



Australian Government  
Australian Signals Directorate

**cyber**.gov.au

# ASD Essentials for OT



**E**ssentials

# Table of contents

- Introduction** ..... 3
  - What is operational technology ..... 3
  - ASD Essentials framework structure ..... 3
  - More about the Essentials ..... 4
- OT chapter elements** ..... 5
  - Domains ..... 5
  - Priority phases ..... 7
- ASD Essentials for OT matrix** ..... 9
  - Matrix structure and use ..... 9
  - Capability domains ..... 9
  - Visibility and response ..... 11
  - Technical domains ..... 12

# 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 Essentials series chapter is designed to help these organisations protect operational technology (OT) environments from cyber threats.

## What is operational technology

OT systems are those that detect or cause a direct change to the physical environment through the monitoring or control of devices, processes and events. OT includes the simple automation systems found in everyday environments as well as large and complex systems controlling critical infrastructure (CI). While the principles addressed in this chapter are applicable to all OT, the target audience of this chapter of the Essentials series includes operators of OT responsible for complex systems control, automation and safety across critical service sectors.

Critical service sectors include public transit systems, critical supply chain logistics, power generation, transmission and distribution, water and wastewater, medical services provision and large-scale industry. Securing and maintaining OT is crucial for minimising disruption to critical services.

The term **vital OT** is used in this document to reference the subset of critical systems that it is unacceptable to have offline for an extended period, from the perspective of the safe provision of a minimum viable product. This definition takes into consideration the ability to maintain critical operation through manual processes and implementation of Business Continuity Plans (BCP).

## 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 in Figure 1.

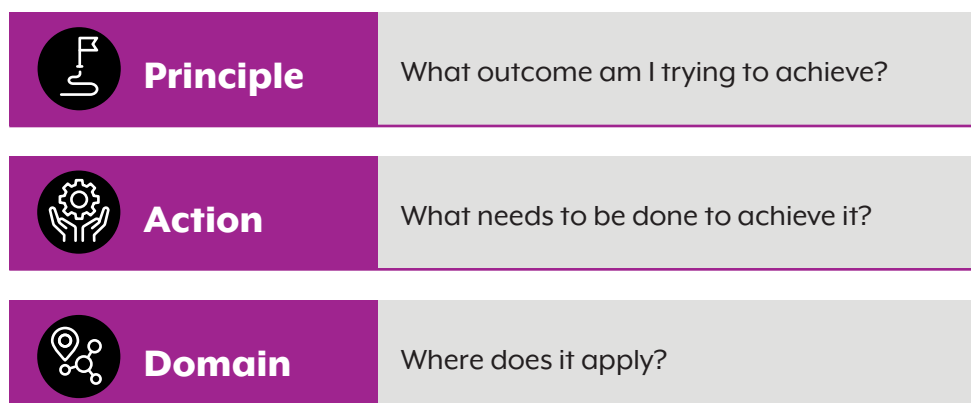


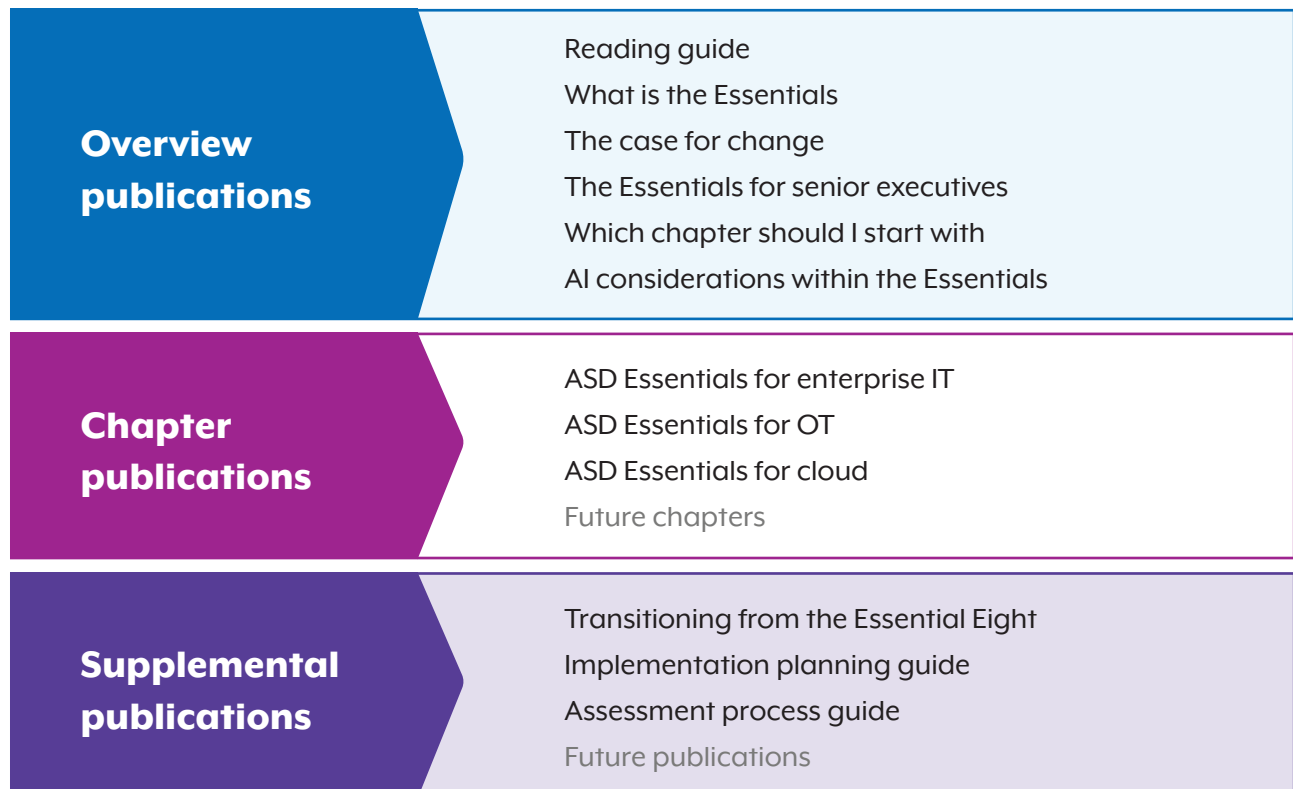
Figure 1. How the ASD Essentials framework layers work

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 the scale of critical infrastructure can still use this chapter 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](https://cyber.gov.au)

# OT 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.

The description of the User devices domain in the Essentials for OT chapter is written to highlight that the risk associated with introducing endpoint-type devices to any OT environment is extremely high. Subsequently, all devices within the OT system must be considered as privileged and treated accordingly. The User devices domain is therefore not considered within the technical domains mapping later in the chapter.

The Essentials for OT chapter is to be read with application of the definitions in the [ASD Essentials glossary](#).

**Table 1 - Domains and risk context**

| Domain                                 | Description                                                                                                                                                                         | Risk Context                                                                                                                                                        |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Governance and culture</b>          | 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.                                                  |
| <b>Visibility and response</b>         | Procedures and capabilities for detecting, analysing and responding to cyber security events and incidents. In OT, visibility often has a second use in engineering fault analysis. | Limited visibility and response can delay the detection, analysis and containment of intrusions. In OT, this could lead to potentially catastrophic system failure. |
| <b>Critical processes and services</b> | Core systems and networks which are essential to safely deliver the product or service for which an organisation exists.                                                            | Compromise or loss of these systems can disrupt the organisation's ability to deliver critical outcomes or services.                                                |

| Domain                         | Description                                                                                                                                                                                                                                      | Risk Context                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Boundary services</b>       | Assets at network boundaries that broker connectivity between environments of different trust levels, including internet-facing services, edge devices and points of connection to other OT systems.                                             | Internet-facing and boundary services may be routinely exposed to adversary scanning and exploitation making them common targets for initial access.                                                                                                                                                                                                                                                                                         |
| <b>Identity services</b>       | Identity, credential and access management services such as directories, authentication and authorisation services or credential stores.                                                                                                         | Compromise of identity services can enable an adversary to gain persistent or privileged access across the enterprise.                                                                                                                                                                                                                                                                                                                       |
| <b>Privileged environments</b> | Systems, services and devices that support privileged activities, management services and high-impact administrative functions. Within OT, this includes items which, in an enterprise IT context, would be considered user or endpoint devices. | Compromise of privileged systems can give an adversary extensive control over systems, services and security controls. Within OT, any device with connectivity within a privileged environment must be considered a privileged device.                                                                                                                                                                                                       |
| <b>Business systems</b>        | Supporting enterprise functions that collectively enable organisational operations.                                                                                                                                                              | Compromise can disrupt day-to-day operations and provide pathways to more sensitive or critical systems. Business systems may exist within the IT systems of an organisation, with their OT process support possibly making them considered part of the OT systems.                                                                                                                                                                          |
| <b>User devices</b>            | Endpoints issued to the workforce, including desktops and laptops.                                                                                                                                                                               | The critical nature of OT systems, coupled with the high-risk cyber security possibilities present in many environments, should prohibit the use of typically configured end-user or endpoint devices within OT environments. Use of such devices risks the unintended introduction of cyber threats directly into the privileged OT environment. All devices within the OT system must be considered as privileged and treated accordingly. |

## 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 technical **domains** are sequenced differently in this chapter to reflect the operational safety requirements of OT environments. OT cyber security prioritises the safe and continuous operation of physical processes. This can require greater emphasis on protecting critical processes, controlling connectivity and administrative access, and using compensating controls where changes such as patching or replacing legacy equipment cannot be made without affecting operations.

The technical domains are grouped into the following priority phases:

### Priority phase 1: Boundary services and Critical processes and services

Boundary services are prioritised because they provide pathways between OT systems and external or less trusted environments. Critical processes and services are prioritised because their compromise or disruption could have significant safety, operational, environmental or service-delivery consequences. Addressing these domains together strengthens the protection of pathways into the OT environment while protecting the systems and processes with the greatest potential consequence.

### Priority phase 2: Privileged environments and Identity services

Privileged environments and Identity services control administrative and privileged access to OT systems. Weaknesses in these domains can allow an adversary to gain elevated access, move through the environment or make unauthorised changes to critical systems and processes. Addressing these domains together reduces the likelihood that an initial compromise can escalate.

### Priority phase 3: Business systems

Business systems are addressed after the domains that protect critical operations, connectivity and privileged access. This sequencing reduces the likelihood that compromise of a business system can provide a pathway to critical OT systems while strengthening the protection of business functions that support OT operations.

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.

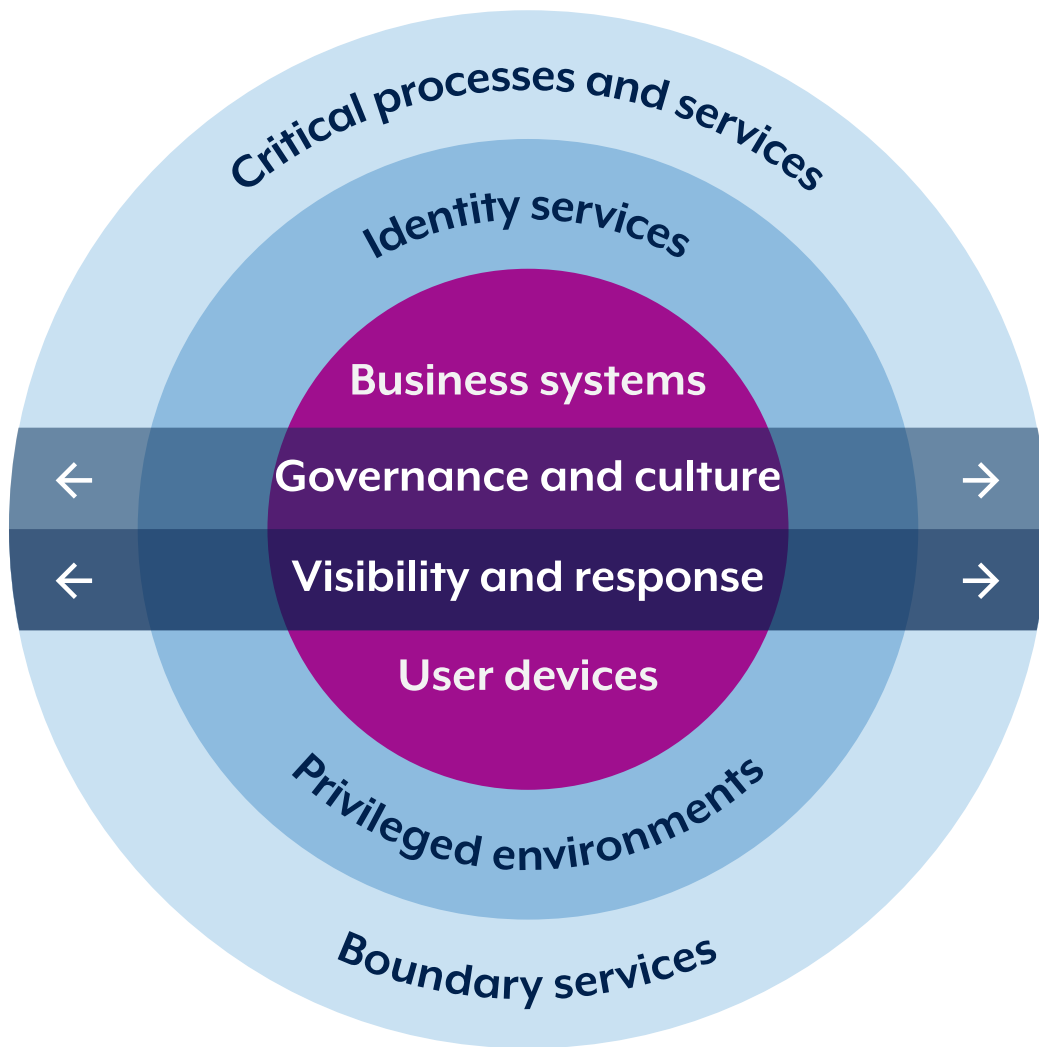


Figure 3. Essentials priority phases

# ASD Essentials for OT 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 five included 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 OT 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 controls across OT, and define cyber security responsibilities within role descriptions. |

| Principle                                               | Action                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GOV-10 - System exposure minimisation</b>            | Protect OT system information, and the systems outside the OT environment that are critical to OT functionality, as high-value assets, and prevent public disclosure of OT device installation details, requiring third parties to do the same.                                                                  |
| <b>GOV-11 - Supplier cyber security assurance</b>       | Establish and maintain a process to assess and manage supply chain risk for hardware, software and third party service providers, and to confirm that providers of services essential to OT understand the criticality of vital OT and can meet agreed levels of prioritised support.                            |
|                                                         | Establish and maintain a process to only use software, hardware and services from trustworthy suppliers that have demonstrated a commitment to the security of, and transparency for, their products and services                                                                                                |
| <b>GOV-14 - Legacy system management</b>                | Establish and maintain a process for identifying, assessing and managing the cyber security risk associated with legacy and unsupported systems that remain operationally critical, until they can be removed or replaced.                                                                                       |
| <b>GOV-07 - Continuous cyber security improvement</b>   | Conduct regular exercises of isolation and sustained isolated operation, covering isolation decision-making, threat hunting before reconnection, safe removal of isolation, sustained operation for the defined isolation period, artefact capture, and staff movement in a degraded communications environment. |
| <b>PRO-20 - Remote access to operational technology</b> | Notify local operators of authorised remote maintenance or supplier activity, so that unexpected changes are not normalised or ignored.                                                                                                                                                                          |
| <b>PRO-14 - Cyber security awareness training</b>       | Ensure all personnel receive cyber security awareness training that is tailored to how they will interact with OT systems in their assigned roles, and update it on a regular basis to reflect current threats and operational considerations.                                                                   |

## Visibility and response

Matrix 2 - Visibility and response capability domain

| Principle                                                  | Action                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IDE-01 - Asset identification</b>                       | Use an approved asset inventory mechanism that supports automated discovery to detect new and changed assets, recording physical and logical location, role, criticality, dependencies, known vulnerabilities and existing compensating controls.                                                                       |
| <b>IDE-02 - Business criticality rating identification</b> | Identify and document vital OT, and the enabling systems and services on which vital OT depends, including those located outside the OT environment.                                                                                                                                                                    |
| <b>IDE-04 - Security risk identification</b>               | Identify and analyse the OT attack surface, security boundaries and connectivity, including the points through which complete isolation can be enacted, and review these inputs on a continuous basis.                                                                                                                  |
| <b>RES-01 - Cyber security incident planning</b>           | Update business and operational continuity plans to reflect the impact that isolation will have on business and operational processes.                                                                                                                                                                                  |
|                                                            | Use documented, tested and approved OT incident response procedures when responding to cyber security incidents, covering situations such as safety events, setting out who participates in response and recovery, including third parties, loss of visibility, and workstation compromise.                             |
|                                                            | Establish and maintain a document management capability for system documentation, and retain per-site copies of playbooks, drawings, installation, reset and configuration instructions, break-glass secrets and keys, and emergency contact information in a form that does not depend on the systems being recovered. |
| <b>RES-05 - Cyber security incident coordination</b>       | Maintain alternative communications for site-to-site and site-to-staff use during degradation or loss of normal communications, and establish processes to have the right staff at the right site when isolation is enacted.                                                                                            |
|                                                            | Build into response plans the capability to collect forensic artefacts for later offline analysis within pre-approved areas.                                                                                                                                                                                            |
| <b>RES-03 - Cyber security incident response</b>           | Establish, maintain and exercise a plan to rapidly disconnect remote access when malicious activity is identified.                                                                                                                                                                                                      |
| <b>RES-02 - Cyber security incident reporting</b>          | Establish and maintain an effective process, independent of systems outside the OT environment, for personnel to raise an OT cyber security concern.                                                                                                                                                                    |
| <b>REC-02 - System recovery assurance</b>                  | Maintain the capability to recover, without supplier support, any system that cannot acceptably remain offline, at least to a minimum viable level of service, including a plan to replace key OT devices following destructive attacks.                                                                                |

## Technical domains

Matrix 3 – Technical domains

| Principle                                      | Action                                                                                                                                                                                                                           | MITRE ATT&CK                                     | Critical processes and services | Boundary services | Identity services | Privileged environments | Business systems |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|---------------------------------|-------------------|-------------------|-------------------------|------------------|
| IDE-01 - Asset identification                  | Continuously identify and document infrastructure, operating systems, applications, identities, credentials and data as distinct assets.                                                                                         |                                                  | ✓                               | ✓                 | ✓                 | ✓                       | ✓                |
| IDE-05 - Asset interdependencies               | Identify and document safety components for physical and electrical systems, including the connectivity and dependency relationships between safety systems.                                                                     |                                                  | ✓                               |                   |                   |                         |                  |
| IDE-06 - Resilience requirement identification | Identify and document the communication and alerting infrastructure that carries safety functions to external alarm systems, and assure the reliability of those paths where communication services are degraded or unavailable. | <a href="#">Loss of safety</a>                   | ✓                               | ✓                 |                   |                         |                  |
| PRO-01 - Secure system lifecycle               | Design, size and configure new network devices so that network traffic capture can be enabled without a subsequent configuration change.                                                                                         |                                                  | ✓                               | ✓                 | ✓                 | ✓                       |                  |
|                                                | Sanitise and securely dispose of hardware, including devices returned to a supplier for maintenance, using trusted onsite or domestic disposal services.                                                                         | <a href="#">Theft of operational information</a> | ✓                               | ✓                 | ✓                 | ✓                       | ✓                |

| Principle                                                  | Action                                                                                                                                                                                                                                                        | MITRE ATT&CK                                                          | Critical processes and services | Boundary services | Identity services | Privileged environments | Business systems |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|---------------------------------|-------------------|-------------------|-------------------------|------------------|
| <b>PRO-16 - Cyber supply chain security</b>                | Identify, test and resolve third-party dependencies that would fail under isolation, including licensing, activation, updates, supplier support, and licences coupled to physical hardware identifiers.                                                       | <a href="#">Loss of availability</a>                                  | ✓                               | ✓                 | ✓                 | ✓                       |                  |
|                                                            | Verify the integrity and provenance of assets, software, components and updates before they are introduced into the OT environment, and record the origin and handling history of new, repaired and serviced assets.                                          | <a href="#">Supply chain compromise</a>                               | ✓                               | ✓                 | ✓                 | ✓                       | ✓                |
| <b>PRO-13 - Identity, credential and access management</b> | Confirm the functionality of break-glass accounts, and the availability of their secrets, for administrative access during isolation from other authentication mechanisms.                                                                                    |                                                                       |                                 |                   | ✓                 |                         |                  |
|                                                            | Use phishing-resistant MFA for users authenticating across a perimeter into OT, and from any network not under the organisation's sole OT administrative control.                                                                                             | <a href="#">Valid accounts</a><br><a href="#">Remote services</a>     |                                 | ✓                 | ✓                 |                         |                  |
|                                                            | Ensure that credentials are unique per device or account, changing default, supplier and simple passwords before a device is commissioned or replaced, and where unique credentials are not supported, apply a compensating control that protects the device. | <a href="#">Default credentials</a><br><a href="#">Valid accounts</a> | ✓                               | ✓                 | ✓                 | ✓                       | ✓                |

| Principle                                | Action                                                                                                                                                                                                                                                                  | MITRE ATT&CK                                                                                               | Critical processes and services | Boundary services | Identity services | Privileged environments | Business systems |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-------------------|-------------------------|------------------|
| PRO-12 - Least privilege access          | Establish and maintain a process to grant, track and periodically review approval of all remote access users, using secure protocols and restricting access to the minimum level required for the work being performed.                                                 | <a href="#">Remote services</a>                                                                            |                                 | ✓                 | ✓                 |                         |                  |
|                                          | Provision administrative and privileged functions in OT as distinct roles, each assigned to a unique account with only the minimum access and privileges required to perform defined operational functions.                                                             | <a href="#">Valid accounts</a>                                                                             |                                 |                   | ✓                 | ✓                       |                  |
| PRO-05 - Secure administration           | Manage supporting site infrastructure from a dedicated management network within the most critical network to which it is connected.                                                                                                                                    | <a href="#">Lateral tool transfer</a><br><a href="#">Remote services</a>                                   |                                 |                   | ✓                 | ✓                       |                  |
|                                          | Ensure administrative, engineering and troubleshooting access to OT can only be initiated from dedicated and hardened environments that are isolated from unprivileged workloads and located in a segment of equal or greater trust than the system being administered. | <a href="#">Lateral tool transfer</a><br><a href="#">Valid accounts</a><br><a href="#">Remote services</a> | ✓                               |                   |                   | ✓                       |                  |
| PRO-04 - Secure configuration management | Detect and respond to configuration changes within OT and its demilitarised zones, including changes to name resolution records, through automation or continuous technical assessment.                                                                                 | <a href="#">Modify parameter</a>                                                                           |                                 | ✓                 |                   |                         |                  |

| Principle                                | Action                                                                                                                                                                                                                                                                                                                                                                                                               | MITRE ATT&CK                                                                                                                                                                                                               | Critical processes and services | Boundary services | Identity services | Privileged environments | Business systems |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-------------------|-------------------------|------------------|
|                                          | Define and deploy approved configuration baselines that disable or remove unnecessary physical ports, communications ports, services, insecure settings and weak protocols where systems support it, prevent unauthorised changes to name resolution records, monitor for access attempts against exposed services, and bring critical OT elements that can be updated to the same baseline as their IT equivalents. | <a href="#">Default credentials</a><br><a href="#">Exploitation of remote services</a><br><a href="#">Adversary in the middle</a><br><a href="#">Remote system discovery</a><br><a href="#">Internet accessible device</a> | ✓                               | ✓                 |                   | ✓                       |                  |
|                                          | Harden new instances of control software, including modelling, forecasting and automated decision support systems that provide input to control, where feasible, and where doing so does not degrade the availability or safety of the OT system.                                                                                                                                                                    | <a href="#">Exploitation of remote services</a><br><a href="#">Modify program</a><br><a href="#">Manipulation of control</a>                                                                                               | ✓                               |                   |                   |                         |                  |
| <b>PRO-06 - Vulnerability management</b> | Apply security patches or updates within defined risk-based timeframes, record each asset that cannot or will not be patched along with the reason, and bring critical OT elements that can be updated to the same hardening baseline as equivalent critical elements in IT.                                                                                                                                         | <a href="#">Exploitation of remote services</a><br><a href="#">Exploit public-facing application</a><br><a href="#">Internet accessible device</a>                                                                         | ✓                               | ✓                 | ✓                 | ✓                       | ✓                |

| Principle                                  | Action                                                                                                                                                                                                                                                                                                           | MITRE ATT&CK                                                                                                                                       | Critical processes and services | Boundary services | Identity services | Privileged environments | Business systems |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-------------------|-------------------------|------------------|
|                                            | Apply compensating protections where assets cannot or will not be patched, or where they remain operationally critical but are no longer supported by security patch release.                                                                                                                                    | <a href="#">Exploitation of remote services</a><br><a href="#">Exploit public-facing application</a><br><a href="#">Internet accessible device</a> | ✓                               | ✓                 | ✓                 | ✓                       | ✓                |
|                                            | Establish and maintain a register of assets that cannot be patched, or that will not be patched, recording for each the reason, the compensating protections applied, the residual risk accepted and the authority accepting it, and review each entry at defined cadence whenever the asset's exposure changes. |                                                                                                                                                    | ✓                               | ✓                 | ✓                 | ✓                       | ✓                |
| <b>PRO-07 - Trustworthy software</b>       | Ensure only approved and integrity-verified software is permitted to execute on systems that support it, with exceptions minimised, risk-accepted, time-bound and regularly reviewed.                                                                                                                            | <a href="#">User execution</a><br><a href="#">Scripting</a><br><a href="#">Command line interface</a>                                              | ✓                               |                   |                   | ✓                       |                  |
| <b>PRO-10 - Regular and proven backups</b> | Conduct regular testing of rebuild, backup and restoration procedures to ensure that they are reliable and capable of meeting defined recovery time objectives and recovery point objectives, including rebuilding in the absence of backups.                                                                    | <a href="#">Data destruction</a><br><a href="#">Modify program</a>                                                                                 | ✓                               | ✓                 | ✓                 | ✓                       |                  |

| Principle                                     | Action                                                                                                                                                                                                                                                                                                          | MITRE ATT&CK                                                                                                                | Critical processes and services | Boundary services | Identity services | Privileged environments | Business systems |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-------------------|-------------------------|------------------|
|                                               | Backup the firmware, configuration, licence, calibration, project and logic files and supplier images required to rebuild OT, held per site and isolated from network access, on a defined schedule aligned to criticality and rate of change, and maintained to support restoration to a common point in time. | <a href="#">Data destruction</a><br><a href="#">Modify program</a>                                                          | ✓                               |                   |                   |                         |                  |
| PRO-18 - Network segmentation and segregation | Limit communication between OT assets and any other network to explicitly approved pathways and services, based on business requirements, location and trust levels, and design new OT systems so that each service can exist within its own network segment or enclave.                                        | <a href="#">Remote services</a><br><a href="#">Internet accessible device</a><br><a href="#">Lateral tool transfer</a>      | ✓                               | ✓                 |                   |                         | ✓                |
|                                               | Isolate OT sites and business function zones within protected network segments, with communication between them policy driven through a demilitarised zone rather than direct and unlimited.                                                                                                                    | <a href="#">Remote services</a><br><a href="#">Exploitation of remote services</a><br><a href="#">Lateral tool transfer</a> |                                 | ✓                 |                   |                         |                  |
|                                               | Segment safety systems from non-safety parts of the OT environment, enforced at a network boundary rather than by device configuration alone, and protect safety systems against change originating outside the site safety system boundary.                                                                    | <a href="#">Loss of safety</a>                                                                                              | ✓                               |                   |                   |                         |                  |
|                                               | Isolate non-production OT environments from production and from each other, where such environments exist.                                                                                                                                                                                                      | <a href="#">Lateral tool transfer</a><br><a href="#">Remote services</a>                                                    |                                 | ✓                 |                   |                         |                  |
|                                               |                                                                                                                                                                                                                                                                                                                 |                                                                                                                             |                                 |                   |                   |                         |                  |

| Principle                                 | Action                                                                                                                                                                                                                                                  | MITRE ATT&CK                                                                                                                              | Critical processes and services | Boundary services | Identity services | Privileged environments | Business systems |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-------------------|-------------------------|------------------|
| PRO-19 - Operational technology isolation | Establish and maintain demilitarised zones that isolate OT at its perimeters from all networks not under the organisation's sole administrative control.                                                                                                | <a href="#">External remote services</a><br><a href="#">Exploitation of remote services</a><br><a href="#">Internet accessible device</a> |                                 | ✓                 |                   |                         |                  |
|                                           | Document the procedures used to enact isolation, including clear physical identification of the cables and equipment involved.                                                                                                                          |                                                                                                                                           | ✓                               | ✓                 |                   |                         |                  |
|                                           | Ensure isolation points can only be managed from within vital OT, so that enacted isolation cannot be reversed externally.                                                                                                                              | <a href="#">External remote services</a><br><a href="#">Remote services</a><br><a href="#">Valid accounts</a>                             |                                 | ✓                 |                   |                         |                  |
|                                           | Maintain the capability to isolate vital OT and sustain safe operation for a defined period aligned to critical service continuity requirements, and verify the effectiveness of isolation mechanisms on enactment and throughout the isolation period. | <a href="#">Lateral tool transfer</a><br><a href="#">Remote services</a><br><a href="#">Connection proxy</a>                              | ✓                               | ✓                 |                   |                         |                  |
|                                           | Ensure the services on which vital OT depends operate independently of systems outside the OT environment, using separate software, credentials, storage, policy and servers, so that those services remain available throughout isolation.             | <a href="#">Loss of availability</a><br><a href="#">Loss of control</a><br><a href="#">Loss of view</a>                                   | ✓                               | ✓                 | ✓                 |                         | ✓                |

| Principle                                               | Action                                                                                                                                                                                                                   | MITRE ATT&CK                                                                                                                                                                 | Critical processes and services | Boundary services | Identity services | Privileged environments | Business systems |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-------------------|-------------------------|------------------|
| <b>PRO-20 - Remote access to operational technology</b> | Ensure remote access is not routed directly into OT, terminating all traffic in the OT demilitarised zone before the next hop.                                                                                           | <a href="#">External remote services</a><br><a href="#">Remote services</a><br><a href="#">Exploitation of remote services</a><br><a href="#">Internet accessible device</a> |                                 | ✓                 |                   |                         |                  |
|                                                         | Enforce explicit session establishment controls before remote access is permitted, including time-bound grants, no permanent connections, and disconnection after a defined period of inactivity.                        | <a href="#">External remote services</a><br><a href="#">Remote services</a><br><a href="#">Valid accounts</a>                                                                |                                 | ✓                 | ✓                 |                         |                  |
| <b>PRO-15 - Physical access control</b>                 | Maintain physical site access controls, and plan for a safe site environment for operators to work in, that continue to function in a degraded or isolated state.                                                        |                                                                                                                                                                              | ✓                               |                   |                   |                         |                  |
|                                                         | Implement physical security controls at devices and sites where physical access poses heightened cyber security risk, and disable unused physical ports and removable media interfaces where business continuity allows. | <a href="#">Replication through removable media</a><br><a href="#">Transient cyber asset</a>                                                                                 | ✓                               |                   |                   |                         |                  |

| Principle                                      | Action                                                                                                                                                                                                                                            | MITRE ATT&CK                                                                                                                    | Critical processes and services | Boundary services | Identity services | Privileged environments | Business systems |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-------------------|-------------------------|------------------|
| <b>DET-01 - Centralised event logging</b>      | Perform host-based logging on operator, engineering and server systems within the OT environment, and maintain log collection, query and investigation capability that remains available when systems outside the OT environment are unavailable. | <a href="#">Indicator removal on host</a>                                                                                       | ✓                               | ✓                 | ✓                 | ✓                       | ✓                |
| DET-04 - Baselined high-risk access activities | Record all remote access sessions with the details of the user, timestamp and target, and monitor them for deviations from validated patterns.                                                                                                    | <a href="#">Remote services</a><br><a href="#">External remote services</a>                                                     |                                 | ✓                 |                   |                         |                  |
| DET-02 - Cyber security event detection        | Capture and monitor network traffic continuously on both sides of all OT-connected demilitarised zone boundaries.                                                                                                                                 | <a href="#">Port scanning</a><br><a href="#">Remote services</a>                                                                |                                 | ✓                 |                   |                         |                  |
|                                                | Capture and monitor traffic at interfaces between segments within OT, using detection methods with a high signal-to-noise ratio, and alert on control protocols crossing segment boundaries where they are not expected.                          | <a href="#">Port scanning</a><br><a href="#">Standard application layer protocol</a><br><a href="#">Remote system discovery</a> |                                 | ✓                 |                   |                         |                  |

**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>

