



Australian Government
Australian Signals Directorate

cyber.gov.au

ASD Essentials overview

The Essentials for senior executives

Essentials

Contents

- Executive summary** 3
- ASD Essentials series framework** 4
- Purpose** 5
- Benefits of the ASD Essentials series** 6
 - Improved visibility of security posture 7
 - Transitioning Essential Eight investment 9
- Executive oversight of implementation** 9
 - What senior executives should expect 10
 - Questions senior executives should ask 11
- Conclusion** 12

Executive summary

Australian organisations continue to face cyber threats from increasingly capable malicious cyber actors. State-sponsored actors remain a serious threat, while cybercriminals and other malicious actors use a range of techniques to gain access, escalate privileges and disrupt operations. Cyber threats affect organisations across all sectors, regardless of size or profile. For decision-makers, cyber threats can have consequences beyond technology systems, operational continuity, organisational reputation and compliance with legal, regulatory and contractual obligation.

The Essentials ensures consistent foundations are applied to cyber security as technologies change. Evolution in artificial intelligence capabilities is a modern example where the Essentials framework can be used regardless of whether an organisation consumes, develops or deploys AI.

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has developed ASD Essentials as an evolution of the Essential Eight to help organisations direct cyber security investment towards the areas of greatest need. Through a prioritised and outcome-focused approach, the framework guides organisations in sequencing their efforts to protect critical functions, reduce risk earlier, and achieve security improvements that can be efficiently scaled across enterprise IT, cloud and operational technology environments.

For senior executives, three key aspects of the Essential series approach are relevant:

1

Cyber security posture reporting provides greater visibility and clarity to senior executives. Rather than relying on a single maturity level, the Essentials series reports posture by domains – groupings of your business functions and assets that share similar risks. Domains can be prioritised, allowing a strategic approach to protecting the most critical assets in your network.

This gives senior executives clearer visibility of where security outcomes are being achieved and where further attention is required.

2

Existing Essential Eight investment remains valuable. The ASD Essentials framework builds on the Essential Eight rather than replacing the work organisations have already completed. Existing controls and capabilities contribute to the evolved framework, while the broader approach helps organisations prioritise where additional uplift may be required.

3

Executive accountability is more explicit. The Essentials series places greater emphasis on formal executive and board-level accountability for cyber security, including oversight of organisational risk, investment and resourcing..

The introduction of the Essential series does not mean organisations are expected to start again. The transition should begin by understanding how existing Essential Eight controls and other cyber security investments contribute to alignment with the Essentials series.

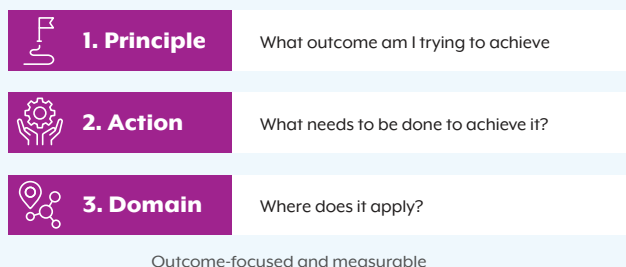
ASD Essentials series framework

The Essentials — shows what to protect, how to protect it, and where to begin.

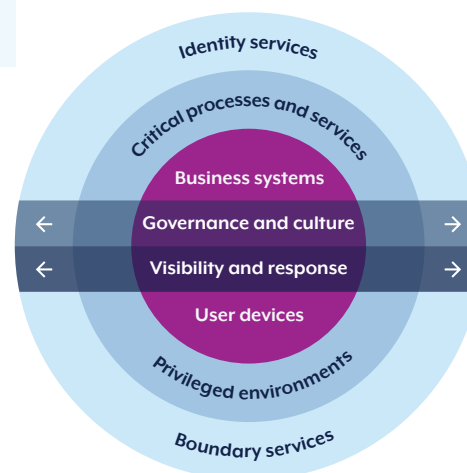
The Essentials series provide a practical approach to understanding what must be protected, what outcomes should be achieved, and where security effort should be focused.

How the framework works

This framework is a modern, principles-based approach to cyber security for Australian organisations.



The Essentials domain model



Domains are groupings of business functions and assets that share similar risks.

Separate chapters for different technology environments:

Enterprise IT

Operational Technology

Cloud

Designed to be

Future-focused

Compatible

Flexible

Threat-informed

Why it matters to leaders

+ Clear priorities	Focus effort on what matters most.
+ Risk-aligned investment	Direct resources to greatest risk reduction.
+ Better decisions	See strengths, gaps and exposure.
+ Stronger accountability	Enable governance and oversight.
+ Consistent reporting	Measure outcomes across the enterprise.
The Essential series builds upon investments made under the Essential Eight	

Implementation journey

1) Understand

Context, risks and obligations

2) Select

Relevant priorities and domains

3) Plan

Activities, investment and sequencing

4) Implement

Actions that achieve outcomes

5) Assess & report

Effectiveness and improvement

6) Sustain

Maintain, reassess and refine

Purpose

This guidance helps senior executives understand the ASD Essentials series framework and the role they play in its successful implementation. It outlines the key considerations for governance, investment, risk management, reporting and oversight, while helping leaders understand what they need to know to empower their teams to deliver effective cyber security outcomes. The guidance also identifies the questions decision-makers should ask before approving investment and throughout implementation to ensure progress, risks and security posture are managed.

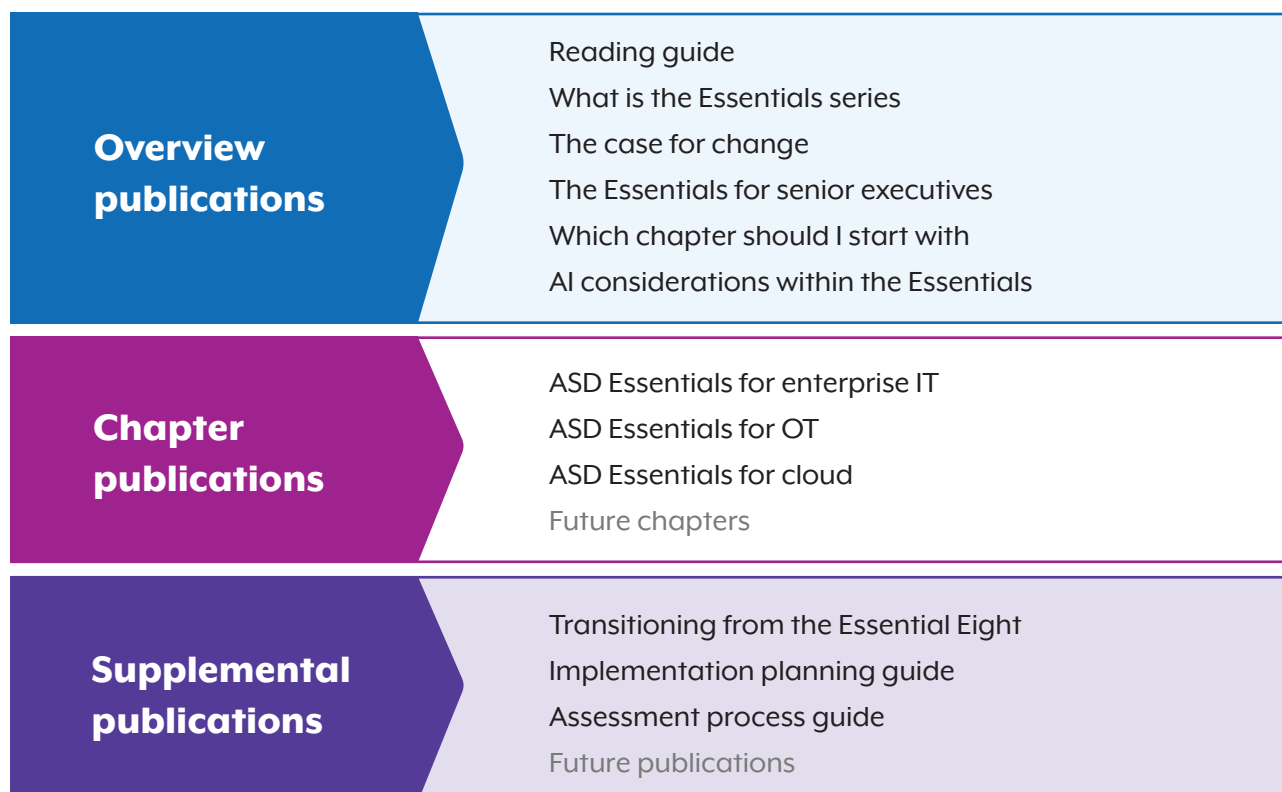


Figure 1. ASD Essentials framework

Benefits of the ASD Essentials series

The ASD Essentials series gives organisations a clear view of what to protect, what cyber security outcomes to achieve and where to begin.

Each chapter uses the same *principles*, *actions* and *domains* model, supporting a consistent approach as organisations adopt guidance for different technology environments. This model aims to answer a number of implementation questions as shown.

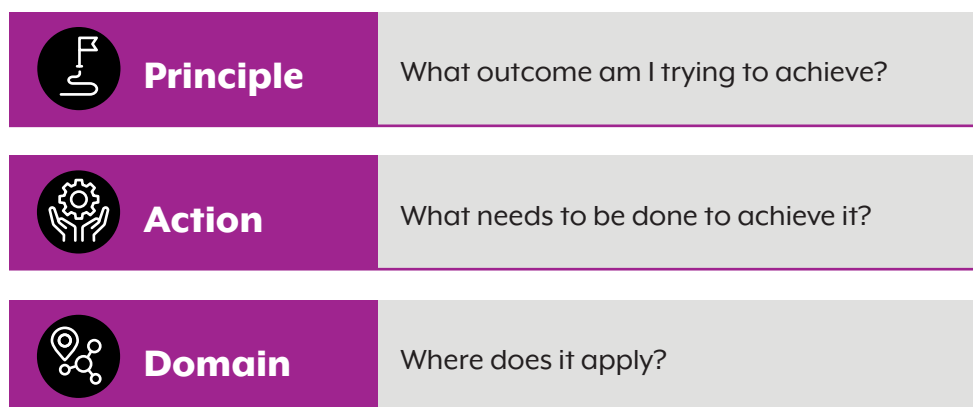


Figure 2. How principles, actions and domains work together

Benefits of this model include:

- **Priority phases** help organisations sequence technical implementation in a prioritised and risk-informed manner rather than attempting to uplift the entire environment at once.
- **Actions** describe what must be achieved without prescribing a particular vendor, product or architecture. Organisations can select controls that suit their environment and obligations.
- Existing investment in Essential Eight controls can contribute to **actions** in the Essential series where they achieve the required outcomes.
- Reporting by **domain** provides decision-makers with clear visibility of effective security outcomes, outstanding gaps, and priorities for further investment or risk treatment.
- Each chapter uses the same **principles**, **actions** and **domains** model, supporting a consistent approach as organisations adopt guidance for different technology environments.

Priority 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.

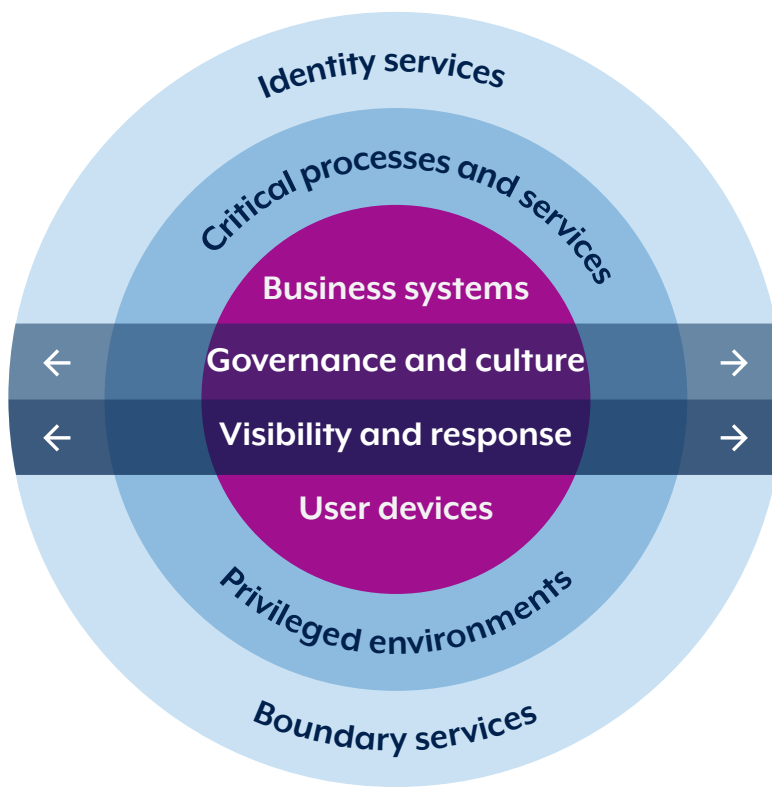


Figure 3. Essentials for enterprise IT priority phases

Improved visibility of security posture

In the ASD Essentials series framework, *domains* help organisations organise cyber security around business functions and the assets that support them. By grouping areas with similar risks, *domains* enable organisations to prioritise security efforts where they will have the greatest impact. Reporting security posture by *domain* provides decision makers with clearer visibility of strengths, weaknesses and risk exposure, supporting more informed decisions about investment, risk treatment and improvement priorities.

Table 1 summarises the cyber security risk addressed by the *ASD Essentials for enterprise IT domains*.

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 controls degrading over time.
Visibility and response	Procedures and capabilities for detecting, analysing and responding to cyber security events and incidents.	Limited visibility and response capability 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	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.
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 and may affect health and safety.
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.

Transitioning Essential Eight investment

It is important to remember that when transitioning to the Essential series, existing Essential Eight investment remains valuable. Many controls implemented under the Essential Eight contribute to actions in the ASD Essentials series chapters, but organisations should assess those controls against the new framework rather than assume they are equivalent.

For example, organisations that have invested in multi-factor authentication (MFA) under the Essential Eight can build on that capability. The ASD Essentials series continues to recognise MFA as an important security measure, while also helping organisations address a broader range of identity-related risks. This provides stronger protection against the techniques commonly used by today's cyber adversaries.

Organisations should identify which existing controls meet or contribute to applicable actions, where those controls need to be extended and where new capability is required. *Transitioning from the Essential Eight provides detailed transition guidance.*

Executive oversight of implementation

Cyber security requires ongoing governance, investment and sustainment. The ASD Essentials framework is designed to support a continuing program that aligns governance, architecture, operations and resourcing with organisational risk.

The series strengthens executive oversight of cyber security by requiring clear accountability at executive and board levels. It encourages organisations to define their cyber security risk appetite and ensure sufficient people, funding and resources are available to implement, maintain and continuously improve security measures over time.

These capability requirements apply across all priority phases. Senior executives should therefore consider implementation and sustainment together as an ongoing capability.

What senior executives should expect

Senior executives should consider the following factors when making decisions about implementation, investment and ongoing oversight of ASD Essentials implementation.

- **A clear understanding of the sequencing model.** Priority phases recommend the implementation order for technical domains. They are not maturity ratings and do not indicate assurance. A statement such as ‘we have reached priority phase 2’ describes implementation scope, not how secure the organisation is. Overall security posture is expressed through the effectiveness ratings.
- **Formal executive and board-level accountability.** Executive and board-level cyber security accountabilities should be formally defined and established, including responsibility for setting, monitoring and adjusting organisational risk appetite. Senior executives should understand where these accountabilities sit within their organisation.
- **Alignment with operating context.** The implementation plan should reflect regulatory obligations, critical functions, stakeholder expectations, risk appetite and available resources.
- **A current-state baseline.** The organisation should assess applicable actions in the relevant domains and identify gaps. Existing Essential Eight and other cyber security investments should be included in this assessment.
- **Realistic implementation and sustainment expectations.** Implementation is not a one-time activity that ends when the priority phases are complete. The program should account for implementation, ongoing operation, reassessment and refinement. There is no completion date for effective cyber security.
- **Sustainable resourcing.** Funding proposals should distinguish implementation costs, ongoing operation and assessment or assurance costs. Actions require personnel, processes and resources to remain effective over time.
- **Evidence of effectiveness.** Claims that an action or security outcome is effective should be supported by appropriate evidence. Depending on the environment and risk, this can be validated through activities such as simulated exercises and independent testing.
- **Clear reporting arrangements.** The organisation should agree what will be reported, how often and to whom. Reporting should show assessed posture, material gaps, remediation progress, accepted risk and domains **not assessed**.
- **Continued regulatory compliance.** Organisations should continue to meet applicable legal and regulatory obligations during transition to the Essentials series and follow any direction issued by relevant regulators.

Questions senior executives should ask

Senior executives should ask these questions when considering an ASD Essentials implementation proposal and revisit them as the program progresses. The answers should inform investment decisions, risk acceptance and subsequent reporting.

- Which of our key functions and assets sit in each domain, and which domains hold the assets whose compromise would be most consequential for the organisation?
- What did our Essential Eight investment buy us under the ASD Essentials framework, and what is genuinely new work, such as the governance principles and the expanded detection and response capability?
- When will we see the first posture report, what will it cover and what will be reported as **not assessed**? Are the reasons justified for the assets deemed not assessed?
- What specific risk reduction do priority phase 1 investments provide? Which observed attack paths does hardening those domains disrupt for us?
- Where does the plan depart from ASD's recommended sequencing, and what is the documented, risk-based justification?
- How will effectiveness be validated, and will independent assessment or adversary-simulation testing be used, and on what cycle?
- What are the ongoing operational costs and resourcing needs once priority phase 3 is reached, and how will resourcing be reviewed against threat trends and incident outcomes?
- How are exceptions, compensating controls and accepted risks governed? Who owns them, when do they expire and when do we re-approve or close them?
- What are the anticipated disruptions to operations and user experience during implementation, and how will they be managed?
- How will we continue to meet our current regulatory reporting obligations during the transition?

These factors and questions are not exhaustive. By considering these and others relevant to the organisation's unique operating environment, senior executives can turn the ASD Essentials framework into a well-governed, strategic investment rather than a compliance exercise.

Conclusion

The ASD Essentials framework gives senior executives a structured way to oversee cyber security investment, implementation and sustainment. Priority phases help sequence effort, while assessment by domain provides visibility of where security outcomes are effective and where material gaps remain.

Existing Essential Eight investment continues to provide a foundation, but organisations should assess it against the applicable principles and actions in the relevant ASD Essentials series chapter.

Effective implementation requires more than technical controls. It now requires clear accountability, sustained resourcing, evidence of effectiveness and reporting that enables senior executives to understand and manage cyber security risk.



**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>

