



Australian Government
Australian Signals Directorate

cyber.gov.au

Implementation planning guide

Essentials

Contents

Purpose	3
Audience	4
Planning considerations	4
Securing executive commitment	5
The need for change	5
Structuring the business case	6
Anticipating executive questions	7
Reporting commitments	8
Scoping domain assets	9
Start with operating context	9
Defining the environment through the six technical domains	9
Non-production environments	10
Functions, not business units	10
Limiting scoping activities	12
A workshop method for scoping	12
Scoping the two capability domains	13
Conducting a gap analysis	14
Method	14
Inputs	15
Outputs	15
Planning implementation	16
Phase sequencing	16
Delivery approaches	16

Prioritising with the ATT&CK mapping	17
Deliver and measure	18
Designing controls	19
Indicators of good practice	20
Build the evidence repository with the program	21
Operational evidence of effectiveness	21
Sustainment planning and reusable patterns	22
Design as reusable patterns	22
Establish the reassessment cadence	24
Manage exceptions as a lifecycle	24
Resource the steady state	24
Assembling the implementation strategy	25
Planning checklist	26

Purpose

This guide is a supplemental publication as part of the Essentials series. It helps organisations turn those requirements into an implementation strategy by providing practical guidance for securing executive commitment, defining implementation scope, identifying gaps, planning and delivering remediation, preparing for assessment and sustaining cyber security outcomes over time.

The ASD Essentials framework describes cyber security outcomes through principles, the actions required to achieve them and the domains where those actions apply. Each ASD Essentials series chapter applies the framework to a specific technology environment and uses priority phases to provide a recommended sequence for implementing its technical domains.

Figure 1 shows how these planning activities work together to support implementation and sustainment.

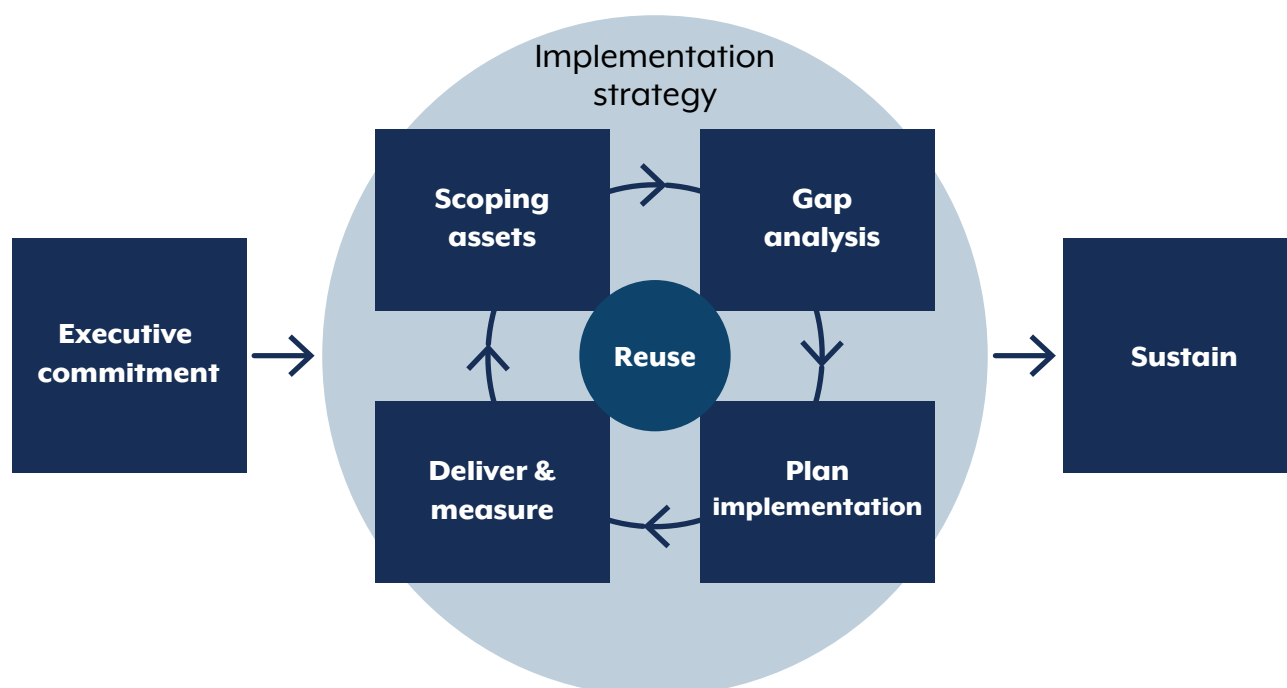


Figure 1. Implementation roadmap

This guide should be read alongside the relevant ASD Essentials series chapter for the environment, such as the *ASD Essentials for enterprise IT* chapter. The Assessment process guide provides further guidance on assessing implementation and reporting cyber security posture. Organisations transitioning from the Essential Eight should also refer to *Transitioning from the Essential Eight*.

Examples in this guide use the *ASD Essentials for enterprise IT* to demonstrate how the planning approach can be applied in practice. However, this guide can be used to inform implementation for any of the Essential series chapters.

Audience

This guide is written for security architects, cyber security program leads, chief information security officers and other roles responsible for the implementation program.

Planning considerations

Plan around ASD's recommended priority phases, not implementation of the whole chapter at once. Priority phases enable organisations to take an organised and targeted approach to implementing an ASD Essentials series chapter without planning every phase in detail at the outset. A credible implementation strategy should define the scope, costs and delivery approach for the priority phase 1 domains, while treating subsequent phases as forward plans to be refined using lessons learned.

Design for assessment from day one. ASD Essentials assessments focus on control effectiveness, not deployment alone. Organisations should establish mechanisms for ongoing assurance, monitoring and documentation as controls are implemented, providing visibility that controls remain in place and continue to operate effectively over time. Incorporating these activities during implementation is typically less resource-intensive than attempting to reconstruct evidence during an assessment. Attempting to do so later often results in avoidable rework.

Design capabilities once as patterns. Many capabilities that implement the actions apply across multiple domains. Organisations should design them as repeatable patterns and progressively apply them in priority phase order, reducing duplicated effort and creating economies of scale across the chapter.

Securing executive commitment

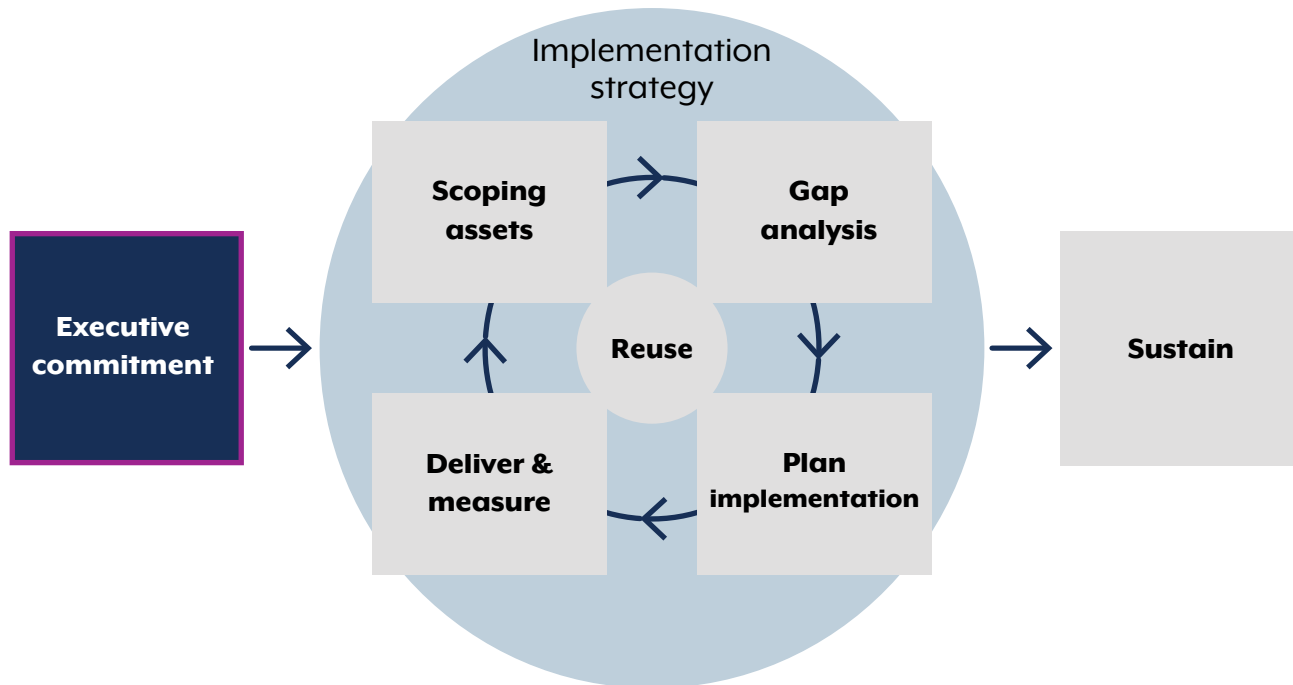


Figure 2. Executive commitment

The ASD Essentials framework makes the executive role explicit. Under the **Executive cyber security accountability principle** within the framework, the board of directors or executive committee is accountable for cyber security, including setting, monitoring and adjusting organisational risk tolerance and appetite. Under the **Security risk management assurance principle**, risk management activities are subject to ongoing monitoring and assurance. The same executive body also monitors and assures the **Cyber security resourcing principle**, which requires that suitable and sufficient personnel and resources must be identified, acquired and maintained.

Executive commitment is now assessable content within the Governance and culture domain, and the framework requires sustained executive engagement to enable effective security outcomes for the organisation.

For further information about executive commitment, refer to *The Essentials for senior executives*.

The need for change

Executives who have funded an Essential Eight program will reasonably ask why further investment is required. The case for change rests on three points drawn from the design of the framework:

- **Australia's threat environment has changed which shifts the cyber security risks and likely targets.** While the Essential Eight maturity levels reflected increasing levels of adversary targeting, highly capable adversaries now pose a credible threat to a broader range of organisations. The Essentials series therefore applies sophisticated adversary tradecraft threat modelling across all principles, actions and chapters.

Comprehensive principle coverage across all domains is the target for every organisation, with implementation paced and prioritised according to organisational capability, resourcing and risk.

- **Existing investment is carried forward.** Every Essential Eight mitigation strategy maps to at least one cyber security principle. A program implementing an ASD Essentials series chapter redirects and extends prior investment rather than replacing it. Previous investments in other cyber security frameworks are also considered in the Essentials assessment methodology, allowing organisations to reuse appropriate evidence to support Essentials reporting.
- **The framework is built to show measurable progress early.** Early priority phases focus effort on domains where actions disrupt commonly observed tradecraft, achieving meaningful risk reduction within a contained scope of work and building the operational practices needed in later phases.

Structuring the business case

A business case aligned to the structure of the applicable ASD Essentials series chapter is easier to defend than one built on a bespoke narrative, because every element traces to something the executive can later see reported. ASD suggests structuring the investment ask in project tranches that mirror the priority phases.

Table 1 provides an example of how an organisation securing its enterprise IT environment could structure project tranches to align with the priority phases in Essentials for enterprise IT.

Table 1: Example project tranches aligned to priority phases

Tranche	Scope	What the executive is buying
Tranche 1	Boundary services and Identity services, plus establishment of Governance and culture and Visibility and response	Disruption of the most common entry and escalation paths; the governance, detection and assessment capabilities every later phase depends on
Tranche 2	Critical processes and services and Privileged environments capability domains extended	Hardening of the highest-consequence assets and the elevated access pathways used to administer them
Tranche 3	Business systems and User devices capability domains at full enterprise coverage	Coverage of the remaining enterprise environment, constraining what an adversary can do from any foothold

Costing within each tranche should distinguish:

- capability build (tooling, licensing, engineering)
- operating uplift (the ongoing people and process cost)
- assessment (internal assessment effort plus periodic independent assessment)

Identifying sustainment costs from the outset helps prevent controls from degrading because of insufficient operational funding. This is particularly important because the framework's reassessment cadence will identify controls that are not maintained effectively.

Decision-makers should be told early that the shape of the investment changes across tranches, not just its size. Capability build investment declines as patterns established early, such as logging, baselines and authentication, are reapplied rather than redesigned. Operating uplift grows as each tranche hands more of the environments into sustainment. Assessments stay broadly steady, since each tranche bring a comparable set of domains into scope.

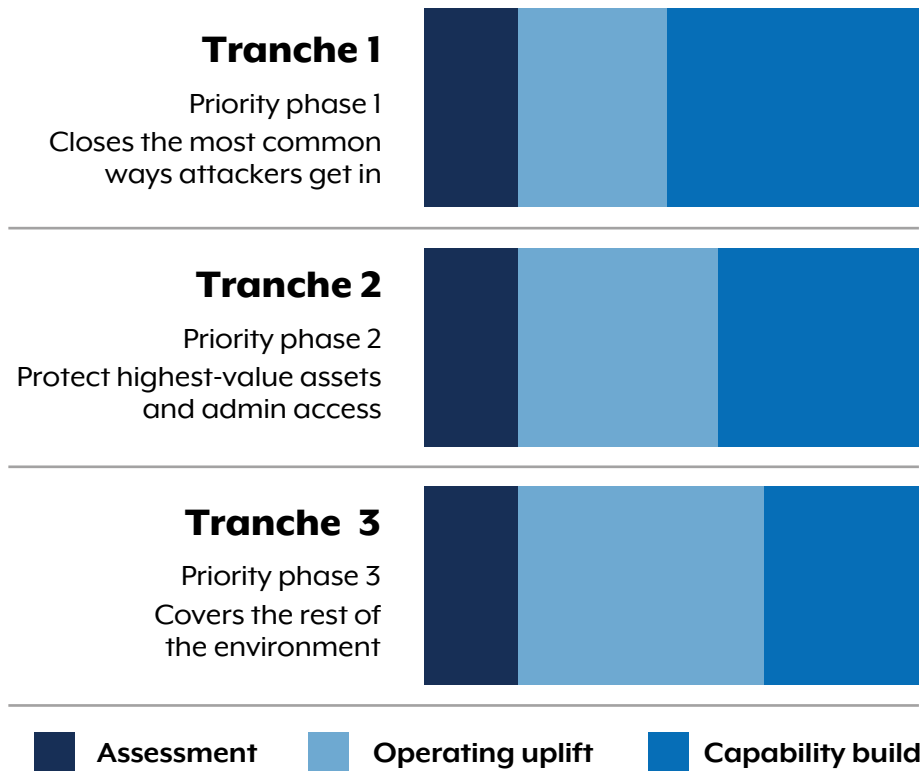


Figure 3. Three-tranche investment bars

Anticipating executive questions

Table 2 provides framework aligned responses to common executive questions about implementation, investment and reporting.

Table 2: Framework aligned responses to common executive questions

Common questions	Response grounded in the framework
Why can we not remain at our current maturity level?	Maturity levels are no longer defined as implementation targets and do not correspond directly to the priority phases. The evolved framework expects all organisations to progress through each phase, with coverage of the cyber security principles across all domains representing the intended end state. The priority phases are therefore interim stages of progression, not levels at which an organisation should remain indefinitely.

Common questions	Response grounded in the framework
Does completing a priority phase tell us we are secure?	No. Priority phases provide an implementation sequence, not a measure of security, compliance or maturity against a particular adversary. Assurance is based on the effectiveness ratings of the cyber security principles within each domain. The reporting format therefore presents principle ratings rather than assigning an overall level.
When will we be finished?	Cyber security implementation does not have a definitive completion date. Once the organisation has progressed through the priority phases of the applicable chapter, it should transition to an ongoing sustainment model that maintains, reassesses and refines controls in response to changes in threats, organisational operations and the framework. The business case should distinguish between the implementation program end date and the ongoing sustainment run rate.
How will we know the investment worked?	Through a standardised assessment posture report: counts of principles rated fully effective , partially effective , not effective and not assessed per domain, with percentage progression over time, alongside the detail view of specific gaps and remediation. Charting successive assessments shows where investment has improved the organisation's cyber security posture.
What if we cannot fund all tranches now?	Early priority phases are designed to show measurable progress within a realistic timeframe and to develop the practices later phases need. A decision to defer implementation of a priority phase should be guided by risk to the organisation and documented accordingly; ASD do not recommend skipping domains or deferring priority phases indefinitely.

Reporting commitments

Agreeing the reporting requirements with the executive at program initiation avoids later disputes about progress. ASD recommends committing to the following:

- the standard reporting format organised by priority phase and domain
- a domain-level radar view for board reporting overlaid across successive assessments
- the accompanying detail view of principles rated **partially effective** or **not effective** with remediation activity, so that visible progress is not used to obscure outstanding risks
- honest use of **not assessed** as a neutral status for domains not yet addressed, distinguished from **not effective** in all reporting.

Scoping domain assets

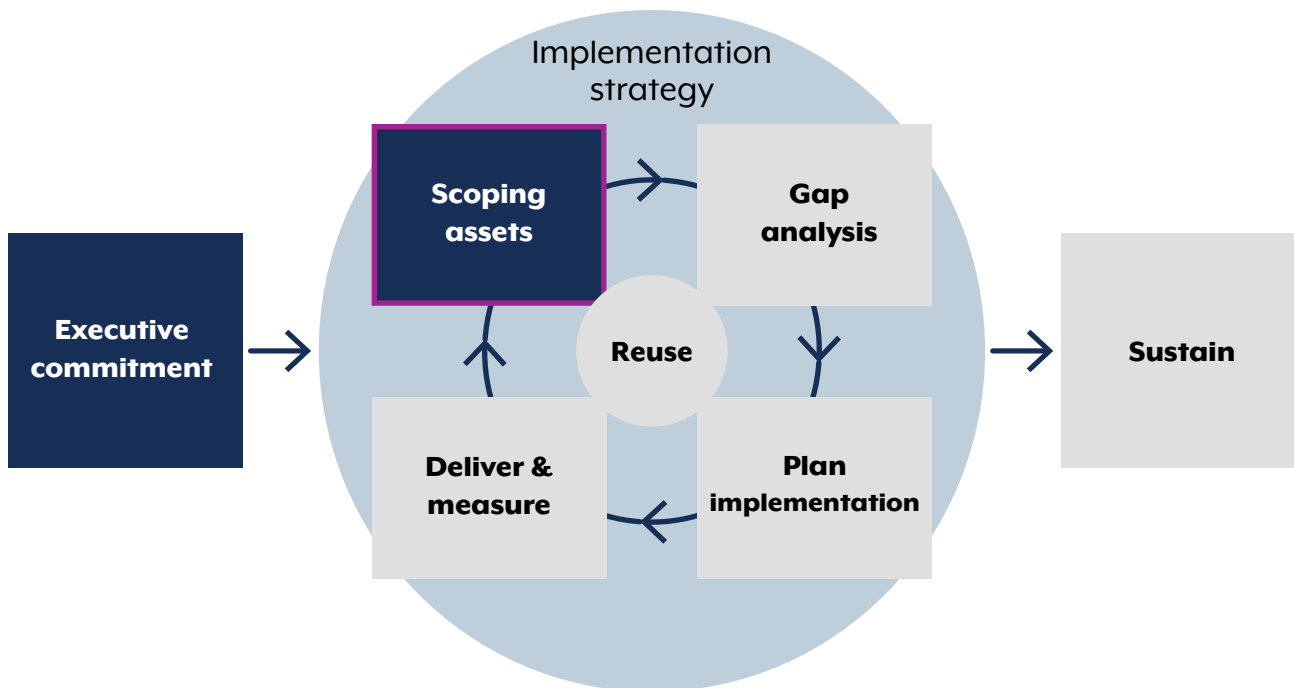


Figure 4. Scoping assets

Scoping translates the applicable chapter's broad domains into named systems and assets that engineers can harden and assessors can examine. It is a critical planning activity because the scope statement establishes what constitutes coverage for each subsequent effectiveness rating. As the domain definitions are intentionally broad to accommodate diverse IT environments, each organisation is responsible for making, documenting and justifying its scoping decisions.

Start with operating context

Before mapping assets, record the organisation's operating context, including regulatory obligations, international partnerships, stakeholder expectations, risk tolerance and appetite and the resources and funds available for cyber uplift. Operating context informs scoping decisions, such as whether an interagency connection is included within the *Boundary services scope* or which *processes qualify as critical within the Critical processes and services domain*.

Defining the environment through the six technical domains

A domain is a logical grouping of business functions and the critical assets that support them, where those functions and assets share similar risks. The six technical domains divide an organisation's technology environment according to the functions it performs, rather than according to specific technologies or organisational structures. Together, the domains provide a comprehensive view of the functions technology performs across an organisation's digital systems.

Defining the environment supports planning for the implementation of the priority phases within the chapter, and the subsequent measurement under the ASD Essentials framework. Grouping assets

by function and consequence of compromise enables the priority phases to target the functions most likely to be attacked first and supports consistent interpretation of domain effectiveness ratings across organisations.

The practical test for placing an asset is not who owns or operates it, but what role it performs. Table 3 provides questions to help determine the technical domain in which an asset should be scoped, based on the role it performs.

Table 3: Questions to determine an asset's technical domain

Technical domain	Questions about asset role
Boundary services	Does it broker connectivity or data flows across a boundary between environments?
Identity services	Does it anchor decisions about who and what to trust through authentication, authorisation or identity lifecycle functions?
Critical process and services	Does it directly deliver a primary organisational outcome or contribute to the health or safety of personnel or the community?
Privileged environments	Does it enable, broker or govern elevated control over other systems?
Business systems	Does it support day-to-day operations without being individually critical?
End user devices	Does it provide the general workforce with direct access to the environment?

Non-production environments

When mapping assets, include non-production environments such as development, testing and staging. Assign these environments to domains on the same basis as other assets, considering their function, connectivity, data, privileges and potential impact on production. Where a non-production environment holds production trust or administrative access, can connect to production, or can modify or deploy production systems, apply protections equivalent to those of the production environment it can affect.

Functions, not business units

Organisations with divisional structures may try to map domains onto the organisational chart – treating a subsidiary, division or brand as a domain. This does not reflect the framework model. Domains decompose an environment by function, not by business structure. An organisational unit may constitute an environment rather than a domain, encompassing functions and supporting assets across multiple domains.

Example: A parent organisation with two businesses (Enterprise IT).

A parent organisation operates two distinct businesses. Neither business is a domain. Each business's IT environment decomposes into six technical domains in its own right: each is likely to have its own boundary systems, its own identity and authentication arrangements, its own critical processes, privileged access pathways, supporting business systems and workforce devices. The parent therefore scopes the domains per environment, unless a function is genuinely shared.

Where the businesses share a function – such as a common identity tenancy, consolidated internet gateway or a shared security operations capability – scope the shared function once. Its scope statement should span both environments and record the consuming environments. Shared functions typically carry a higher consequence of compromise because they span environments, and this should be reflected when prioritising within a priority phase.

Apply the following approach when scoping and reporting across multiple environments:

1. Scope each domain separately within each environment and scope each shared function once.
2. Apply the priority phase sequence within each environment.
3. Report posture for each environment with a consolidated view for the parent organisation.

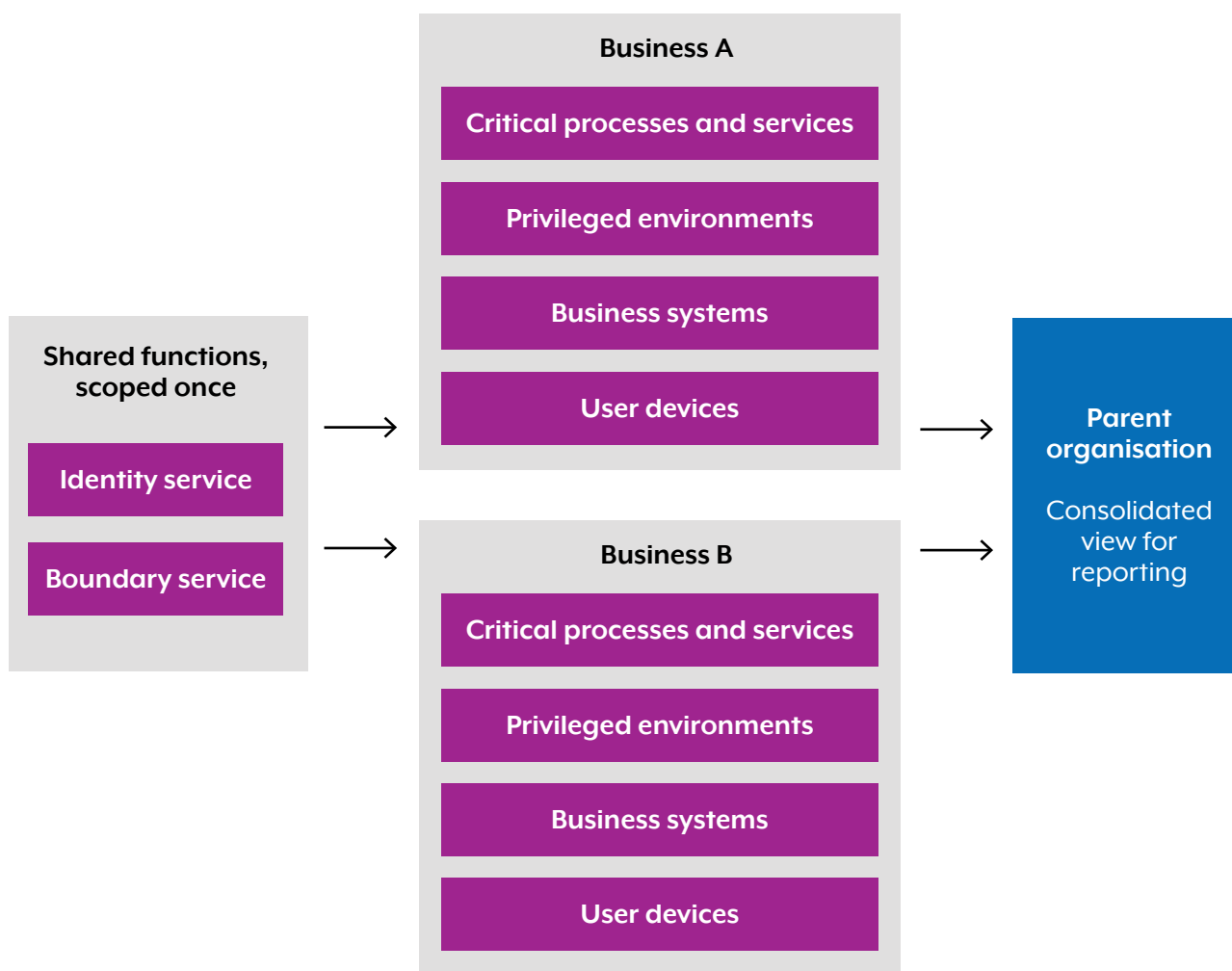


Figure 5. Parent organisation decomposition

When reporting across multiple environments, consolidation should not mask domain weaknesses within any individual environment. If business units are subject to different risk profiles or regulatory obligations, each environment should maintain its own operating context and implementation priorities.

Limiting scoping activities

Scoping is not a comprehensive enterprise-wide asset discovery activity. Under the recommended implementation sequence, organisations initially scope only the domains within priority phase 1. Additional domains are scoped in later phases, informed by lessons learned. This staged approach reduces upfront effort and maintains a proportionate planning burden. Figure 5 shows the four asset categories used as a starting point for scoping.



Figure 6. Asset types for scoping

As a starting point, identify assets within each scoped domain across six categories: infrastructure, operating systems, applications, identities, credentials and data. Not every domain may contain significant assets in every category. Draw on existing asset inventories, system registers, business impact assessments and architecture documentation. Where significant gaps in asset visibility are identified, record them for resolution when addressing the relevant domains. The Visibility and response domain includes actions designed to support automated asset discovery and inventory, so imperfect visibility is a finding to record rather than a barrier to starting.

A workshop method for scoping

A repeatable method keeps scoping decisions consistent and produces the documentation required for gap analysis and assessment. For each domain:

1. Assemble the evidence base

Example evidence sources include configuration management database extracts, network and identity architecture diagrams, the business impact assessment, internet-facing service registers and cloud tenancy inventories.

2. Identify candidate assets within each asset category

For the **Identity services domain** in an enterprise IT environment, examples may include:

- **Infrastructure.** Domain controllers, federation servers and supporting network segments.

- **Operating systems.** Server instances underpinning directory and federation services.
- **Applications.** Directory services, federation platforms, directory synchronisation tools and certificate authorities.
- **Identities.** User, privileged, service, shared, emergency and machine accounts, including associated roles, permissions, group memberships and identity attributes.
- **Credentials.** Passwords, passphrases, cryptographic keys, certificates, authentication tokens and other credential material used to authenticate users, services and system.
- **Data.** Directory databases, user and group objects, credential material, authentication tokens, federation trust metadata, access policies and audit logs.

3. Test assets against the domain definition and consequence of compromise

If compromising the asset would result in the consequence defined for that domain, it is in scope. Record each inclusion and exclusion decision with a brief rationale. Exclusions are particularly important as they help assessors and future reviews understand the scope boundaries.

4. Resolve multi-domain assets

Assets and functions that operate across multiple domains should be documented against each relevant domain. Apply the actions from the earliest applicable priority phase first and add later phase actions as implementation progresses. For example, an internet-facing customer application in an enterprise IT environment may be addressed under Boundary services in priority phase 1 and Critical processes and services in priority phase 2.

5. Baseline the scope statement

Issue a version-controlled scope statement for each domain that lists in-scope assets by category, exclusions with rationale, multi-domain assets and identified visibility gaps.

Scoping the two capability domains

Governance and culture and **Visibility and response** are scoped differently because their assets are largely programs and artefacts rather than digital systems. Governance and culture includes cyber security strategies, policies and procedures, awareness and training programs, security roadmaps and risk registers.

Visibility and response includes asset registers, incident response plans and procedures, and detection and response platforms. Scope both domains early, with the expectation that their scope will expand as additional technical domains come into scope. The scope statement for each domain should record its intended growth through future priority phases.

Conducting a gap analysis

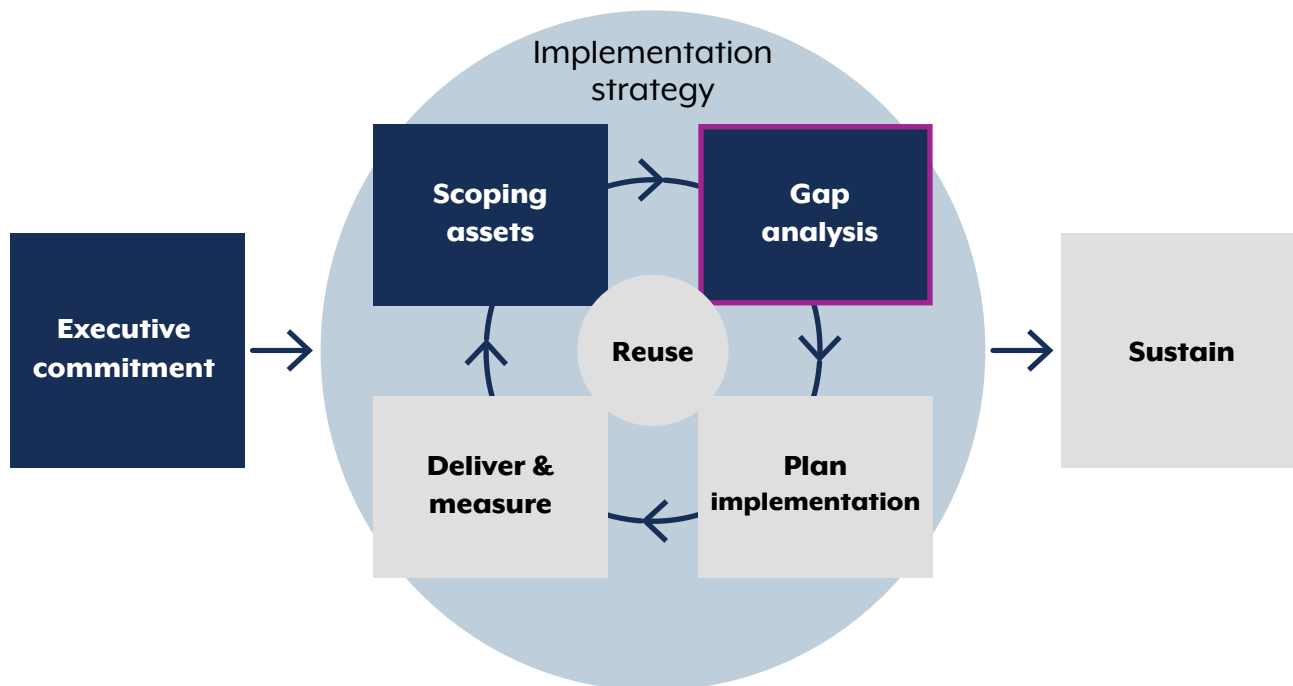


Figure 7. Gap analysis

Scoping establishes which assets are included within each domain. Gap analysis then determines whether existing controls address the applicable actions for those assets, identifies deficiencies and defines the implementation work that remains. These findings inform the sequencing, resourcing and reporting decisions described throughout the remainder of this guide.

The purpose of a gap analysis is not to assign formal effectiveness ratings. For implementation planning purposes, each action is classified as addressed, partially addressed or not addressed. Effectiveness ratings are assigned later, when the available evidence can be evaluated through the assessment process.

Method

Organisations should conduct the gap analysis on a domain-by-domain basis. For each domain within scope for the current implementation cycle, identify the applicable principles and review the associated actions against existing capabilities.

For each action, organisations should determine whether:

- **The action is addressed by existing controls.** No implementation work is identified at this stage. Document the existing controls and available evidence so their effectiveness can be assessed later.
- **The action is partially addressed by existing controls.** Existing controls address some, but not all, of the action or known gaps in scope, consistency or enforcement. Document the gaps in sufficient detail to inform implementation planning.
- **The action is not addressed by existing controls.** No existing control addresses the intent of the action. Record the new work that must be planned and resourced.

Findings should be recorded against each applicable domain rather than against the action alone. The same action may be addressed at one domain and absent at another, and this distinction informs both the sequencing of remediation and subsequent measurement.

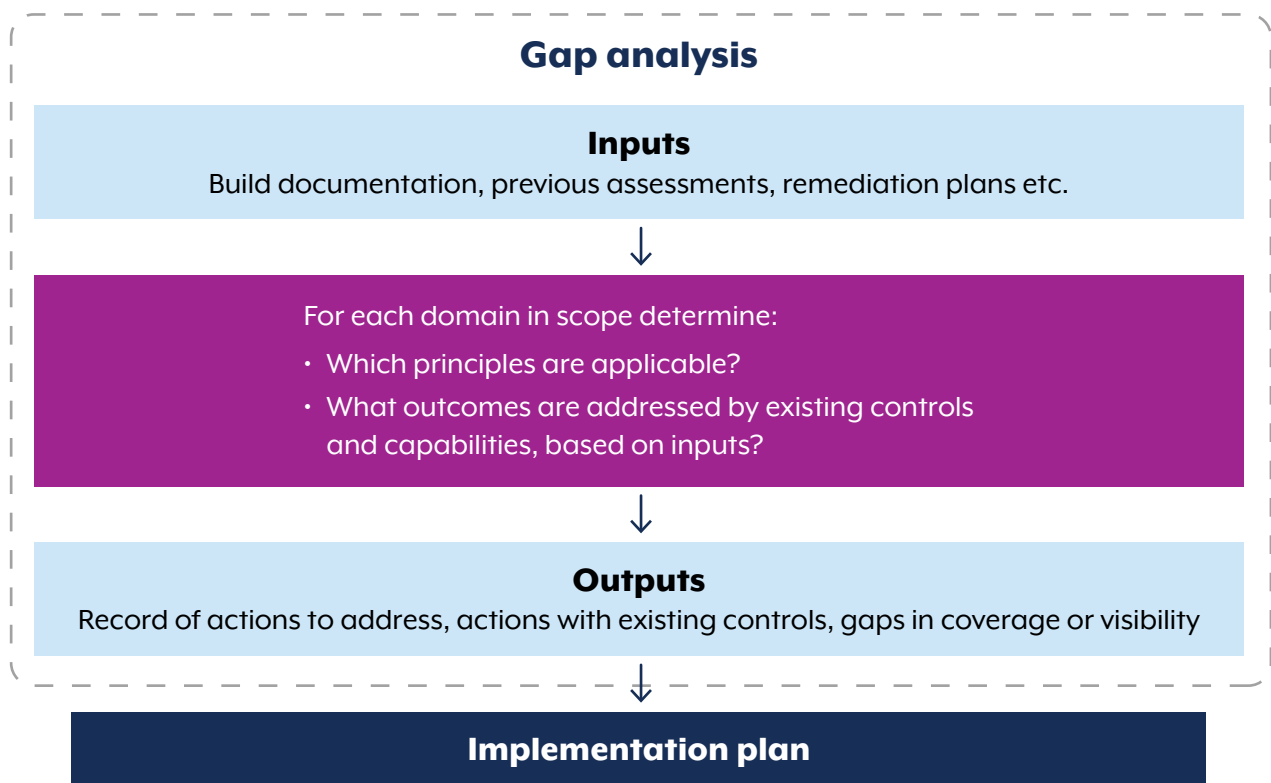


Figure 8. Gap analysis flow

Inputs

Existing documentation continues to provide value where it remains current and accurate. Relevant sources may include previous assessment reports, system and configuration documentation, logging architecture documentation, exception registers and remediation plans. Organisations transitioning from the Essential Eight should refer to Transitioning from the Essential Eight, which identifies where existing investments are recognised within the ASD Essentials framework and where additional strengthening may be required.

The validity of any carried-over evidence should be verified before it is relied upon. A review that is no longer current, an exception that has expired without re-approval, or a configuration baseline that no longer reflects the operational environment should each be treated as a finding.

Outputs

A completed gap analysis provides the information needed to plan implementation. This includes a record of applicable actions and findings for each domain, evidence of actions already satisfied by existing controls, and sufficient detail on coverage gaps to support scoping, sequencing and resourcing decisions.

Deficiencies in asset visibility should also be recorded. As the Visibility and response domain includes actions that improve asset discovery and inventory capabilities, such deficiencies should be addressed through the framework rather than regarded as a barrier to implementation.

Planning implementation

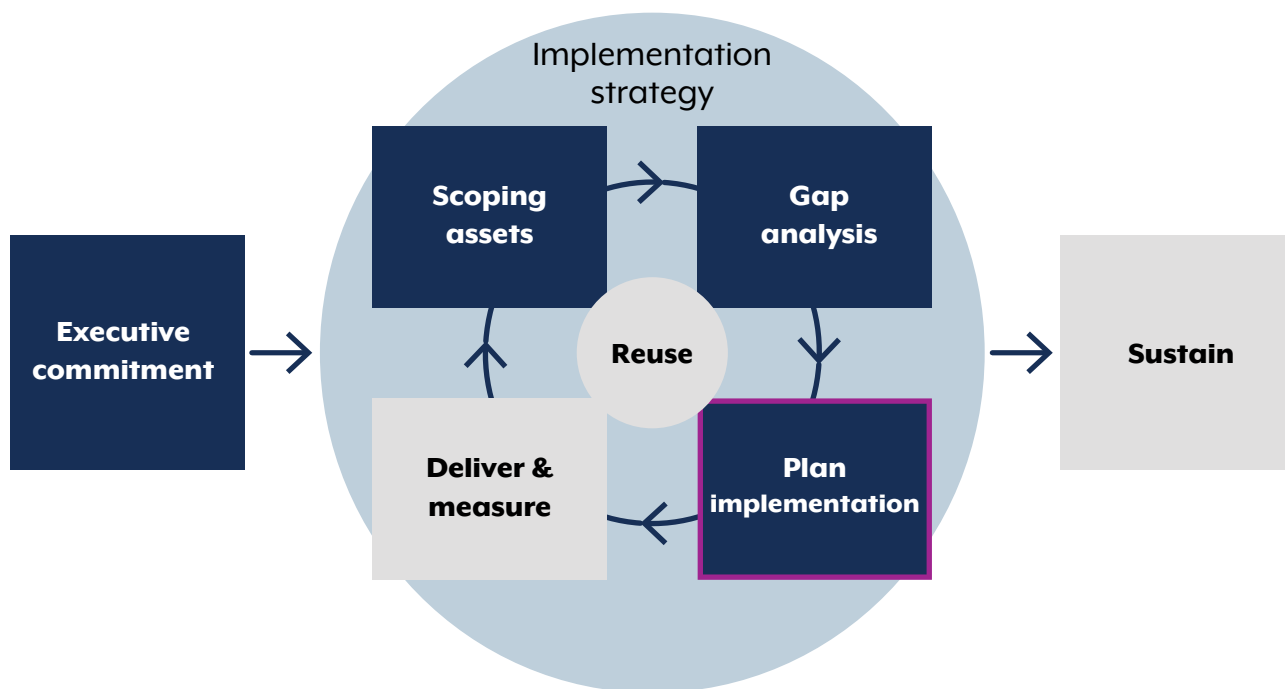


Figure 9. Planning implementation

With domains scoped and gaps identified, the plan must decide what to fund, in what order and through which delivery approach. This guide combines the priority phase sequence, with two delivery approaches and the MITRE ATT&CK mapping to support a defensible investment order.

Phase sequencing

Priority phases define the recommended order for addressing domains, based on ASD threat intelligence, common control gaps and implementation opportunities. It is recommended that an earlier phase's domains are addressed before a subsequent phase's domains; the phases should be followed in sequence because each phase builds on the capabilities established in the preceding one.

Organisations with specific cyber threat intelligence or regulatory drivers may adjust the recommended phasing of domains, but the provided sequence represents ASD's recommended approach, and any departure should be a documented, risk-based decision.

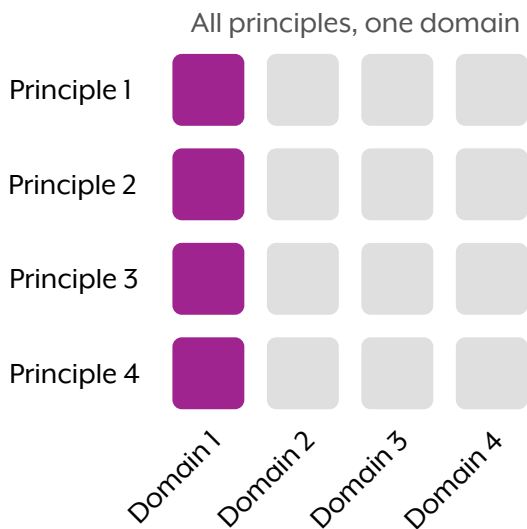
Delivery approaches

This guide describes two ways organisations can structure delivery, a domain-focused approach takes one domain and applies all the applicable principles before moving to the next, producing clear, demonstrable outcomes against a defined scope. A principle-focused approach takes one principle and applies it across multiple domains in priority phase order, giving more consistent coverage and better value from enterprise-wide tooling and licensing.

Domain-focus is the recommended default for organisations early in their journey, or without the internal capability to weigh the trade-offs confidently. Established programs may choose either, or combine both, as their operating context warrants.

Option 1: Domain-focus

One domain at a time



Option 2: Principle-focus

One principle at a time

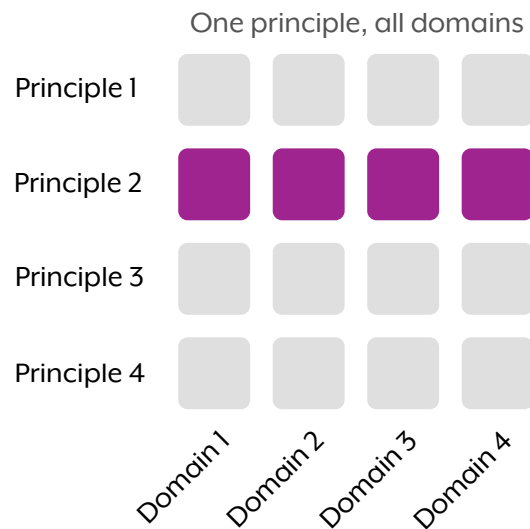


Figure 10. Planning focus options

Procurement and licensing strategy

The delivery approach may also have commercial implications that organisations should consider when planning implementation activities. For example, a domain-focused rollout may better align investment with project tranches and budget cycles, while a principle-focused rollout may, in some circumstances, support enterprise-wide procurement approaches or operational efficiencies at scale.

The right approach depends on the organisation's procurement arrangements, licensing models, funding preferences, risk appetite and confidence in the proposed solutions. As this guide is focused on security outcomes rather than commercial decision-making, organisations should apply their own procurement, financial and governance processes when determining the most appropriate approach. Different approaches may be appropriate for different controls within the same program.

Prioritising with the ATT&CK mapping

Within a priority phase, the applicable chapter's MITRE ATT&CK mapping supports threat-informed prioritisation. The recommended method includes:

- identifying the threat groups, campaigns and techniques most relevant to the organisation's environment, drawing on ASD threat advisories, sector-specific and commercial and open-source cyber threat intelligence
- identifying the techniques most consistently observed against the sector
- using the mapping to find the actions that contribute most directly to mitigating those techniques.

This threat-informed approach is intended for organisations with sufficient maturity to obtain, interpret and apply threat intelligence. Less mature organisations are not expected to use it and may prioritise actions based on their operating context, risks and available resources.

Where a small number of techniques account for a large share of the threat, the actions mapped to them become priority candidates for early investment. The same logic can inform remediation urgency for partially effective ratings. A gap relating to techniques commonly observed in an organisation's threat context may warrant earlier remediation than one relating to rarely observed behaviours and tradecraft.

The mapping informs prioritisation within a priority phase, not across phases, and it carries the following limitations:

- The ATT&CK knowledge base evolves continuously.
- The mapping is necessarily generalised.
- Threat intelligence is itself, imperfect.

It should inform prioritisation alongside, not in place of, the broader risk management process.

Deliver and measure

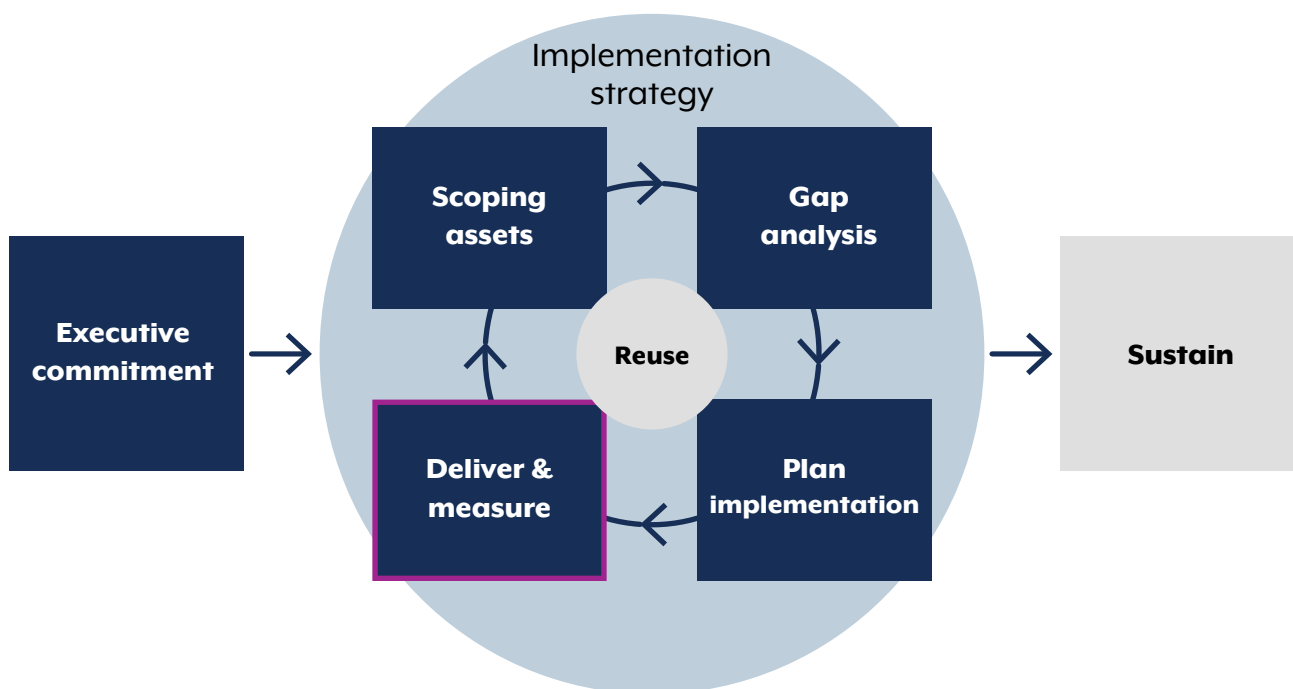


Figure 11. Deliver & measure

The Essentials series rates each action against each applicable domain on a four-tier scale. A **fully effective** rating requires the intended security outcome to be achieved consistently, with supporting evidence.

Designing controls

Assessment examines four assessment dimensions to ensure effectiveness: coverage, consistency, currency and evidence quality. Programs that treat these as considerations only at assessment time incur additional effort to demonstrate control effectiveness. In contrast, programs that design controls so these attributes are observable from deployment generate evidence as a by-product of normal operation.

Table 4 shows how each assessment dimension can be considered during control design and the evidence that can be generated during operation.

Table 4: Designing for the assessment dimensions

Dimension	Design question at build time	Evidence generated in operation
Coverage	Can all assets within the domain's defined scope be identified, and can unmanaged or missed assets be detected?	Coverage reports reconciled against the version-controlled scope statement, with discovery alerts for unmanaged assets.
Consistency	Is the control deployed from a single approved definition (for example, a baseline, ruleset, or policy-as-code) rather than configured individually on each asset?	Version-controlled baselines or rulesets with approval records, supported by drift detection reports and remediation evidence.
Currency	How is the control kept aligned with the environment and threat landscape, and who is accountable for its review?	Scheduled review and revalidation records, plus an exception register containing approved, time-bound exceptions and expiry dates.
Evidence quality	How will reliable evidence of control operation be collected, protected and retained, using automation where supported and proportionate?	Centralised logs of control decisions (allowed/blocked, granted/denied), operational dashboards, and validation test results mapped to ATT&CK techniques.

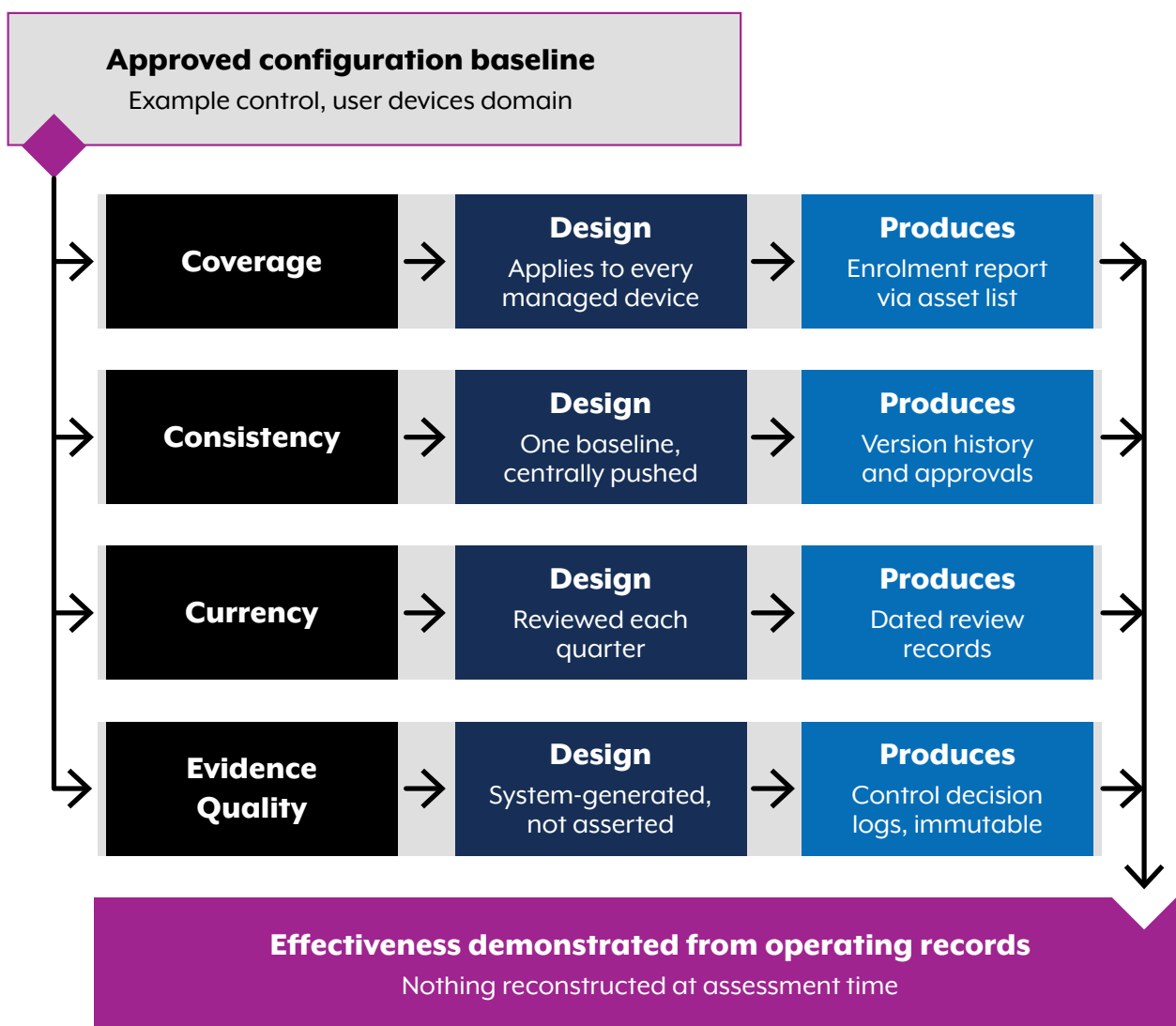


Figure 12. Control design dimensions - example

Indicators of good practice

The assessment process guide encourages the use of the indicators of good practice (IGPs), which provide measurable statements for determining a current self-assessed effectiveness rating of **not effective**, **partially effective** and **effective** ratings. This rating is distinct from the actions current implementation status which may be recorded during the gap analysis. Organisations should record the effectiveness rating and implementation status in separate fields or columns within the assessment register.

The presence of any single not effective statement is normally sufficient to justify a not effective rating. A partially effective rating requires evidence that the action delivers specific worthwhile security benefits, rather than evidence of partial activity alone.

The IGP statements consistently require defined review cycles, documented approvals, timely completion and reassessment following organisational change. To prepare, organisations should ensure every control is subject to scheduled review, supported by documented approval and accompanied by a remediation plan for known deficiencies.

Build the evidence repository with the program

During the gap analysis, organisations are expected to document how existing controls satisfy each action, even where no remediation is required. This information should be maintained as part of a per-domain evidence register that maps each applicable action to its control implementation, scope coverage, evidence sources and current self-assessed rating. Structured in this way, the register serves as the primary working paper for self-assessment, the evidence package for independent assessment and the supporting detail for security posture reporting.

Independent assessors bring a fresh perspective and judgement, helping to identify gaps and weaknesses that may have become accepted through familiarity. Where proportionate and affordable, organisations may choose to engage an independent assessor, but this is not required. Maintaining a comprehensive evidence register will enable assessors to concentrate on evaluating control effectiveness, rather than undertaking time-consuming document discovery and evidence collection.

Operational evidence of effectiveness

Deployment evidence alone is insufficient to support or maintain an **effective** rating. Organisations should establish a validation program that generates operational evidence that aligns with the intent and criticality of each action and be obtained using validation methods proportionate to the organisation's available capability and resources. Methods may include control validation testing, penetration testing, red team exercises, purple team activities, and breach and attack simulation; however, these advanced methods may not be required for every action

The ATT&CK mapping can be used to design and scope these activities by targeting the techniques each action is intended to mitigate. For example, an action addressing trustworthy software may be validated by attempting to execute unsigned binaries or unapproved interpreters, providing evidence that the control operates effectively in practice rather than merely being deployed.

For organisations with sufficient cyber security maturity and capability, the mapping can inform detection engineering by identifying techniques that are material to the organisation and assessing whether suitable telemetry and detection coverage exist. This does not require a separate detection rule for every preventive action or mapped technique. Validation activities should be proportionate to the priority, criticality and available capability, and scheduled after remediation where assurance is required before ratings are used in reporting.

Sustainment planning and reusable patterns

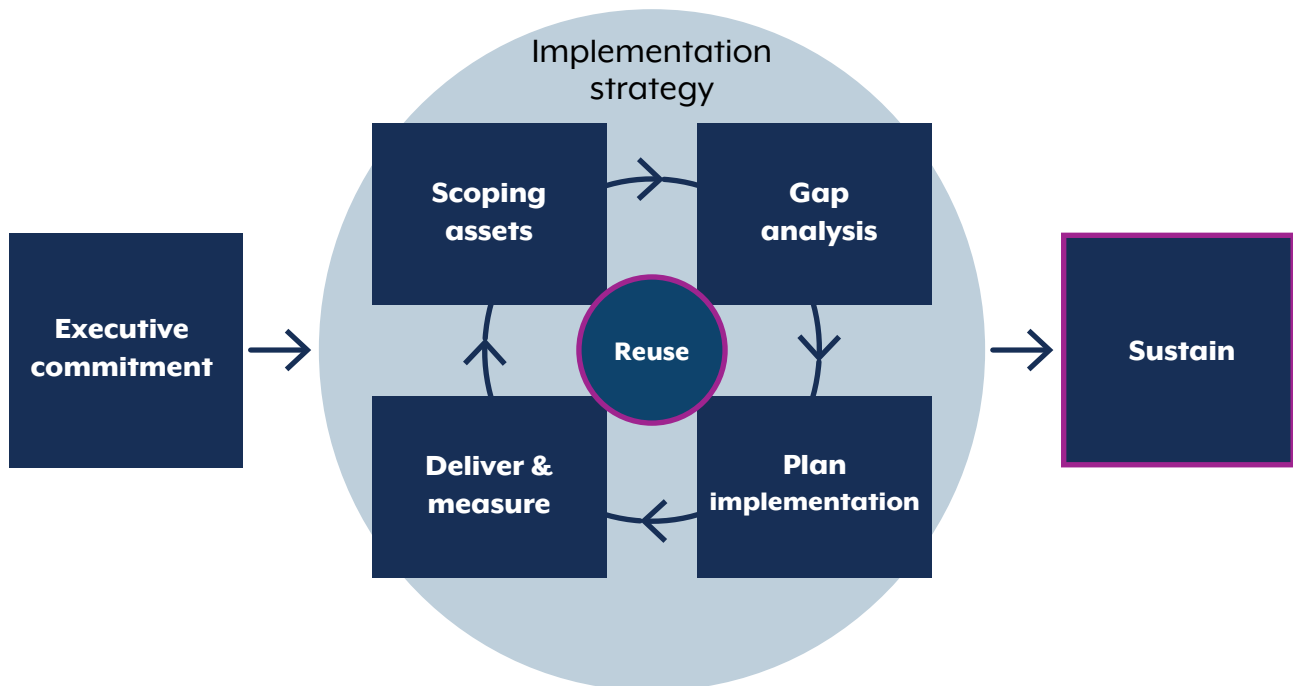


Figure 13. Sustain & reuse

Organisations are expected to maintain, reassess and refine controls in each domain on an ongoing basis as the threat environment, the operating context and the framework itself evolve. A sustainable end state is one where all applicable actions have been addressed across the domains the required principles are operating effectively and the organisation has the governance, resourcing and operational capability to maintain that posture. Sustainment is therefore a planned deliverable of the program, not what happens after it.

Design as reusable patterns

Organisations are encouraged to build cross-cutting capabilities as documented, repeatable patterns rather than as domain-specific projects. The best pattern candidates are the actions that apply across multiple domains within the chapter, including, multi-factor authentication, configuration baseline definition and drift detection, centralised event logging, vulnerability management and backup architecture.

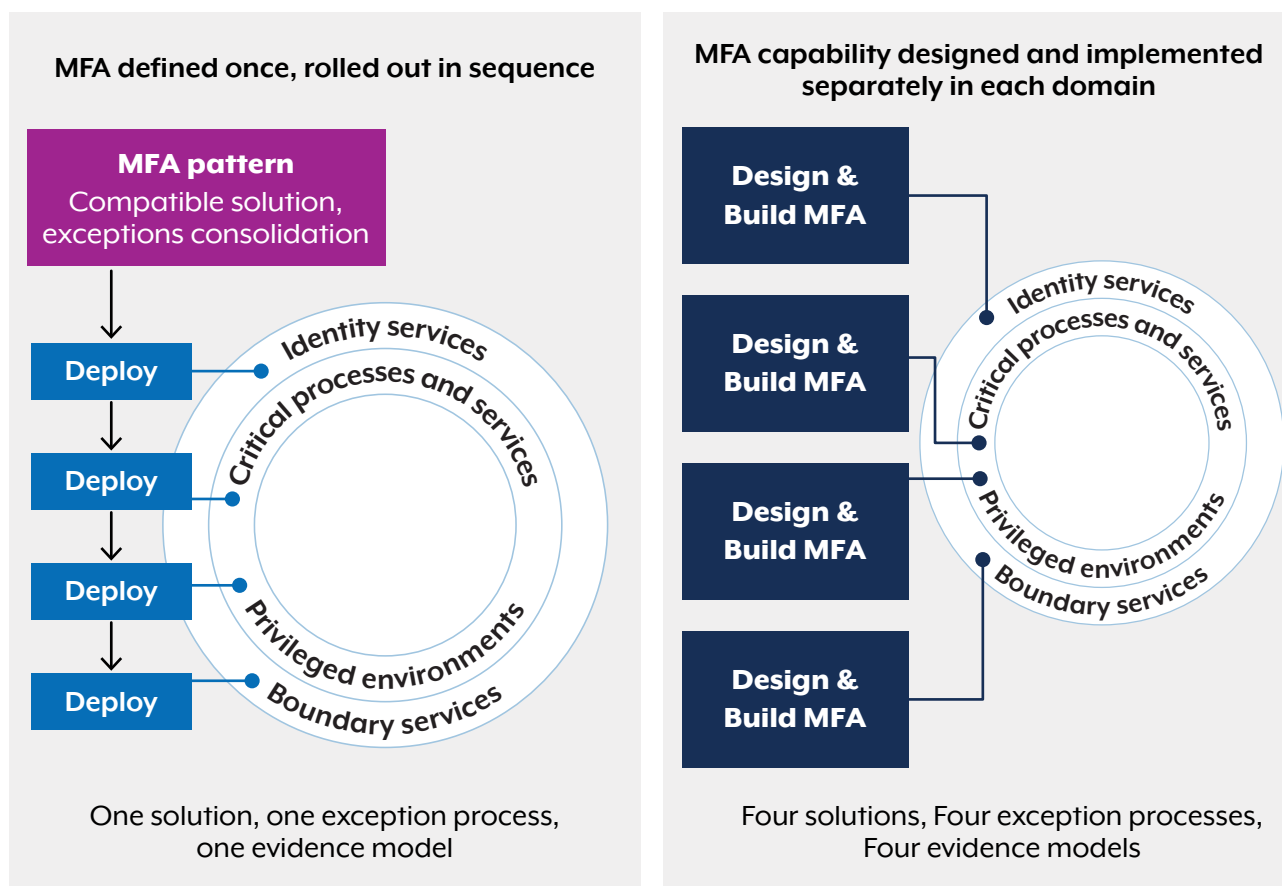


Figure 14. Reusable patterns

A pattern is worth documenting once it captures sufficient detail to make subsequent implementations consistent, repeatable and less costly. A useful pattern should record the following details.

- **Intent.** The cyber security principles and actions the pattern supports, and the adversary techniques and tradecraft it is intended to mitigate.
- **Applicability.** The domains to which the pattern applies, aligned to priority phases, including any domain-specific tailoring. For example, domains with a higher consequence of failure may require stricter baselines or accelerated patching timeframes.
- **Solution.** The technology-agnostic design, approved configuration baseline, and integration points with capability domains, including logging requirements and associated governance artefacts.
- **Evidence model.** How the pattern demonstrates coverage, consistency and currency and where operational evidence is generated and retained. This ensures each implementation is instrumented for assessment from the outset.

Patterns provide a further benefit during reassessment. When framework requirements or the threat environment change, updating and redeploying a single pattern is significantly more efficient than rediscovering how the capability has been implemented across multiple domains.

Establish the reassessment cadence

Establish a regular, risk-based cadence for reassessing domains against the applicable principles and actions. Bring a reassessment forward following material changes to the IT environment, threat environment, organisational priorities, or following a relevant cyber security incident.

Where reassessment identifies an action previously rated effective has degraded, document the gap and initiate remediation through the same gap-analysis-to-implementation process used during the program. The measurement model is designed to be applied identically at each reassessment. Include periodic independent assessment in the cadence, particularly where external assurance is required, to strengthen the credibility of posture reporting to regulators and governing bodies.

Manage exceptions as a lifecycle

Exceptions, compensating controls and accepted risks are common sources of security posture degradation. Each should be reviewed as part of every reassessment. An exception that has expired without review, a compensating control that no longer operates effectively, or an accepted risk that has not been reconsidered against the current threat environment may indicate an opportunity either to close the gap or to formally re-approve the residual risk.

To support this process, organisations should establish and maintain an exception register from the outset. At a minimum, the register should record named owners, approval details, review requirements and expiry dates. Maintaining a current register ensures reassessments can draw on an authoritative source of record rather than requiring exceptions, compensating controls and accepted risks to be identified and reconstructed retrospectively.

Resource the steady state

The Cyber Security Resourcing principle requires organisations to periodically review cyber security resourcing in response to changes in the threat environment, incident outcomes and organisational priorities. Sustainment resourcing should be planned on a capability-pattern basis rather than by individual domain. Estimate the initial and ongoing cost of each pattern, including:

- licences and subscription
- integration
- data ingestion and retention
- workforce
- training
- baseline reviews
- drift remediation
- detection tuning
- validation activities
- evidence maintenance.

Apply that cost across all implementing domains to establish a defensible steady-state funding requirement. This supports the horizon-based budgeting approach described in [Structuring the business case](#).

Governance sustainment should be planned and tracked using the same approach. Activities such as accountability reviews following organisational change, maintenance of reporting cadences, and verification of training currency should be recorded within the relevant governance registers and managed through the Governance and culture domain. Consolidating both technical and governance sustainment obligations in this manner improves accountability, supports reassessment activities and provides a clearer view of ongoing resource requirements.

Assembling the implementation strategy

When actioned as intended, the preceding sections produce a set of artefacts that, when combined, form the implementation roadmap. Table 5 brings the planning activities together into an indicative program structure and identifies the artefacts each stage should produce.

Table 5: Indicative implementation strategy

Stage	Key activities	Artefacts produced
Executive commitment	Record the operating context, brief executives, agree investment tranches and the reporting model, and establish program governance.	Executive briefing and business case; agreed reporting format and cadence; program governance terms of reference.
Scoping assets	Define the domains included in the first priority phase using the method in A workshop method for scoping .	Version-controlled scope statements for each domain, including exclusions, multi-domain assets and identified visibility gaps.
Gap analysis	Assess applicable principles and actions against existing capabilities and classify each action as addressed, partially addressed or not addressed.	Gap register; initial evidence register documenting how existing controls satisfy applicable actions.
Plan implementation	Categorise gaps as domain-focused or principle-focused, apply ATT&CK-informed prioritisation within the priority phase, determine the delivery approach for each capability, and identify reusable pattern candidates.	Remediation registers with owners and delivery approaches; procurement strategy; pattern backlog.
Deliver and measure	Implement remediation activities, design controls with the assessment dimensions in mind, conduct validation activities and assess each action against the rating model.	Pattern documentation; validation results; posture report, including remediation plans for partially effective ratings.
Progress	Repeat the scope, analyse and deliver cycle for each priority phase, extending capability domains and reapplying established patterns where appropriate.	Updated scope statements, posture reports and pattern versions for each priority phase.

Stage	Key activities	Artefacts produced
Sustain and reuse	Establish the reassessment cycle, including independent assessment, manage exceptions and accepted risks, and review resourcing against threat trends, incidents and organisational change.	Reassessment schedule; maintained exception register; sustainment resourcing plan.

The framework does not prescribe implementation timeframes. Organisations are expected to progress through the priority phases at a pace that reflects their capability, available resources and risk environment. The key requirement is that the implementation strategy clearly defines the sequence of work and the artefacts to be produced at each phase. These artefacts provide the foundation for assessment, posture reporting and ongoing sustainment.

Planning checklist

Before finalising the implementation strategy confirm that:

- executive accountabilities are formally defined, with the agreed reporting arrangements and risk appetite set and assessable under **Governance and culture**
- operating context was documented before scoping decisions were made
- versioned scope statements exist for every domain in the current cycle, including exclusions with rationale and multi-domain assets
- every remediation item is tagged with a delivery approach, its domains in priority phase order, and an owner
- prioritisation within the current level is threat-informed via the ATT&CK mapping, and any departure from the recommended domain sequence is a documented risk-based decision
- every control has a defined risk-based review cadence, approval records, drift or coverage monitoring and an entry in the evidence register
- validation exercises are scheduled for each priority phase and mapped to the techniques the actions are intended to mitigate
- cross-cutting capabilities are documented as patterns with intent, applicability, solution and evidence model

**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>

