Phishing User Execution 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.	Phishing Remote Services Ingress Tool Transfer	✓		✓			

Principle	Action	MITRE ATT&CK	Boundary services	Identity services	Critical processes and services	Privileged environments	Business systems	User devices
PRO-14 - Cyber security awareness training	Ensure all personnel receive cyber security awareness training, that is tailored to how they will interact with systems, applications and data in their assigned roles, before being granted access to organisational systems and data.	Phishing Valid Accounts	✓	✓	✓	✓		
DET-01 - Centralised event logging	Protect event logs from unauthorised access, modification or deletion, including by encrypting them during transit and at rest and securing the systems and accounts used to store, manage and analyse them.	Indicator Removal Impair Defenses	✓	✓	✓	✓	✓	✓
	Forward high-value, security-relevant event logs and configuration changes from infrastructure, operating systems and applications to a central log storage capability.	Indicator Removal Impair Defenses	✓	✓	✓	✓	✓	✓
DET-04 - Baseline high-risk access activities	Continuously monitor and analyse software execution behaviour on systems to detect where legitimate tools and utilities are being used for malicious purposes.	Valid Accounts System Binary Proxy Execution Command and Scripting Interpreter	✓	✓	✓	✓		
DET-02 - Cyber security event detection	Ensure event logs are normalised, time-synchronised and enriched to support correlation across systems and environments.		✓	✓	✓	✓	✓	✓

**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>

