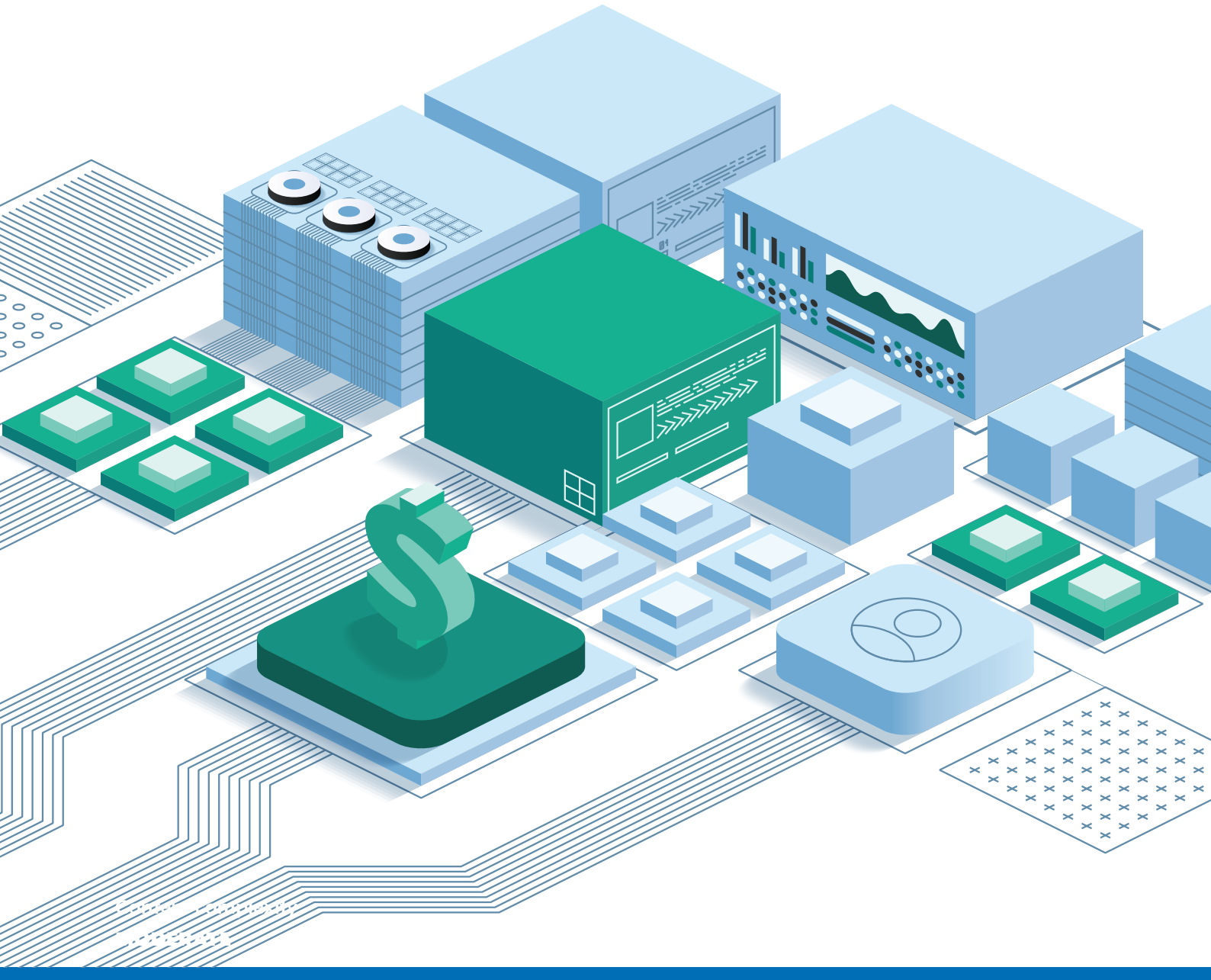
Investing in modern defensible architecture



Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

Communications Security Establishment Canada

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada

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

Introduction

Cyber threats are a fundamental business risk that can directly impact an organisation's operational continuity, financial stability, regulatory and legislative requirements, and reputation.

Organisations can take practical and proactive steps in the design and build of their information environments to significantly minimise the risk of harm to their most critical systems. By investing in and implementing **modern defensible architecture** (MDA), organisations can improve the resilience of their information environments over time, and more readily adapt controls and mitigations as threats evolve. However, every organisation is different, and the way they approach and prioritise investment and implementation will be unique to their organisational strategy, threat context, and business and security objectives.

Designing and implementing architectural improvements to an information environment takes significant **time, resources** and **investment**.

While difficult, investing in and implementing MDA delivers **significant benefits** to organisations. MDA **builds resiliency, supports continuous delivery** of business services, **empowers users** to work securely, and **provides visibility** of organisational compliance with security policies.

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

- Canadian Centre for Cyber Security – 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 guidance helps organisations develop an **MDA investment roadmap** based on their organisational strategy, business and security objectives, risk profile and threat context. The guidance enables organisational leaders to make informed decisions on investment opportunities, design considerations and gaps, and identify appropriate people, skills and technologies.

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 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*. Organisations should ensure that they harden and protect existing systems in parallel with implementing MDA.

MDA brings together these key principles from cyber security architecture into 10 core Foundations for modern defensible architecture (the MDA Foundations).

MDA is much more than a simple IT fix. It cannot be bought off the shelf as a single product or specific toolset. For many organisations, implementing MDA will require a generational approach that will touch virtually every system, application and user access point. This means weaving MDA methods, technologies and strategies into every part of an organisation's systems, budgets and operational plans. Just as importantly, organisations need to factor these requirements into their hiring, training and ongoing professional development initiatives.

Audience and scope

This guidance is written for **ICT managers, enterprise architects** and **cyber security architects** to support them in developing an MDA investment roadmap to present to those within their organisation responsible for making cyber security and information technology investment decisions.

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

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

Supporting material

Foundations for modern defensible architecture

This document references the MDA Foundations throughout. The MDA Foundations provide a baseline of 10 secure architecture and design practices that prepare organisations to adapt to current and emerging cyber threats and challenges. The MDA Foundations provide a cohesive, logical approach to designing, building, maintaining, updating and enhancing digital systems.

Modern defensible architecture for senior decision-makers

Modern defensible architecture for senior decision-makers is written for organisational senior decision-makers, including boards, who set strategic direction, determine resource allocation, manage risk, and provide oversight of an organisation's cyber security.

Develop an MDA investment roadmap

ASD's ACSC recommends that organisations develop an investment roadmap to facilitate implementation of the MDA Foundations. Organisations that assess their strategy, people and skills, and technology using this guidance will be well-positioned to accomplish the goals of MDA.

Figure 1 outlines the staged approach of this guidance.

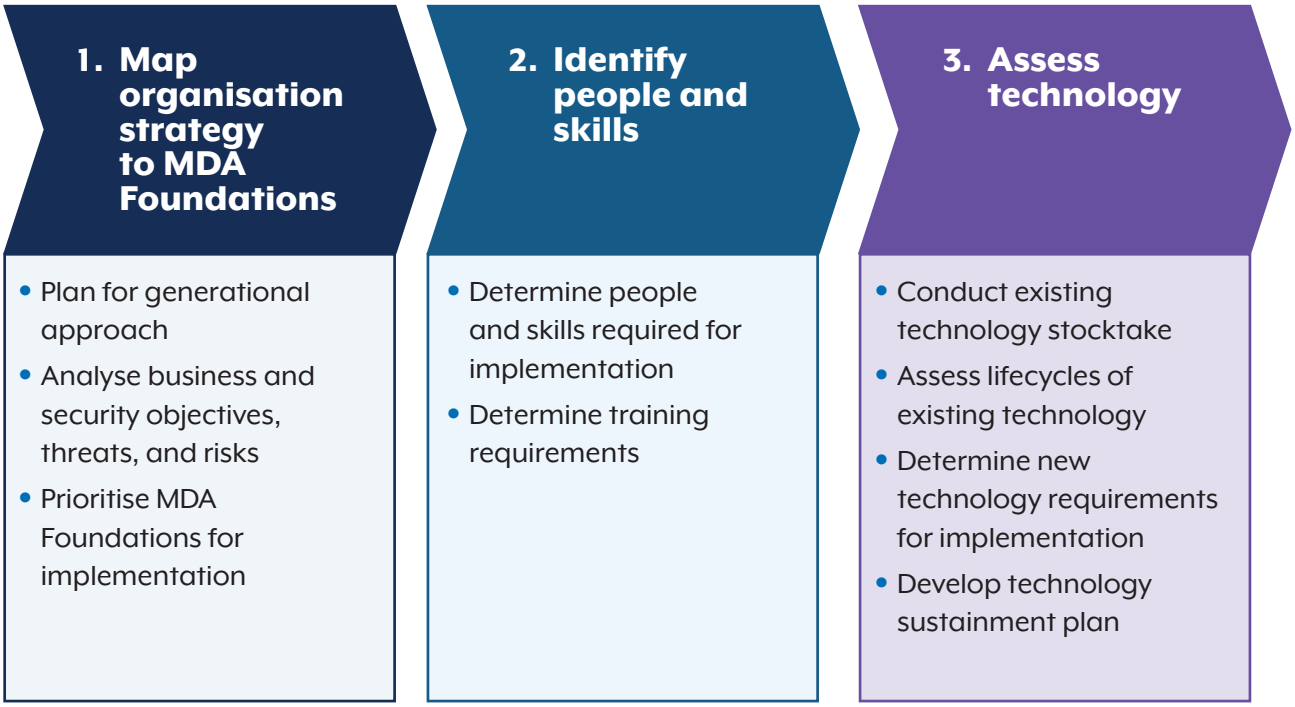


Figure 1. Investment stages

This guidance provides a three-staged approach for developing an **MDA investment roadmap**:

1. Analyse strategic business objectives and identify complementary security objectives in order to determine which MDA Foundations to prioritise.
2. Analyse current people, skills and training to identify gaps that need addressing in order to successfully implement and use capabilities for the prioritised MDA Foundations.
3. Review existing technology against business and security objectives and prioritised MDA Foundations to identify where technology uplift can be employed, or where new technology needs to be implemented.

While this guidance presents the steps chronologically, they are interlinked. The 3 stages work together and all 3 are necessary for the successful development of an MDA investment roadmap. Ultimately, each key area – strategy, people and skills, and technology – must feed into the organisation's investment roadmap. Figure 2 shows how each stage feeds into the next to build an investment roadmap.

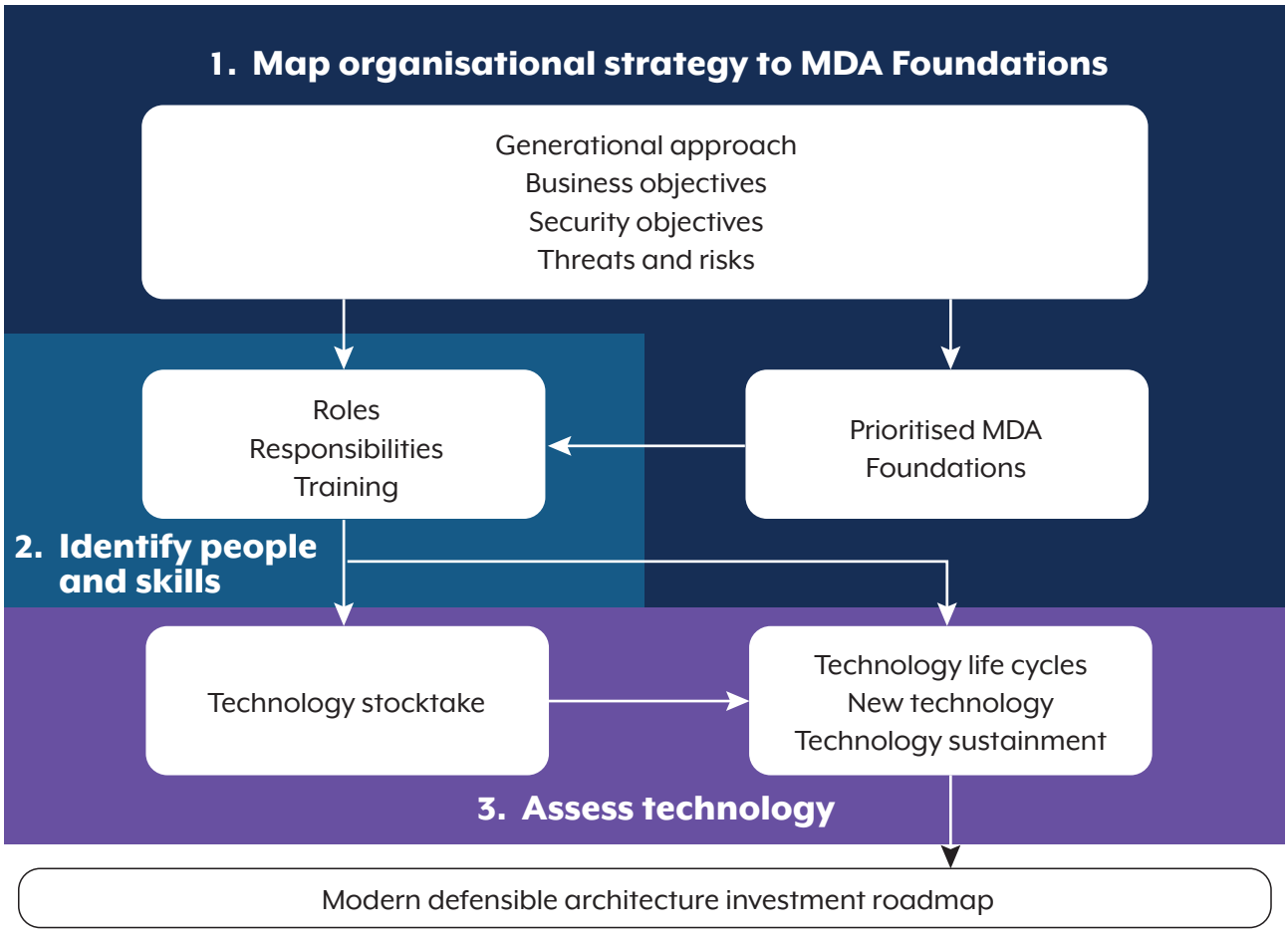


Figure 2. Investment roadmap

Each step outlines key **questions to consider**. Organisations should endeavour to answer as many of these questions as possible. However, the questions do not represent an exhaustive list. They should be supplemented with specific questions, insights and risk assessments that are relevant to the organisation's unique operating environment.

The investment roadmap will form a critical component of the organisation's future security roadmap. Each implementation of a new MDA Foundation will provide a positive feedback loop to already established MDA Foundations, further enhancing the effectiveness of security controls.

Stage 1 – Map organisation strategy to MDA Foundations

Figure 3. Stage 1

Mapping business and security objectives, based on both threats and risks, to the MDA Foundations will enable organisations to identify priority areas for investment.

When beginning their MDA implementation, no two organisations will be starting from the same point. Previous ICT investments will have already shaped the security posture of the organisation's information environments. Organisations will need to take this into account and consider which factors are important to their business and security objectives, combined with their unique risk profile and threat context.

This does not mean that current efforts or investments are incompatible with MDA. Existing strategies, people and skills, and technologies can and should be leveraged when developing an MDA investment roadmap.

Generational approach

Modern defensible architecture implementation must be considered as a long-term security strategy, one that aligns with business resilience, digital transformation and operational scalability.

Instead of focusing on short-term compliance objectives or technology refreshers, MDA implementation should focus on continued investment over time to achieve generational transformation.

MDA is not a short-term solution to discrete cyber security challenges, it is about positioning organisations for long-term defensibility and resilience. Therefore, MDA requires a realistic understanding of scope and complexity and a solid commitment to a deliberate, phased investment strategy.

Questions to consider:

1. Does the organisation have a long-term cyber security roadmap?
2. Are organisation investments focused on short or long-term challenges?
3. Will the proposed solutions allow the organisation's security architecture to evolve as business and security objectives evolve?
4. Can the organisation's security architecture evolve without being rebuilt from scratch?
5. Will investment be allocated to building a human capability to support the ICT investment?
6. Does the strategy consider increased visibility and overheads as new data sources and technologies are implemented, and how these will impact staffing and other technical solutions?

Figure 4 provides an example of the generational approach organisations will need to take when targeting priority areas within their information environment for MDA uplift. Each organisation is different and will start in areas that are the highest priority to them.

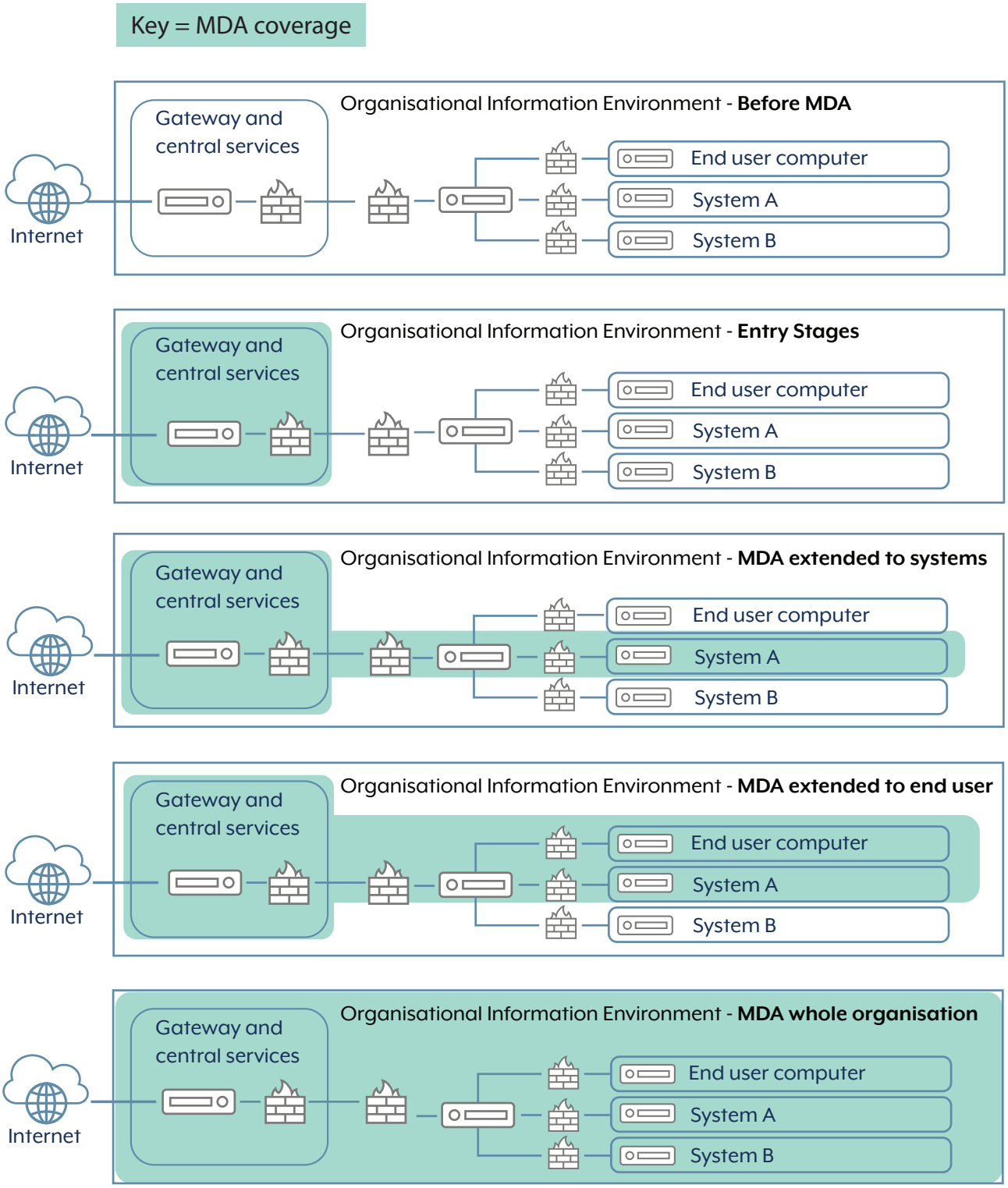


Figure 4. Generational approach to uplift

Business objectives

Organisational business objectives will influence prioritisation of the MDA Foundations and how they may be achieved. Security objectives will support and enable business objectives. The MDA Foundations need to achieve these security objectives. For example, organisations may have an operating model that allows employees to work remotely, which would introduce a requirement for secure enterprise mobility.

Questions to consider:

- What are the organisation's top business objectives for the next 3 to 5 years?
- What current digital initiatives are considered 'mission-critical' to deliver on the organisation's business objectives?
- How does the organisation maintain customer trust, and what commitments has the organisation made to build confidence in services and deliverables?
- What existing partnerships and external relationships are important to maintaining continuity of services and operations?
- What systems, services and data is the organisation responsible for?
- How do users currently interact and access organisational systems, services and data?
- What jurisdictions, industry regulations or existing contracts is the organisation required to comply with to ensure unrestricted operations?
- What platforms are required to support or facilitate the organisation's ability to deliver services and products?
- What are the organisation's ways of working; for example, working from home (WFH), secure enterprise mobility, bring-your-own-device (BYOD), service delivery, trusted access, etc.?
- What is the impact of not being able to provide identified technological capabilities to support core systems?

Security objectives

Security objectives support business objectives by mitigating threats and enabling business opportunities within acceptable organisational risk tolerances. By assessing the criticality of business objectives, organisations will be in a position to understand and align associated security objectives.

Questions to consider:

- Would a disruption to the availability of systems affect the achievement of business objectives?
- Does the organisation hold classified data that needs to be protected?
- Are there any external systems that depend on the integrity of the data and services provided by the organisation?
- Does the organisation have a documented risk appetite or risk tolerance?
- Has the organisation historically prioritised resourcing to a particular domain or field of cyber security (protection, detection, recovery, etc.)?
- Does the organisation receive any critical input from services or businesses that are not within organisational control?
- Does the organisation use third-party service providers to implement parts of their cyber security strategy?
- Does the organisation face any contractual, compliance, regulatory, or legislative[1] requirements that may influence security objectives?
- Does the organisation have mandatory reporting requirements?
- What happens if a critical/core function, process or data is affected by a cyber incident?

Example – Business objectives and security objectives

This example identifies a business objective and its supporting security objective. Organisations need to align business and security objectives to ensure security is a complementing outcome. Identifying these complementary objectives will assist organisations in prioritising the MDA Foundations for investment.

Business objective: To increase field-sales revenue by giving sales representatives anywhere-anytime access to the live customer relationship management (CRM) platform on mobile devices.

Security objective: To preserve the confidentiality of customer data, guarantee data integrity for sales made on site, maintain high availability and comply with relevant privacy acts.

MDA Foundation: To provide high-confidence authentication (F2), contextual authorisation (F3), reliable asset inventory (F4), and secure endpoint (F5) to effectively manage and enable remote working, while reducing risk.

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.

Threats and risks

Once an organisation understands their business and security objectives, they can then begin to analyse the threats and risks that can impact these. When an incident or compromise does occur, organisations need to be able to map what the impact will be. Organisations can start by asking the following questions to understand their ability to detect and defend against the threats and risks their objectives face.

Questions to consider:

- Does the organisation maintain a comprehensive cyber security risk register?
- Does the organisation use sector-specific cyber threat intelligence sources?
- Is there regular reporting about cyber threats to the industry sector or similar organisations?
- Has the organisation identified threat sources that are likely to target their organisation or industry?
  - For example, advanced persistent threats (APTs), malicious insiders, third and fourth-party supply-chain attacks.
- Has the organisation mapped attack patterns to see how likely a threat would be to target the organisation?
- Are there previous cyber security incidents that have impacted the organisation?
- What is the organisation's current attack surface?
  - Does the organisation maintain a complete and accurate asset inventory?
  - Does the asset inventory detail allowed resource and asset connections and pathways?
  - Does the organisation have known gaps in visibility or controls?
  - Does the organisation maintain a list of known vulnerabilities that it is susceptible to that need to be risk managed?
  - Has the organisation suffered a past incident that revealed a weakness that has not been adequately addressed?
  - Does the organisation use legacy systems, or any technology or platforms that are no longer supported by the manufacturer?
  - Does the organisation have systems or devices that are not regularly updated and maintained?
  - Can the organisation detect threats in real time and respond?
- What security controls does the organisation currently have in place?

Combining organisational insights with relevant threat intelligence is key to making good cyber decisions. Upon answering the questions above, organisations can consolidate the results to identify areas of significant risk. In turn, this will help organisations to identify which of the MDA Foundations to prioritise and invest in first.

Example – Threat picture

This example uses threat intelligence and organisational risk analysis to identify areas of the organisation that have the highest inherent risk. The organisation can prioritise these areas by identifying and investing in the mitigating MDA Foundation/s.

Threat intelligence shows the organisation is at risk of being targeted by credential theft and social engineering campaigns. Previously, the organisation has dealt with stolen devices, and a third-party supplier has impacted their supply chain.

Currently, there are minimal controls in place to detect and reduce or mitigate the risk of an adversary exploiting these weaknesses.

Threat	Objective	Likelihood	Impact	Residual risk	Current controls
1. Phishing and credential theft	Confidentiality of customer data	High	High	Extreme	Annual security training
2. Lost or stolen devices	Availability and integrity of data and sales systems for mobile workforce	High	Medium	High	Six-digit passcode required
3. Third party breach	Availability of mobile services	Low-Medium	High	Medium	Once-off security onboarding questionnaire for vendors
4. Malicious software or OS zero-day	Integrity of CRM data	Medium	High	Medium-High	Signature based anti-virus agent installed on endpoints

Prioritised MDA Foundations

Initial investment in MDA should focus on leveraging and enhancing existing technologies and reducing attack surfaces. Over the longer term, organisations should work towards achieving uplift across all the MDA Foundations, as combined they provide the most complete outcomes.

Determining which of the MDA Foundations to prioritise will be based on organisational business opportunities and threats to the organisation. In assessing these risks, organisations need to consider the availability and compatibility of their technological capability, current workforce skills, resources, cost, value and outcomes. Once these elements are understood, organisations can create a prioritised roadmap for implementing the MDA Foundations. This will allow them to start their technological analysis for selected MDA Foundations, while looking to the necessary skills required to achieve them – skills that both exist within their current workforce and that must be acquired over time.

Example – Mapping to the MDA Foundations

This example aligns the organisation's prioritised security initiatives to the appropriate MDA Foundations.

Initiative	MDA Foundation	Threats (Table above)	Effort/ Cost	Reasoning
Roll out passkey-based MFA across all mobile channels, including conditional access that blocks phishing fallout.	High confidence authentication	1. Phishing and credential theft	Medium	Removes a large attack vector and is a prerequisite for further security measures.
Implement MDM to do real-time device health attestation. Enforcement of data encryption and remote wipe capability.	Secure endpoint Context authorisation	2. Lost or stolen devices 4. Malicious software or OS zero-day	Medium-High	Directly addresses lost/ stolen device events and establishes data streams for contextual access.
Stand up enterprise asset and Software as a Service inventory.	Reliable asset inventory Reduce attack surface	3. Third party breach 4. Malicious software or OS zero-day	Medium	Foundation for understanding exposure and third-party concerns.

Stage 2 – Identify people and skills

Figure 5. Stage 2

Having the right people with the right skills is critical for implementing the MDA Foundations. The changes MDA will bring to organisational processes and ways of working will require careful consideration. Organisations need to consider how they will acquire and build the required skills, regularly update knowledge of technological solutions, and ensure a clear understanding of business and security objectives.

Organisations will need to determine the knowledge and skills needed to fill gaps that have been identified in their current workforce. To achieve the MDA Foundations outcomes, organisations will require not just individuals, but teams of people working across significantly different technical fields. All teams need to work towards common goals and use a consistent technical language and taxonomy. In doing so, organisations will be better positioned to achieve quality outcomes.

For the successful implementation of the MDA Foundations across an organisation, people and their skills need to be assessed as a business risk and opportunity.

Questions to consider:

- Does the organisation have access to the right people and skills to achieve the identified business and security objectives?
- Does the organisation maintain a record of users and services that can access systems?
- Can the organisation provide or obtain required training and upskilling?
- Does the organisation have the required processes across procurement and change management to support the required technologies and platforms?
- Does current organisational culture help build towards a resilient and modern environment?

Roles and responsibilities

Organisations must consider the technical roles required to successfully implement the MDA Foundations. Skills required for each role will vary and will be unique to the way in which each organisation seeks to implement the MDA Foundations.

The nature of the organisation, the threats it faces and the technology it uses will determine the people required to accomplish business and security objectives and implement the MDA Foundations. Consideration of existing roles and available skills can reduce the need for excessive hiring, and will help identify the gaps that can be filled with a skills uplift or where new capabilities are required.

A comprehensive list of roles and/or teams that may be required to support or implement each MDA Foundation can be found in the Annex – Roles for the MDA Foundations.

Security personnel

Security personnel will support MDA by implementing a shift in security philosophy. They will create and enforce security policies and monitor all activity to proactively identify and mitigate potential risks.

Questions to consider:

- Does the organisation have an up-to-date skills register?
- Are current staff skills adequate to implement priority MDA Foundations?
- Does the organisation have adequate security personnel to maintain current security initiatives and support new ones?
- Does the organisation have a clear upskilling path for identified skill gaps?
- Do team members have experience with any of the required technologies that have been identified?
- Can the organisation translate board-level business objectives into measurable security outcomes?
- Can the organisation show traceability back to the business objectives and security outcomes?

Supporting personnel

Supporting personnel, such as those in procurement and legal areas, support MDA by ensuring the entire organisation is aligned with its principles. Procurement teams, for example, are vital in vetting and selecting vendors and technologies. Legal teams are essential for establishing and enforcing policies that govern data access and privacy, and ensuring the organisation meets its legislative and regulatory requirements[1]

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.

Questions to consider:

- Do procurement personnel have sufficient knowledge of security goals, objectives and supporting requirements?
- Does the organisation have the skills to evaluate proposed technologies?

Executives

Executives provide authority for MDA implementation. They set strategic direction, determine resource allocation, manage risk, and provide oversight of their organisation's cyber security.

Questions to consider:

- Does the executive cohort support security architecture objectives?
- Do employees in the governance area have suitable skills and experience to translate implementation progress through to senior decision-makers?
- Have unique business needs been factored into requirements and associated work plans?
- Does the organisation have sufficient employees to have a security lead dedicated to each priority?
- Is there an approved risk appetite statement or framework that aligns with security objectives?

Employees

Employees are on the front lines of interacting with the organisation's environment. Their role is to actively participate in security by following established protocols, such as being vigilant about phishing attempts, reporting suspected incidents, and understanding the principle of 'least privilege' by only accessing or giving access to data and systems necessary for specific job functions. By consistently interacting with the organisation's systems in a secure and mindful way, they help to reinforce MDA.

Questions to consider:

- Is a security awareness training and education program in place and fit for purpose?
- Do employees have the required understanding to use the new technologies being deployed?
- Can employees perform simple troubleshooting when they are blocked from a certain action and understand the escalation process if the action is business critical?

Customers

Customers play a supportive role in MDA by securely interacting with the organisation's products and services. Customer demand for secure products and services provides a powerful business case for organisations to invest in and reinforce MDA. Meeting these customer expectations is a key driver for market competitiveness and brand trust.

Questions to consider:

- Do customers understand their security requirements for interacting with your organisation?
- Have product testing teams checked with real customers that changes implemented improve trust and usability?
- Are Terms and Conditions (T&Cs) or contractual arrangements updated to reflect an environment that uses modern and emerging technologies?

Example – Roles and teams required

Continuing the example of secure enterprise mobility, this example takes the security initiatives from the previous analysis of the organisation strategy to identify the required roles/teams needed to achieve MDA Foundation goals.

Initiative	Role/Teams involved
Roll out passkey-based MFA across all mobile channels, including conditional access that blocks phishing fallout. (MDA Foundations 2 and 3)	Identity and access management teams, platform engineers, directory services administrators, change and communication leaders, service desk education, legal and procurement teams, field sales staff and education.
Implement MDM to do real-time device health attestation. Enforcement of data encryption and remote wipe capability. (MDA Foundation 5)	Endpoint engineers, architects, mobile security engineers, compliance policy writers, incident responders, network engineers and procurement teams.
Stand-up enterprise asset and Software-as-a-Service (SaaS) inventory. (MDA Foundations 4 and 6)	Asset register owner, API integrators, SaaS governance analysts, data validators, procurement teams, development teams and internal auditors.

Training

Organisations investing in MDA need to prioritise comprehensive training and upskilling for their existing staff. For specific personnel, training will focus on mastering new technologies and tools, while others will support the sustainment or uplift of existing technology. DevSecOps teams need to be upskilled in secure development and deployment practices, learning how to embed zero trust principles directly into their workflows from the start. Crucially, all general employees require clear and consistent training on the 'why' behind the change, focusing on adhering to new security policies and procedures within their role. Organisation-wide training is essential to ensure that every individual understands their responsibilities and actively participates in maintaining the organisation's security posture. Incorporating a dedicated budget for training and upskilling in the investment roadmap is therefore a strategic necessity, as it secures the human element.

Questions to consider:

- Has the organisation identified required training?
- Is the required training available and accessible to the organisation?
- Does the organisation have a budget for the required training?

Stage 3 – Assess technology

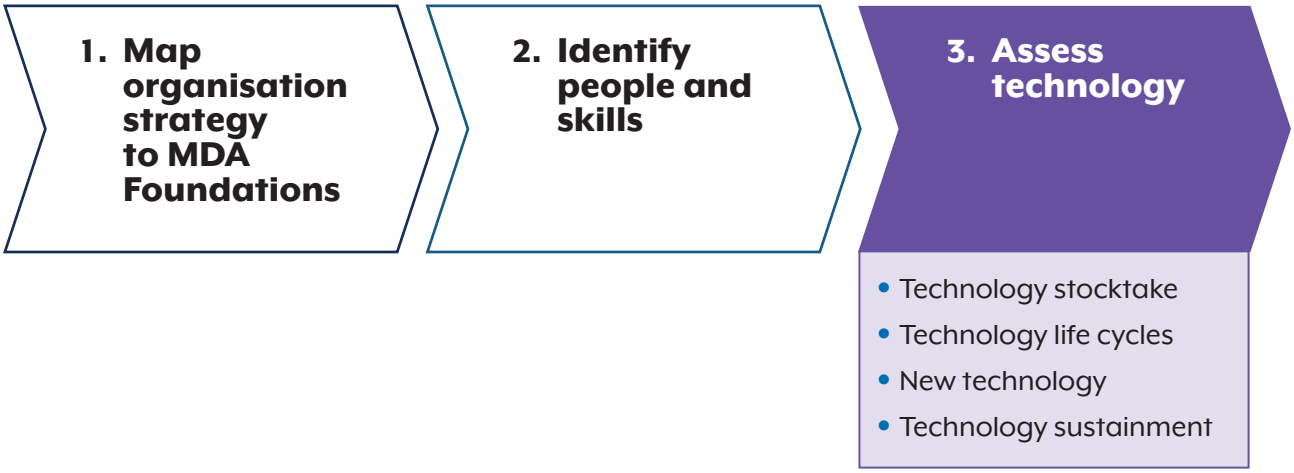


Figure 6. Stage 3

Achieving a mature and secure information environment with MDA requires a strategic approach to technology investment. Organisations building new information environments may find this easier than those with existing ones, which often have significant technical debt. However, this should not deter any organisation, as MDA can be implemented iteratively over time.

The transition to MDA is a strategic journey, not a single project. The biggest challenge for organisations is knowing where to start and what to prioritise. Achieving all the MDA Foundations immediately will not be feasible; implementation requires a phased approach with multiple discrete projects integrated into the organisation's cyber security roadmap. Technology choices must be strategic, building towards business and security objectives without creating unmanageable burdens.

To navigate this journey, organisations should focus on 4 key areas for technology uplift:

- **Stocktake of current technology:** Organisations need to have a clear understanding of their existing technologies and capabilities that support their business and security objectives and prioritised MDA Foundations.
- **Evaluate technology life cycles:** Organisations need to consider the life cycles of their current technologies and those they plan to procure to ensure long-term compatibility and sustainability.
- **Analyse new technology impact:** Organisations need to analyse the potential impact of new technologies. While new solutions offer benefits, they can also introduce risks, such as compatibility and management complexities that must be addressed proactively.
- **Develop technology sustainment plans:** Organisations need to ensure the personnel capabilities within their organisation can support and sustain both existing technology and any new technology implemented.

Technology stocktake

Organisations need to complete a stocktake of their current technology assets and capabilities. Assessing these capabilities against current and future business and security objectives will assist in analysing capability gaps. It will also support decision-making as organisations work towards implementing the prioritised MDA Foundations.

Questions to consider:

- Do the organisation's current technology capabilities meet current and future security objectives?
- Does the organisation have complete visibility of all assets including cloud, hardware and software?
- Are the current technologies capable of fully or partially achieving MDA Foundation security objectives?
- Do the current technology manufacturers have a roadmap of changes that may add to an organisation's capability to support their transition to new technologies and platforms?
- What risks do current technologies pose to the organisation if they are kept or replaced?

Example – Technology current state

This example shows an organisation's current technology state. Without this, an organisation will not be able to make a properly informed decision on where to invest in new technology or technology uplift to support the prioritised MDA Foundations.

Initiative[2]	Capability/ Data point	Current state	Key takeaway vs security objective
1	Enterprise identity provider	Three separate on-premises directories + SaaS 'Shadow identity provider' for HR.	No single source of truth, users joining, moving or leaving takes weeks to action.
1	MFA in use	82% password only, 15% SMS codes, 3% hardware tokens.	Most authentication method are susceptible to phishing, help-desk resets via phone, with a high volume of callers.
2	Endpoint / Mobile management	Legacy MDM covers 40% of phones, laptops are unmanaged once signed out.	Users free-install anything; no baseline enforcement.

2 The initiatives in this example refer to the initiatives contained in 'Example - Roles and teams required' on page 19.

Initiative[2]	Capability/ Data point	Current state	Key takeaway vs security objective
2	Device health attestation	Not supported by current tooling. Policy has been planned but not actioned.	Every device is seen as compliant, outdated and compromised devices are granted full production access.
2	Remote wipe capability	Manual wipe via email request, average delay is 3 business days.	Lost devices have an unacceptable data exposure window.
3	Discovery and correlation engine	None, interns and junior staff hand-merge CSVs.	Asset duplicates rampant and shadow IT assets are not visible.
3	Inventory of company devices and cloud services	Asset list claims to track everything but lists fewer than 1 in 3 devices and only 1 in 5 cloud services.	List is updated by hand once a month with spreadsheets, no duplication checking occurs. Decommissioned devices are not removed from the list.

Technology life cycles

Organisations need to build the transition to MDA into their organisation's technology refresh cycles. It will likely not be feasible to transition an organisation to a fully compatible information environment in a single project unless the organisation is building a complete greenfield environment. Thus, organisations should seek to integrate implementation into their standard technology refresh cycles. Organisations should identify and prioritise areas of high risk by understanding vendor enhancements, vendor support lifetimes and technology refresh intervals.

Questions to consider:

- What are the life cycles of the organisation's current technologies?
- What technologies in the organisation's environment are nearing end of life?
- What legacy systems cannot be effectively enhanced to achieve modern security practices during their lifetime?

New technology

Organisations will at some point need to invest in new technologies to continue their journey towards business and security objectives, and the MDA Foundations. Organisations must ensure that the risks of new technologies never exceed their risk thresholds, even if they support or achieve business and security objectives.

Questions to consider:

- What technology is needed to meet the organisation's future security objectives and prioritised MDA Foundations?
- What are the compatibility risks and requirements between current technologies and proposed technologies?
- Has the organisation identified any risks in proposed technologies that do not meet the organisation's risk thresholds?
- Does the new technology meet both business and security objectives?

Example – Technology life cycles

This example analyses current organisational technology life cycles and how they support business and security objectives. The aim is to understand where the current technology life cycle is up to, how it supports the organisation's transition to MDA, and which MDA Foundation/s each technology covers.

Legacy assets	Vendor support status and age	Lifecycle stage	Vs security objective	Vs business goals	Security action
On-premises directories	OS build last patched 5 years ago, vendor providing extended security updates.	End stage	Current solution cannot issue modern authentication tokens.	Users joining, moving or leaving takes weeks and slows onboarding.	Migrate to a primary identity provider before decommissioning.
Password + SMS MFA	Control gap, not technology age.	SMS MFA deployment stalled	Most authentication methods are susceptible to phishing.	Rising help-desk password resets, risk of breach above appetite.	Enforce MFA, pilot phishing resistant.

Legacy assets	Vendor support status and age	Lifecycle stage	Vs security objective	Vs business goals	Security action
Legacy on-premises MDM application, covers 40% phones	Firmware is frozen and no security patches in 12 months.	End of support	No enforceable baseline, no API for confidence/ health signals.	Lost devices will leak data.	Block network access until devices are enrolled.
Device health attestation	Tooling incapable.	Never implement-ed	Manipulated devices look 'clean'.	Executives locked out when travelling.	Enable hardware-backed attestation.
Discovery / correlation engine	Internal, manual.	Never implement-ed	Duplicates and shadow assets are not identified .	Unable to identify and respond to breaches.	Pilot agentless discovery tooling.

Procurement

When procuring new technologies, it is important that organisations follow advice on *Choosing Secure and Verifiable Technologies* balanced with the requirements needed to achieve their goals.

Questions to consider:

- Have the chosen products been verified in a way that meets the organisation's risk appetite?
- Do the organisation's procurement plans include resourcing, training and ongoing support?
- Do proposed vendors provide training and security documentation?
- Is a relevant technical staff member involved in the procurement process?
- Will procured solutions integrate with current platforms, or will they require further integration?
- Are there documented requirements, including skills, attached to each procurement decision?

Technology sustainment

While building towards business and security objectives, and the MDA Foundations, organisations need to ensure that the personnel capabilities can support and sustain both existing technology and any new technology implemented. As part of their business impact assessment, organisations need to analyse, firstly, the risks to the organisation if new or existing technology cannot be supported or maintained due to skills shortages; and secondly, how these risks will impact the organisation's ability to achieve the MDA Foundations.

Workloads

Organisations will need to have the capabilities to manage existing and new workloads that support the prioritised MDA Foundations.

Questions to consider:

- Does the organisation have the internal skills required to deploy and maintain the technology?
- Are there critical technologies in the organisation's environment that only one or 2 staff understand?
- Are any defensive tools being underused due to a lack of training or available skills?

Management and support

To enable technology sustainment, organisations will need to create sustainment and management plans for both existing and new technologies.

Questions to consider:

- Does the organisation have a sustainment plan for existing technology?
- Does the organisation have a sustainability plan for new technology?
- Does the organisation have a backup plan or succession planning if key staff are unavailable?
- Who in the organisation is responsible for the day-to-day management of the technology?
- Does the technology require ongoing training or support from third parties?
- Does the organisation have the expertise to maintain the technology, including patching and updates to configurations to stay aligned with the MDA Foundations?

Example – Capability mapping to procurement, sustainment and skills risks

This example is for organisations to map technology capabilities to the skills required to maintain and successfully use each capability. The output of mapping analysis should feed into the investment strategy to ensure gaps in current skill sets can be properly resourced.

Capability	Procurement	Sustainment	Skill risks
Unified enterprise identity provider	Licences and migration playbooks. Require knowledge transfer sessions for directory engineers. Require training sessions with vendor for architects.	Schema-drift review by an in-house trained Identity and Access Management (IAM) lead. Certification track for 2 junior engineers per year, ongoing licensing fees, 24 x 7 escalation route to vendor support.	If architects leave before juniors are certified, there is a risk of being locked into expensive vendor engagement to support every change.
Phishing resistant MFA	SDK licences, end-user adoption toolkit to communicate and train field team, UX consulting for staff with disabilities, appropriate licensing or hardware.	Social engineering training, ongoing licensing or hardware as required.	Adoption can stall if users find the MFA too difficult. Ongoing user usage and troubleshooting education is required.
Unified endpoint management (UEM)	Licensing for user devices, and for platform administrator certification.	Baseline owner role in an endpoint management team, quarterly policy tuning, lab devices to test OS updates and set new baselines.	Staff need to stay aware of latest endpoint changes to set relevant compliance and baseline rules.
Agentless asset discovery platform	Subscription/license, training for SOC analysts and others undertaking asset discovery.	Data quality champion, monthly health check-ins, annual training budget for new SaaS adapters.	Lack of skilled users can reduce data quality, break feeds, increase duplications.
Configuration management database (CMDB)	Flexible data model selected, with vendor training for configuration managers. If available vendors to deliver workflow templates for attestation.	Regular CMDB accuracy auditing, integration with discovery tooling and health alerts as new data streams become available.	Loss of skills are likely to cause reversion to spreadsheet culture.
Remote wipe automation	API documents, PowerShell or API training for automation engineer.	Lost device tabletop exercise and playbook. BYOD policy with risk education for users.	Automated scripts maintained by a single developer can break or become outdated if they leave.

Annex

Roles for the MDA Foundations

Each MDA Foundation affects different layers of an organisation. While each organisation will have a different structure, the following is a list of roles or teams that an organisation may require to successfully implement each MDA Foundation. Organisations should consider investing in these resources for each prioritised MDA Foundation.

Role/team	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
Enterprise Architect	x	x	x	x			x	x	x	
Cyber Security Architect	x	x	x	x	x	x	x	x	x	x
ICAM Specialist	x	x	x							
MFA Specialist		x	x							
PKI Administrator	x	x								
Endpoint Security Engineer					x	x				
Mobile Device Management (MDM) Specialist					x					
Network Security Architect						x	x			
Asset Administrator	x			x						
DevSecOps Engineer								x		
Application Security Engineer								x		
Vulnerability Management Analyst						x				x
SOC Analyst										x
Compliance and Risk Officer	x	x	x	x					x	x

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

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