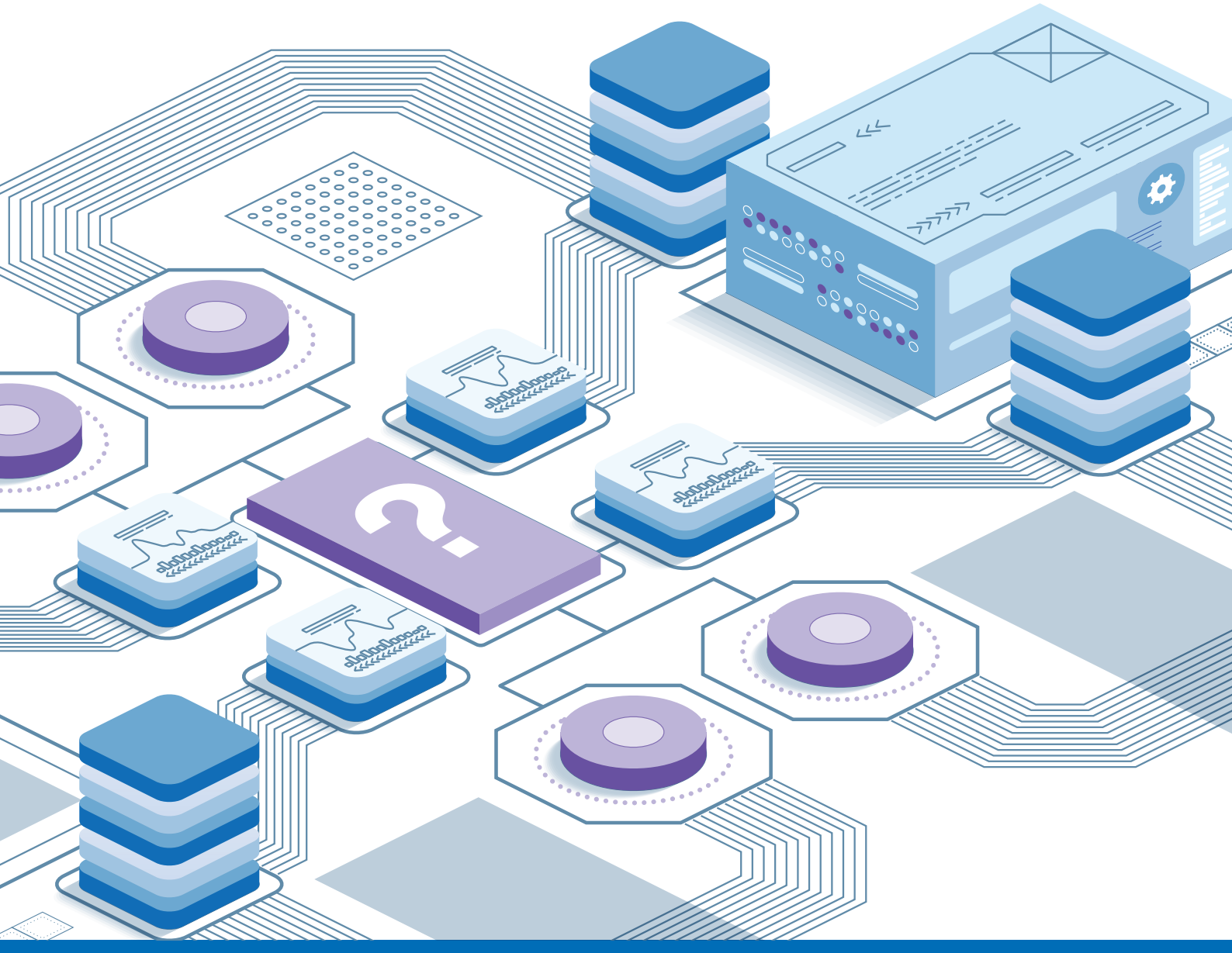
Modern defensible architecture for senior decision-makers



Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

Te Tira Tiaki

Government Communications Security Bureau

National Cyber Security Centre

NEW ZEALAND

Bundesamt für Sicherheit in der Informationstechnik

国家サイバー統括室

National Cybersecurity Office

JPCERT CC®

警察庁

National Police Agency

National Cyber and Information Security Agency

NÚKIB

Table of contents

Executive summary

Australian organisations, industries and individuals remain the target of malicious cyber actors. Cyber security continues to become more complex as organisations embrace flexible working, technologies rapidly develop, and the threat landscape evolves. The nature and persistence of threat actors targeting Australian networks require organisations to adopt a stance of 'when', not 'if', a cyber security incident will occur. The threat has made it increasingly difficult for network defenders to detect, prevent and respond to cyber security incidents.

Modern defensible architecture (MDA) can assist organisations to adapt to the contemporary threat landscape by applying secure design and architecture in their cyber security strategy, resilience planning and implementations. It helps organisations move from reactive and disjointed security measures to proactive cyber security architecture.

The transition to MDA is a strategic journey, not a single project. To assist organisations on this journey, MDA brings together key principles from cyber security architecture into 10 core **Foundations for modern defensible architecture** (the MDA Foundations). Each MDA foundation is mapped to contemporary threat contexts to help prepare organisations to adapt to current and emerging cyber threats and challenges.

Organisations should ensure that continual effort is applied to hardening and protecting existing systems in parallel with implementing MDA.

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) and the following international partners provide the recommendations in this guide:

- Canadian Cyber Security Centre – Canada
- National Cyber Security Centre – New Zealand
- Bundesamt für Sicherheit in der Informationstechnik – Germany
- National Cybersecurity Office – Japan
- JPCERT Coordination Centre – Japan
- National Police Agency – Japan
- National Intelligence Service – Republic Of Korea
- National Cyber and Information Security Agency – Czechia

Document purpose

This document has been developed to assist senior decision-makers to understand the contemporary threat landscape and show how MDA can be used within organisations to defend against current and future threats.

This document prepares senior decision-makers to take practical and proactive steps in the design and build of their enterprise ICT systems and future investment roadmaps. It provides a framework for understanding the threat landscape and thinking about key decisions, including cyber security as a driver of long-term outcomes.

This guidance also presents key factors and questions that senior decision-makers can consider before investing in, or implementing, MDA for their organisation.

Audience and scope

This guidance is written for organisational **senior decision-makers**, including **boards**, who set strategic direction, determine resource allocation, manage risk and provide oversight of their organisation's cyber security.

The information in this guidance is applicable to all types of information environments, including cloud, on-premises and hybrid.

This guidance assumes a **basic level** of computing and cyber security knowledge on the part of the reader.

The case for change

Organisations need to expand from traditional fixed perimeter-based security to a more resilient approach centred on identities, devices and data. Organisations must assume that threats can and do exist both inside and outside their network, and therefore must invest in protective security measures and technologies that ensure continuous authentication and authorisation of every user, device and application, regardless of their location. Security cannot be treated as a one-time setup, it must be treated as a continuous, adaptive process, which evolves as the organisation goes through change.

Protective security practices, such as **zero trust** and **secure-by-design**, have emerged as better-practice approaches to uplift cyber resilience. Yet it can be difficult for organisations to know how to prioritise these uplift activities within their security architecture in a way that is appropriate for their unique threat environment and also makes use of available technologies. MDA helps address these challenges.

What is security architecture?

Security architecture is about knowing what kind of cyber security threats organisations are facing now and into the future – and then deciding what measures, structures and processes need to be put in place to protect and defend the organisation's core assets.

What is modern defensible architecture?

Modern defensible architecture (MDA) is the name of ASD's ACSC's mission to ensure that organisations are considering and applying secure design and architecture in their cyber security strategy, resilience planning and implementations. It is based on the idea that there are certain elements of business and enterprise architecture that are common to any organisation that values cyber security.

MDA has been developed to assist organisations in preparing and planning for the adoption of technologies based on:

1. layered architecture and traceability as a methodical approach that separates security design into distinct levels, each addressing a specific aspect or scope of security management, from high-level business objectives down to specific technical implementations
2. zero trust principles of 'never trust, always verify', 'assume breach' and 'verify explicitly', implemented through zero trust architecture components and capabilities
3. secure-by-design practices that institute an 'early and sustained security' mindset within organisations when it comes to the development and/or procurement of software products and services.

MDA offers a structured framework that complements and strengthens other key mitigation strategies and controls frameworks, including the *Essential Eight Maturity Model* and the *Information Security Manual*.

The biggest challenge for organisations is knowing where to start and what to prioritise. For many organisations, adopting MDA likely represents a generational approach with multiple discrete projects integrated into the organisation's cyber security roadmap. This is essential for building a more secure and resilient digital environment, enabling better risk management and safeguarding critical data and systems.

Foundations for modern defensible architecture

The *Foundations for modern defensible architecture* (the MDA Foundations) provide a baseline of 10 secure design and architecture practices that prepare organisations to adapt to current and emerging cyber threats and challenges. They provide a cohesive, logical approach for designing, building, maintaining, updating and enhancing digital systems. The MDA Foundations are inputs to the business architecture and enterprise architecture that organisations will develop as they prepare themselves for future challenges.

Each of the MDA Foundations represents an organisational goal or capability that facilitates a more efficient adoption of zero trust architecture and technologies. While many of the individual MDA Foundations covered in the guidance are not new concepts, when combined they provide organisations the basis of a modern defensible architecture that is adaptable to emerging technologies and practices, and resilient to current and emerging cyber threats and challenges.

Investing in modern defensible architecture

Organisations that work towards implementing the MDA Foundations will be best prepared to adapt to current and emerging cyber security threats and challenges. However, every organisation is different, and the way they approach and prioritise implementation will be unique to their organisational strategy, business and security objectives, and threat context.

Investing in modern defensible architecture is specific guidance developed for ICT Managers and Enterprise Architects to support them in developing an MDA investment roadmap to present to those responsible for making cyber security and IT investment decisions. The guidance enables organisational leaders to make informed decisions on investment opportunities, design considerations and gaps, and identify appropriate people, skills and technologies.

Enabling a modern defensible architecture

Overview

MDA is much more than a simple one-time IT fix. It can't be bought off the shelf as a single product, service or specific toolset. For organisations, building good security architecture means weaving the principles and foundations of MDA into every part of their systems, budgets and operational plans. Just as important, organisations need to factor these requirements into their hiring, training and ongoing professional development initiatives.

Senior decision-makers considering investing in and implementing an MDA strategy should be thoroughly satisfied with several key factors before committing to such an undertaking. MDA isn't just a project, it's a fundamental shift in security philosophy that impacts people, processes and technology across an entire organisation.

Key factors for senior decision-makers to consider

Before pursuing an MDA strategy, senior decision-makers need to consider the following:

- **An understanding of zero trust:** Senior decision-makers need to be aware of the principles of zero trust, and understand that zero trust is a departure from traditional fixed perimeter-based defence; it assumes that threats can originate from anywhere, including from within the network.
- **Strategic alignment with business objectives:** Any significant security overhaul must directly support the organisation's overarching business objectives.
- **An understanding of the current security landscape:** Before starting, senior decision-makers need to be confident that the organisation has thoroughly assessed its existing security posture, identified vulnerabilities and catalogued its critical assets, applications and data. This forms a baseline against which MDA improvements can be measured.
- **Realistic expectations regarding scope and complexity:** Senior decision-makers need to understand that implementing MDA will likely require a generational approach that will touch virtually every system, application and user access point.
- **Adequate resource allocation:** MDA represents a substantial business investment. Senior decision-makers need to ensure that the necessary financial capital, skilled personnel and technological tools are, or will be, allocated.
- **Robust leadership and governance:** Successful implementation of MDA requires strong leadership and a clear governance framework that integrates IT, security and business units.
- **User experience and operational flow:** Senior decision-makers need to be satisfied that implementation won't unduly hinder legitimate user access or impede business operations.
- **Technology and vendor strategy:** Modern defensible architecture isn't a single product. It's an architectural approach often built upon a diverse set of technologies. Senior decision-makers

need to be satisfied with the organisation's plan for selecting, integrating and managing various technological components.

  - For further information, see *Choosing secure and verifiable technologies: Executive guidance*.

- **Clear metrics for success and reporting:** Senior decision-makers need to understand how the effectiveness of the MDA strategy will be measured, tracked and regularly reported back to them within their unique business context.
- **Regulatory considerations:** Senior decision-makers need to understand how the organisation will continue to meet its requirements under relevant legislation and regulations.[1]

Key questions senior decision-makers should raise

Before agreeing to an MDA strategy, senior decision-makers may wish to raise and discuss the following:

- What specific, tangible security problems will MDA solve that the organisation's current cyber security approach cannot adequately address?
- What risks does the organisation face if MDA is not implemented?
- What are the anticipated disruptions or potential negative impacts to the organisation's operations during the transition phase?
- What is the organisation's strategy for addressing legacy systems and applications that may pose integration challenges within an MDA information environment?
- How will 'success' for the organisation's MDA implementation be defined and measured over the next one, 3 and 5 years?
- Will external expertise, such as independent auditors or specialist consultants, be engaged by the organisation to validate its MDA strategy and implementation?
- Will accountability for planning, implementation and sustainment of the MDA environment sit with senior decision-makers, or will accountability sit with business units?
- What are the ongoing operational costs and resource capabilities for sustaining an MDA information environment?

The factors and questions listed above do not represent an exhaustive list. However, by considering these and other factors/questions relevant to their organisation's unique operating environment, senior decision-makers can enable effective implementation of an MDA strategy. This approach will constitute a well-informed, strategic investment and will genuinely enhance the organisation's security posture and build greater cyber resilience.

1 In 2025, the Australian Government's Protective Security Policy Framework (PSPF) was updated to include requirements to embed a zero trust culture. The PSPF applies to Australian Government entities and third-party service providers delivering services to Australian Government entities. Implementing MDA will assist organisations to meet these new requirements.

Conclusion

MDA will help organisations understand and address the contemporary threat landscape, adopt future-focussed cyber security investment strategies, and be better prepared to respond to future threats as they emerge.

For senior decision-makers, MDA provides a framework for understanding and mitigating threats and risks, as well as high-level principles that can be adopted into an organisational cyber security strategy. This bridges the gap between the highest level of organisational governance, accountability and core business outcomes, and the operational level of ICT investment, cyber security and implementation.

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 2025

With the exception of the Coat of Arms 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 Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre