



Australian Government
Australian Signals Directorate

cyber.gov.au

ASD Essentials overview

The case for change

 Essentials

Why change was needed

Australia's cyber threat environment continues to evolve. Sophisticated tradecraft is used against a broad range of Australian organisations, while malicious actors can operate at scale and target organisations through their suppliers, service providers and other connections.

Australia's dependency on digital and internet-connected technology makes it an attractive target. ASD's Annual Cyber Threat Report consistently finds that cyber threats affect organisations across all sectors, regardless of size or profile. An organisation's cyber security risk is also influenced by the information and systems it holds, the services it supports and the organisations it connects to.

Organisations also operate across technology environments with different risks, operational requirements and constraints. Enterprise IT, cloud and operational technology can require different approaches to achieving the same security outcomes. Emerging technologies may introduce further considerations over time.

The Essential Eight maturity model provided organisations with a prioritised set of controls for strengthening their cyber security. However, a fixed set of prescriptive controls does not always translate across different technology environments or remain suitable as threats and technologies change.

The evolution in artificial intelligence capabilities is a clear example where the consistent principles in the Essentials will ensure cyber security foundations remain stable as organisations adopt AI technologies and respond to AI-enabled threats.

ASD's guidance therefore needs to provide consistent security outcomes while allowing organisations to achieve those outcomes in ways appropriate to their environment.





Informed by the threat environment

The ASD Essentials series is informed by ASD's understanding of the threats affecting Australian organisations. This draws on a combination of intelligence insights, cyber security incident data, partner feedback and public cyber threat reporting.

Together, these sources help ASD identify the security outcomes that matter most and ensure the guidance remains relevant to the threats Australian organisations face.

Evolving the approach

The ASD Essentials series responds to changes in the threat and technology environment through a threat-informed and principles-based approach.

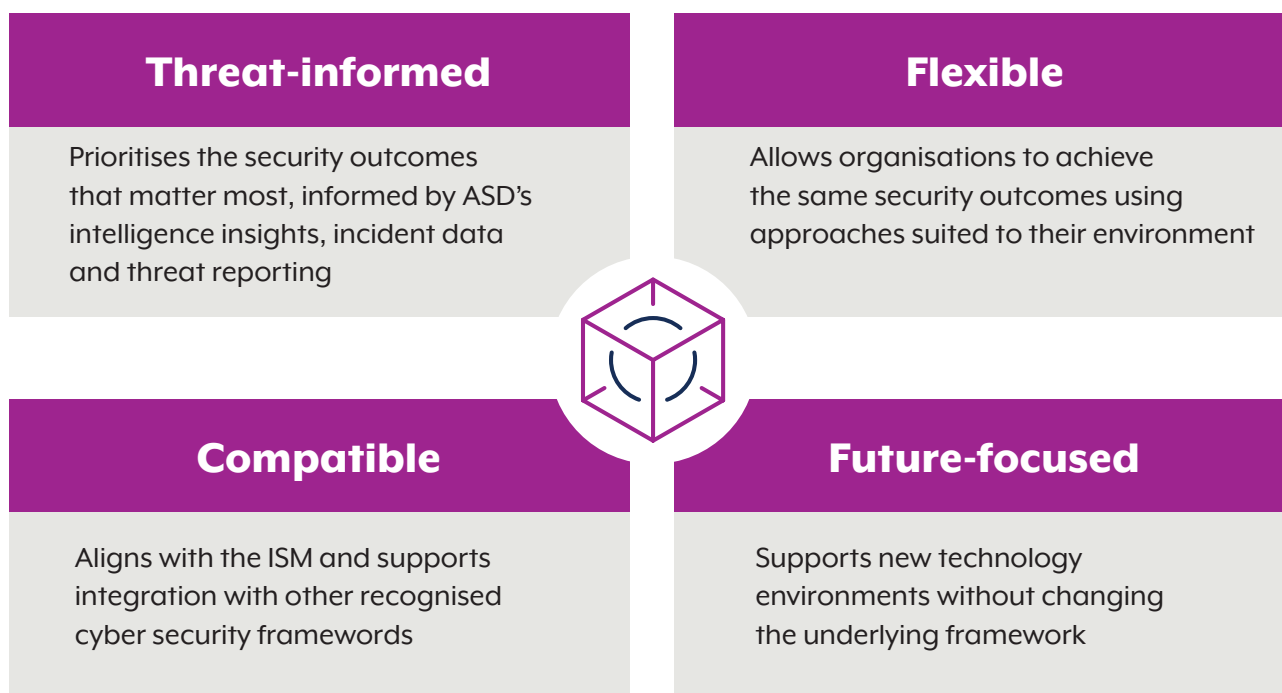
The series focuses on the security outcomes organisations should achieve rather than prescribing a particular product, vendor or architecture. Principles describe enduring security outcomes, while supporting actions describe what organisations need to do to achieve them.

This allows organisations to select controls and implementation approaches suited to their environment while working towards consistent security outcomes.

ASD Essentials series chapters apply this approach to different technology environments. This allows the guidance to account for the risks, operational requirements and constraints of each environment without changing the underlying approach.

Designed to adapt

The Essentials approach is designed to remain relevant as threats, technologies and operating environments change.



The ASD Essentials series is:

Threat-informed

Prioritises the security outcomes that matter most, informed by ASD's intelligence insights, incident data and threat reporting.

Flexible

Allows organisations to achieve the same security outcomes using approaches suited to their environment.

Compatible

Aligns with the Information Security Manual and supports integration with other recognised cyber security frameworks.

Future-focused

Supports new technology environments without changing the underlying framework.

The series also uses **priority phases** to recommend the order in which domains should be addressed. This helps organisations sequence implementation and focus effort on the security outcomes that ASD assesses will provide the greatest reduction in cyber security risk.

By focusing on enduring security outcomes rather than a fixed implementation method, the ASD Essentials series provides a consistent approach that can adapt as threats, technologies and operating environments change.

**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>

