



Australian Government
Australian Signals Directorate

cyber.gov.au

ASD Essentials overview

Frequently asked questions

 Essentials

Frequently Asked Questions

Strategic direction and rationale

What is the Essentials Series?

- The ASD Essentials series is a principles-based cyber security framework that provides organisations with a consistent approach to cyber security across different technology environments.
- The Essentials series provides prioritised advice for organisations, with specific guidance for [enterprise](#), [cloud](#) and [operational technology](#) (OT), recognising that different environments required tailored approaches.
- The Essentials series has strong emphasis on risk-informed decision-making, supported by threat intelligence and organisational context.
- Further information can be found in the [What is the Essentials](#) publication.

Why is ASD replacing the Essential Eight?

- As demonstrated in the Annual Cyber Threat Report 2024-2025, the cyber threat landscape has evolved, with Australian organisations facing increasingly sophisticated threats. Modern enterprise environments are more complex, spanning on-premises, hybrid-cloud and emerging technologies.
- The Essentials series adopts a threat-informed, principles-based approach that is better suited to diverse environments, providing flexibility for organisations to implement controls that achieve security outcomes, without being tied to specific technologies.
- The Essentials series focuses on building sustainable cyber security capabilities that can adapt as threats and technologies change.
- Further information can be found in [The case for change](#) publication.

How will the Essentials series differ from the Essential Eight?

- The Essentials series will move from a maturity levels to phased priorities, allowing organisations to prioritise effort against the highest-risk assets.
- The Essentials series transitions from a list of strategies and prescriptive security requirements that should be implemented, to principles and actions that help organisations assess whether intended security outcomes are being achieved.
- The Essentials series introduces cyber security principles, actions and domains, and empowers organisations to focus security uplift efforts on critical business functions and systems.

Who is the Essentials series for?

- The Essentials series is written primarily for Commonwealth entities, critical infrastructure owners and operators, and large organisations.
- Small and medium sized businesses that do not operate at the scale of enterprise IT can still use this guidance where relevant. The security outcomes described by the principles within the Essential series are equally important for smaller organisations.
- ASD publishes tailored cyber security guidance for small businesses, home offices and individuals at cyber.gov.au.

Why is the Essentials series transitioning from prescriptive controls to a principles-based approach?

- Adopting a principles-based approach to cyber security provides organisations with the flexibility to implement controls in a manner that achieves desired security outcomes.
- The Essentials series provides organisations the opportunity to leverage additional frameworks that are relevant to their operational context when addressing the principles.

What is the transition timeline?

- ASD has been communicating with regulatory bodies around the impact and expected timeframes of transitioning to the new framework and will advise on expectations for transitioning to the new framework in due course.

What is the roadmap for future development of the Essentials?

- ASD will continue to consult and engage with organisations as part of ongoing development of the series and will publish future guidance to assist organisations with their adoption of the Essentials.
- ASD will publish a strategy document outlining the path for future work for the Essentials.
- As technology evolves, ASD will publish considerations relevant to the Essentials framework. ASD's AI considerations for the Essentials will assist organisations in the current environment.

What changes were made to the Essentials series in response to the consultation paper feedback?

- The consultation paper was open for feedback from the 15 June to 12 July 2026. Feedback was received from a broad spectrum of organisations during this period.
- Upon review of the feedback received, ASD made several changes to adapt the Essentials to the themes that were raised as part of the consultation. Some, but not all, of the changes that were made in context of the feedback include:
 - Terminology changes to clarify the concepts presented within the Essentials series.
 - A series of overview publications to help guide newcomers consuming the Essentials for the first time.
 - Increased messaging to assist and inform the executive cohort on the intent and impact of the Essentials series.
 - Increased guidance for scoping systems to the Domains.
 - Guidance on how AI should be considered in the context of the Essentials series.

Components of the Essentials

What are the core components of the new framework?

- The Essentials series introduces several new concepts that articulate the what, how and where to apply security initiatives to strengthen cyber security for organisations.
- At a high level, the Essentials series introduces:
 - **Principles** that describe the cyber security outcomes an organisation should achieve.
 - **Actions** that describe what needs to be done to achieve those outcomes.
 - **Domains** that describe the business functions and assets to which the actions apply.
- The Essentials series outlines **priority phases**, which is the recommended order that the Domains are addressed, reflecting where effort delivers the greatest and most rapid reduction in risk.
- More information can be found in the [What is the Essentials](#) guidance.

How does the Essentials align with ISO 27001, NIST and ISM?

- The Essentials series has been developed with flexibility and compatibility in mind; The Essentials series enables organisations to choose approaches suited to their environment, while aligning with other recognised cyber security frameworks such as ASD's [Information Security Manual](#) (ISM).
- The [Assessment evidence guide for enterprise IT](#) contains references to controls from other frameworks that may serve as evidence of action effectiveness if they have been adopted and implemented by the organisation.

Transition from the Essential Eight

How can organisations prepare for the transition?

- Organisations can start preparing for transition to the Essentials by establishing a transition baseline. Organisations should start by understanding and recording their cyber security posture, informed by their Essential Eight maturity, existing controls, risk assessment results and key business functions.
- Organisations can then undertake scoping activities to identify assets and functions relevant to the priority phase one domains - boundary services, identity services, governance and culture and visibility and response.
- Further advice can be found in [Transitioning from the Essential Eight](#) guidance.

What happens to existing Essential Eight investments?

- Efforts already completed under Essential Eight remain relevant and will directly support alignment with the Essentials series. Organisations currently using the Essential Eight will find that many of their current tools and platforms naturally map into the new framework, while new adopters will benefit from the broad experience and maturity the community has built over time.

Should organisations continue investing in Essential Eight uplift programs?

- ASD does not recommend slowing or stopping the roll-out of pre-approved cyber security initiatives that will uplift an organisations security posture. Organisations should continue their current uplift programs, while assessing alignment with the new framework.
- For major, multi-year investments, ASD has provided guidance to assist organisations to move to the new Essentials framework, including [transition](#), [implementation](#) and [assessment](#) guidance.

How does the Essential Eight map to the Essentials?

- Every Essential Eight mitigation strategy maps to at least one principle in the Essentials series, and in most cases, controls implemented under the Essential Eight will directly satisfy, or substantially contribute to, a corresponding action underneath the principle.
- Further guidance on how Essential Eight investment applies to the Essentials is available within the [transition](#) guidance.

What happens to existing Essential Eight maturity status?

- The Essentials series and the Essential Eight maturity model measure different things; the Essential Eight maturity model measured implementation of specific controls, while the Essentials series measures whether outcome-based actions are effective for the assets within each specific domain.
- The Essentials introduces priority phases that sequence activities across the capability and technical domains.
- Maturity level ratings under the Essential Eight maturity model do not automatically convert into effectiveness outcomes under the Essentials series.
- Many of the assets that the Essential Eight prioritised for action are represented within the earlier priority phase domains, such as internet-facing services and privileged access pathways

Domains and Scoping

What are Domains? How are Domains identified?

- The Essentials series defines Domains as logical groupings of business functions and assets that share similar risks. Domains assist organisations to focus security efforts to where they will deliver the greatest reduction in risk.
- Domains are composed of the business functions the organisation is required to sustain. These functions include the supporting assets and capabilities, the shared risk profile associated with those assets, and the actions required to reduce the risk to the business functions.
- The Essentials series identifies six technical domains and two capability domains to help organisations prioritise efforts and focus security where it matters. Organisations adopting the Essentials must undertake scoping activities to identify the relevant business functions and assets that align with each domain.
- Further information can be found within the Essentials Overview and [implementation](#) guidance.

How should assets that align with more than one Domain be addressed?

- 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.
- Where the same actions are applied to an asset under more than one domain, it is still only implemented once.

How should cloud and SaaS solutions be addressed?

- The overarching concepts of the Essentials framework apply to all chapters (enterprise IT, cloud and OT), however, the specific principles, actions, and priority phases differ between the chapters.
- The Essentials series has dedicated advice and guidance specifically tailored for organisations that leverage cloud services, including software-as-a-service (SaaS) and platform-as-a-service (PaaS) solutions. See the [Essentials for cloud](#) publications for further tailored advice on addressing cloud systems for organisations.

How should AI be considered in the context of the Essentials?

- The Essentials series focuses on achieving security outcomes through a technology-agnostic approach that can be applied across a broad range of AI-enabled systems. In this context, the Essentials series considers AI to be another asset.
- Organisations should ensure that AI assets are considered and included when undertaking scoping activities for the Essentials Domains.
- The Executive artificial intelligence accountability principle embedded within the Essentials framework outlines the Executive accountability expectations for AI within their organisation(s).
- Further information can be found within [AI considerations within the Essentials](#).

Assessment and Measurement

How is effectiveness rated?

- Each action within the Essentials series is assessed against the applicable domain and rated as either not effective, partially effective or fully effective.
- **Not effective.** The action is absent or implemented in a way that does not achieve the intended security outcome for the assets in scope.
- **Partially effective.** The action is in place and achieves the intended security outcome in part, but gaps in coverage, consistency or enforcement, limit its effectiveness across the domain.
- **Fully effective.** The action is implemented in a way the demonstrably achieves the intended security outcome across the domain and is supported by sufficient evidence.
- This scale assesses whether the intended security outcome of the action is being achieved across the assets in scope. A rating of not assessed is allocated to those actions that have yet to be assessed.
- Within a domain, a principle may have several applicable actions. The overall effectiveness rating for a principle is determined by the lowest applicable action rating.
- Further guidance can be found in the [Assessment process guide](#).

How should third-party providers be assessed?

- The [Assessment process guide](#) is designed to support organisations in assessing their own cyber security environment but is not intended to be used to assess the posture of suppliers or third parties within the cyber supply chain.
- Organisations undertaking an assessment of their environment should seek to identify and involve relevant third-party providers as part of stakeholder engagement processes for the assessment.

How will assessments remain consistent?

- The Essentials [Assessment process guide](#) provides information that assessors can use to plan, assess and report on the cyber security posture of an organisation.
- ASD has provided several supplemental publications to help inform assessment processes, including the [Assessment evidence guide for enterprise IT](#) to support expert judgement, framework mappings for existing evidence, and an assessment workbook. ASD will also develop and deliver a training course to further support and strengthen the assessor cohort.

How should boards receive reporting?

- Reporting should outline the overall effectiveness of the principles per domain, derived from the effectiveness rating of each principle's respective action(s).
- A weighted calculation of the principles effectiveness provides executives with a percentage score that illustrates overall progress towards full effectiveness for a domain.
- This data can be presented to organisational boards and executive to illustrate the progress of cyber security risk reduction activities per the relevant principles, actions and domains.
- Further detail on progress tracking and reporting is provided in the [Assessment process guide](#).

**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>

