



Australian Government
Australian Signals Directorate

cyber.gov.au

ASD Essentials overview

What is the Essentials?

The word 'Essentials' in a white, sans-serif font, preceded by a stylized 'E' logo consisting of a white square with a small purple square in its top-left corner.

Essentials

What is the Essentials?

The ASD Essentials series is a framework that provides organisations with a consistent approach to cyber security across different technology environments.

The series is made up of environment-specific chapters. Each chapter applies the same underlying model while accounting for the threats, risks and operational considerations relevant to the environment it covers.

Current ASD Essentials series chapters address enterprise IT, cloud and operational technology. The series is structured so additional environment-specific chapters can be added as needed.

Organisations may find that one chapter is relevant, several chapters apply to different parts of their environment, or a business function depends on assets covered by more than one chapter.

Each chapter uses the same three layers: **principles**, **actions** and **domains**.

How the Essentials framework is structured

Each ASD Essentials series chapter uses principles, actions and domains to describe the security outcomes organisations should aim to achieve, what they need to do and where those requirements apply.

- **Principles** describe the cyber security outcomes an organisation should achieve.
- **Actions** describe what needs to be done to achieve those outcomes.
- **Domains** describe the business functions and assets to which the actions apply.

Figure 1 shows how the three layers answer a sequence of questions.

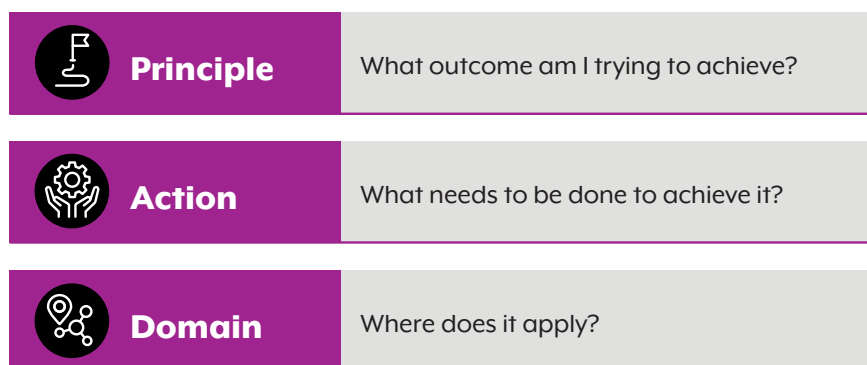


Figure 1. How principles, actions and domains work together

Principles

ASD Essentials principles are drawn from the cyber security principles in ASD's *Information Security Manual (ISM)* and align with ASD's *Modern Defensible Architecture*. They describe the security outcomes organisations should achieve.

The principles provide a consistent foundation across the ASD Essentials series. The intent of a principle remains the same between chapters, while the actions used to achieve that outcome may differ.

Not every principle is relevant to every chapter. Each chapter identifies the principles that apply to its environment.

Actions

Actions describe the administrative and technical requirements used to implement a principle and achieve its intended security outcome.

Actions may vary between chapters because different technology environments have different risks and constraints. The actions selected for each environment consider:

- the relevant threat model
- operational requirements
- commercial viability.

This allows each chapter to account for factors such as threats affecting the environment, availability and safety requirements, system lifecycles and whether suitable capabilities can be implemented at a practical cost and scale.

Where appropriate, actions are mapped to the techniques in the [MITRE ATT&CK](#) knowledge base to show the adversary behaviours they are intended to address. Figure 2 shows how an action is mapped to ATT&CK techniques.

Essentials action		Mapped MITRE ATT&CK techniques			
Principle	Identify, credential and access management	ATT&CK technique	Technique ID	Tactic	What this action disrupts
Action	 Use phishing-resistant MFA for users authenticating to systems, including from untrusted, external or high-risk locations	Valid accounts	T1078	Initial access	Stolen credentials alone are not enough
		Account manipulation	T1098	Persistence	Defines the access needed to register new credentials
		Brute force	T1110	Credential access	Guessing or spraying a password no longer gains access
		Remote services	T1021	Initial access	Exposed remote access cannot be entered with credentials alone
Domain	Assets across all technical domains				



Key point: This is a small instance of the ATT&CK flow. Many other techniques may be relevant to this action

Figure 2. Mapping an action to ATT&CK techniques

Domains

Domains are groupings of business functions and assets that share similar risks. They help organisations focus security efforts where they will deliver the greatest reduction in risk, rather than applying the same security measures across an entire environment.

Shared risk means comparable exposure and consequence of compromise, not that every asset carries an identical risk rating.

A domain is a logical grouping rather than a network or organisational boundary. Assets within a domain may be spread across different systems, locations, suppliers or parts of an organisation.

Domains are used consistently across the ASD Essentials series. However, the specific assets within a domain may vary between chapters according to the technology environment.

Each chapter identifies the domains relevant to its environment and maps actions to the domains where they are applied. Figure 3 shows how domains are grouped together.

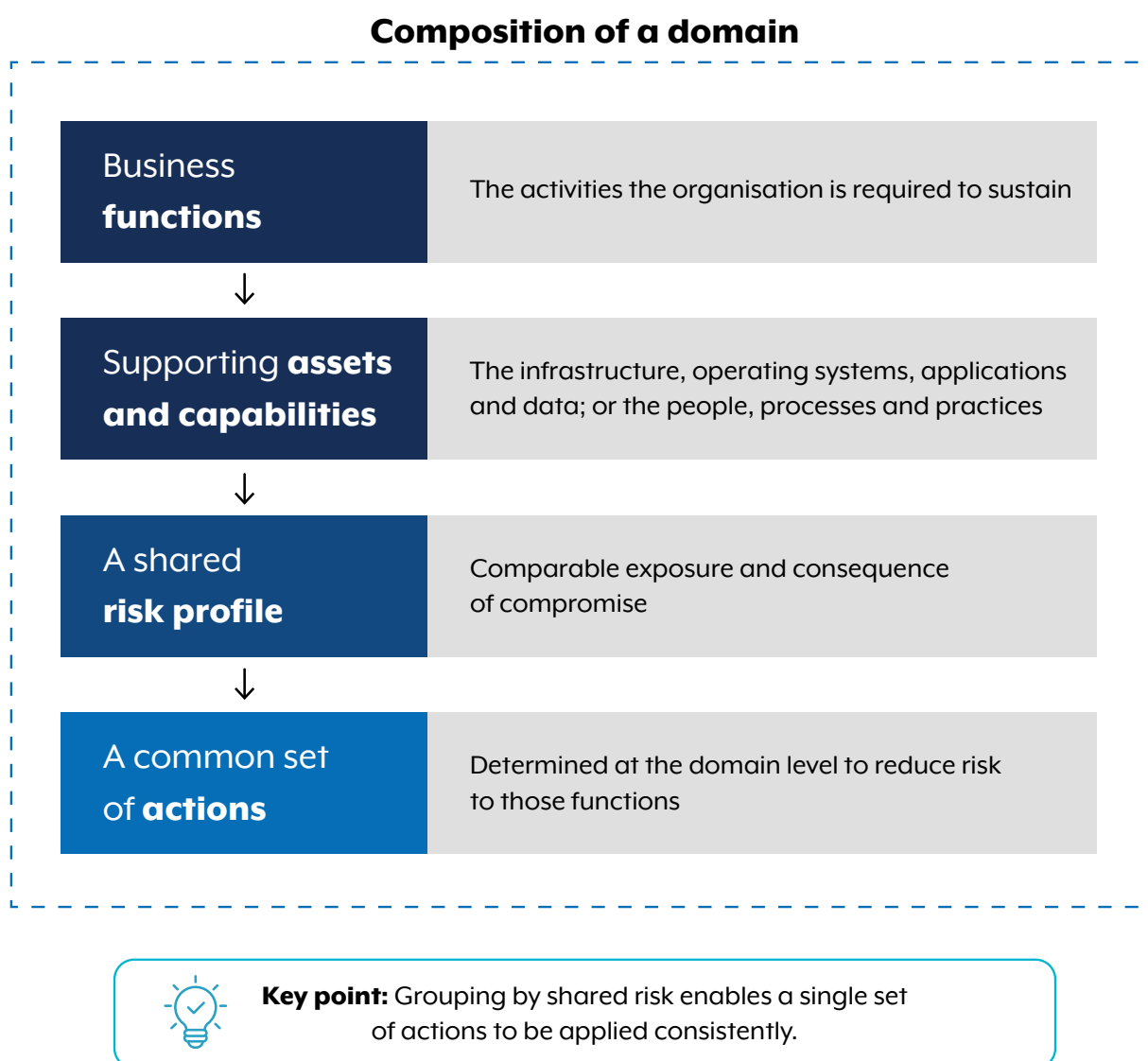


Figure 3. Composition of a domain

How the three layers work together

Principles, actions and domains are designed to be used together.

The principle establishes the intended security outcome. The action describes what the organisation needs to do to achieve it. The domain establishes the assets and functions to which the action applies.

This means implementation considers an action in the context of a particular domain, rather than treating the action as a standalone requirement.

Using the ASD Essentials series

Organisations should use the ASD Essentials series chapter or chapters relevant to their technology environments. There is no requirement for every organisation to use every chapter or to apply relevant chapters in set order.

When applying an ASD Essentials series chapter, an organisation follows the workflow in Figure 4.

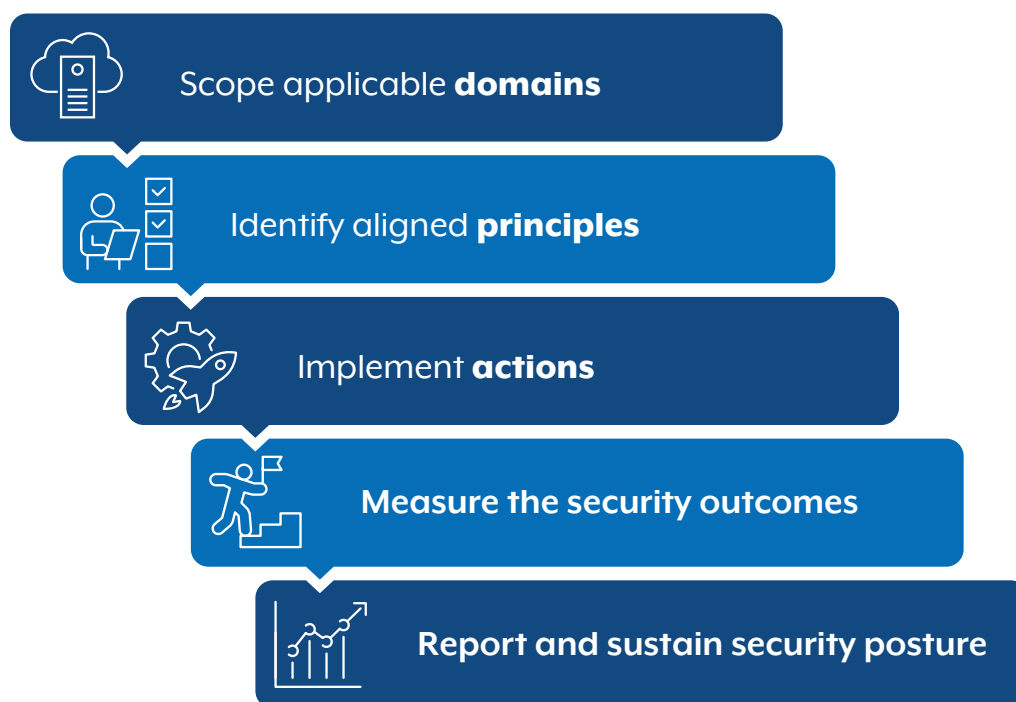


Figure 4. How to implement an ASD Essentials chapter

The common structure of principles, actions and domains supports a consistent approach across different environments while allowing implementation to reflect the risks and operational considerations relevant to each environment.

Other publications in the ASD Essentials series provide guidance on [selecting a chapter](#), [planning implementation](#), [assessing cyber security posture](#) and [transitioning from the Essential Eight](#).

**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>

