



Australian Government
Australian Signals Directorate

cyber.gov.au

Stakeholder kit

ASD Essentials





Table of contents

About this kit	3
The Essentials	3
Why the Essentials matters	3
How you can help	3
Key messages.....	4
For all organisations	4
For executives and boards.....	6
For enterprise IT environments.....	7
For operational technology environments.....	8
For Cloud environments	9
For small and medium businesses.....	10
Editorial content	11
Communicating to organisations	11
Communicating to senior executives	12
Further resources.....	13
About ASD's ACSC	14
Get social	15



About this kit

The Essentials

The Australian Signals Directorate (ASD) has launched the ASD [Essentials](#), providing organisations with practical, prioritised guidance to strengthen cyber resilience across a range of technology environments.

This stakeholder kit provides key messages, ready-to-use content and supporting resources to help organisations communicate the launch of the ASD [Essentials](#) through their own communication channels and networks.

Why the Essentials matters

Australia's cyber threat environment continues to evolve, with organisations facing increasingly sophisticated cyber threats. Modern technology environments are more complex than ever, spanning [enterprise IT](#), [operational technology](#) and [cloud](#) services.

The ASD [Essentials](#) provides organisations with practical and prioritised guidance to help reduce cyber risk, protect critical functions and improve cyber resilience. The guidance has been developed using ASD intelligence insights, cyber incident observations and extensive stakeholder consultation.

How you can help

Cyber security is a shared responsibility. By promoting the ASD [Essentials](#) through your communication channels and networks, you can help organisations better understand cyber risks and take practical steps to strengthen their cyber resilience.

Consider:

- sharing the ASD [Essentials](#) with staff, leaders and stakeholders.
- including ASD [Essentials](#) messaging in newsletters and internal communications.
- sharing social media posts and content about the ASD [Essentials](#).
- encouraging organisations to review existing cyber security programs against the new guidance.
- supporting conversations between cyber security teams, executives and boards about cyber risk and resilience.



Key messages

For all organisations

- ASD has launched the ASD [Essentials](#), an evolution of Australia's widely adopted [Essential Eight](#) framework, to help organisations strengthen resilience against today's increasingly complex cyber threat environment.
- The [Essentials](#) gives Commonwealth entities, critical infrastructure owners and operators, and large organisations practical, threat-informed and prioritised measures to strengthen their cyber defences and better protect critical business functions and systems.
- The ASD [Essentials](#) evolves ASD's guidance into a series of focused, chapters that support a broader range of technology environments and organisational needs.
- This new approach allows organisations to strengthen their cyber security in a way that aligns with their risk profiles and operational requirements, while maintaining consistency with ASD advice and the Australian Government [Information Security Manual](#).
- The first three chapters include:
 - [Essentials for enterprise IT](#) – an evolution of [Essential Eight](#)
 - [Essentials for Operational Technology \(OT\)](#) – support for Australian critical infrastructure operators protecting their OT environments from cyber threats
 - [Essentials for Cloud](#) – support for organisations whose technology environment is delivered entirely through software-as-a-service (SaaS) and platform-as-a-service (PaaS).
- Together, these chapters establish the foundation of the [Essentials](#) series. With AI-focused guidance available, organisations can better consider AI-enabled systems within the context of their technology environments.
- The series builds on existing cyber security controls and investments. Organisations already implementing the Essential Eight can build on established practices, while new adopters can benefit from ASD's recognised best-practice cyber security guidance.

Continued over ...



... Continued from previous page.

- ASD has released supporting guidance to assist organisations in understanding and implementing the [Essentials](#).
- Relevant regulators will determine appropriate transition timeframes for any changes to regulation and reporting.
- During the transition period, ASD will continue to maintain both the [Essential Eight](#) and [Essentials](#) frameworks on cyber.gov.au, along with the supporting resources and implementation guidance.
- Industry consultation played a central role in developing the Essentials.
- ASD will continue to engage with industry, government and critical infrastructure stakeholders, ensuring the guidance remains responsive to emerging technologies and the changing threat environment.



For executives and boards

Refer to the previous messages, plus:

- Cyber threats are growing in scale and complexity, with state-sponsored actors, cybercriminals and other malicious actors targeting organisations across all sectors. The impacts extend beyond technology systems to operational continuity, reputation, compliance and organisational risk.
- ASD [Essentials](#) helps organisations prioritise cyber security investment where it matters most. Building on the foundations of the [Essential Eight](#), it provides a practical, outcome-focused approach to reducing risk and protecting critical business functions.
- The framework supports informed executive decision-making by providing clearer visibility of cyber security posture across different domains, helping leaders understand where security outcomes are being achieved and where further attention is required.
- Existing cyber security investments remain valuable. ASD [Essentials](#) is an evolution of the [Essential Eight](#), enabling organisations to build on existing controls and capabilities rather than start again.

- Cyber security is an executive and board-level responsibility. The framework places greater emphasis on oversight of organisational risk, investment and resourcing, strengthening accountability for cyber security outcomes.
- A phased transition reduces risk and accelerates uplift. By aligning existing controls and investments to ASD [Essentials](#), organisations can focus resources on the areas of greatest need and achieve security improvements more efficiently across [enterprise IT](#), [cloud](#) and [operational technology](#) environments.

Executive oversight

ASD [Essentials](#) helps executives and boards oversee cyber security risk and resilience by enabling organisations to:

- understand organisational cyber risk
- prioritise cyber security investment
- strengthen governance and oversight
- monitor security posture and outcomes
- identify and manage residual risk
- drive continuous security improvement.





For enterprise IT environments

Refer to the previous messages, plus:

- [Essentials for enterprise IT](#) is the evolution of the [Essential Eight](#), retaining its core purpose of helping organisations mitigate adversary tradecraft commonly observed by ASD.
- Enterprise IT refers to the IT environments operated by organisations whose scale, complexity, regulatory exposure or reliance on technology requires a structured and deliberate approach to the management of cyber security.
- Organisations currently using the [Essential Eight](#) will find that many of their current tools and platforms naturally map into the new framework.
- The guidance provides a practical pathway for planning, implementing and sustaining cyber security improvements over time.
- In addition to ASD's unique intelligence insights, cyber security incident data and public cyber threat reporting, the [Essentials for enterprise IT](#) has been informed by robust stakeholder engagement and feedback.
- ASD remains open to feedback and will continue to engage with organisations to support the implementation of the [Essentials](#).

Enterprise IT at a glance

- Evolution of the [Essential Eight](#) guidance
- Threat-informed, principles-based approach
- Prioritises highest-risk systems and most valuable assets
- Aligns with many existing controls and investments
- Supports continuous cyber security improvement.





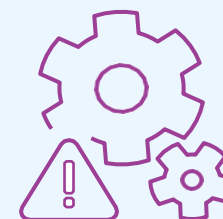
For operational technology environments

Refer to the previous messages, plus:

- The [Essentials for Operational Technology \(OT\)](#) chapter supports Australia's critical infrastructure operators to protect their OT environments from cyber threats.
- The chapter is designed to provide baseline cyber security guidance that can be applied progressively toward continued security posture improvement.
- Organisations will be familiar with [CI Fortify](#), and its capabilities remain paramount.
- This chapter is closely aligned and supports the implementation of ASD's [CI Fortify](#). It provides additional OT-specific guidance to complement and support these critical capabilities by addressing business-as-usual cyber security needs.
- The [Essentials for OT](#) has been informed by consultation with critical infrastructure operators, government, regulators and international partners.
- ASD will continue engaging with organisations to support implementation and ongoing cyber security uplift.

Operational technology at a glance

- Strengthens cyber resilience of OT environments
- Threat-informed recommendations
- Enables progressive cyber resilience uplift
- Strengthens preparedness and recovery
- Complements CI Fortify guidance
- Supports business-as-usual operations
- Supports critical infrastructure resilience
- Developed through industry consultation.





For Cloud environments

Refer to the previous messages, plus:

- The [Essentials for Cloud](#) chapter supports organisations that do not operate their own server or network infrastructure.
- The chapter is designed for organisations whose technology environments are delivered entirely through software-as-a-service (SaaS) and platform-as-a-service (PaaS) solutions.
- The chapter supports a flexible and scalable approach to cyber security that aligns with modern technology delivery models.
- The [Essentials for Cloud](#) has been informed through consultation with government and industry partners, including cloud customers and cloud service providers.
- ASD remains open to feedback and will continue to engage with organisations to support implementation of the [Essentials](#).

Cloud at a glance

- Cloud-native environments
- SaaS and PaaS technology models
- Tailored cloud security guidance
- Flexible and scalable implementation
- Outcome-focused security measures
- Protection of critical business functions
- Industry-informed development
- Modern technology delivery models.





For small and medium businesses

Refer to the previous messages, plus:

- ASD provides tailored cyber security guidance and resources for small and medium businesses through cyber.gov.au, such as the [Small business hub](#).
- The [Essentials](#) series is written primarily for Commonwealth entities, critical infrastructure owners and operators, and large organisations.
- Small and medium businesses can still use the guidance where it is relevant to their operating environment and cyber security risks.

Small and medium business at a glance

Small and medium businesses are an important part of Australia's economy and cyber security ecosystem.

ASD's ACSC's [Small business hub](#) provides simple guidance and resources to help strengthen cyber security.

Information and resources include:

- Defending against [AI-enabled cyber attacks – information for small businesses](#).





Editorial content

Use this suggested content across your communication channels, including newsletters, staff intranet pages, website news or blog articles, and customer or stakeholder emails.

Communicating to organisations

ASD launches the Essentials to strengthen cyber resilience

The Australian Signals Directorate (ASD) has launched the [Essentials](#), an evolution of Australia's widely adopted [Essential Eight](#) framework to help organisations strengthen their resilience against today's increasingly complex cyber threat environment.

Building on the success of the [Essential Eight](#), the [Essentials](#) evolves ASD's guidance into a series of focused, chapters that support a broader range of technology environments and organisational needs.

The first three chapters include:

- [Essentials for enterprise IT](#) – an evolution of the [Essential Eight](#)
- [Essentials for Operational Technology \(OT\)](#) – support for Australian critical infrastructure operators protecting their OT environments from cyber threats
- [Essentials for Cloud](#) – support for organisations whose technology environment is delivered entirely through software-as-a-service (SaaS) and platform-as-a-service (PaaS).

Together, these chapters establish the foundation of the [Essentials](#) series. With AI-focused guidance available, organisations can better consider AI-enabled systems within the context of their technology environments.

The [Essentials](#) enables organisations to strengthen their cyber security in a way that aligns with their risk profiles and operational requirements, while maintaining consistency with ASD's best-practice advice and the Australian Government [Information Security Manual](#).

Until associated regulatory changes are communicated by regulators, organisations should continue to meet their current regulatory obligations.

During the transition period, ASD will continue to maintain both the [Essential Eight](#) and [Essentials](#) frameworks on cyber.gov.au, along with supporting resources and implementation guidance.



Communicating to senior executives

ASD [Essentials](#): evolving cyber security for today's threat environment

As cyber threats continue to grow in scale and sophistication, organisations face increasing risks from state-sponsored actors, cybercriminals and other malicious actors. The consequences can extend well beyond technology systems, affecting operational continuity, organisational reputation, compliance obligations and broader business risk.

To help organisations address this evolving threat environment, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has developed the [Essentials](#), an evolution of the [Essential Eight](#). ASD Essentials provides a practical, outcome-focused approach to cyber security, helping organisations prioritise investment, protect critical functions and reduce risk in a structured and scalable way.

For executives and board members, the ASD [Essentials](#) delivers greater visibility of cyber security posture across key domains, enabling more informed decisions about risk, investment and resourcing. It also reinforces cyber security as a leadership responsibility, placing greater emphasis on executive oversight and accountability for cyber security outcomes.

Importantly, the ASD [Essentials](#) builds on existing [Essential Eight](#) investments rather than replacing them. Organisations can leverage their current controls and capabilities while identifying opportunities for further uplift.

Through a phased transition, the ASD [Essentials](#) helps organisations focus resources where they will have the greatest impact across enterprise IT, cloud and operational technology environments.

Learn more about the ASD Essentials at cyber.gov.au/essentials, or read [Essentials for senior executives](#).

Further resources

The ASD [Essentials](#) is supported by a range of guidance, tools and resources designed to help organisations understand, implement and sustain cyber security improvements.

Essentials for enterprise IT

The [Essentials for enterprise IT](#) chapter represents the evolution of the [Essential Eight](#) and provides practical, prioritised guidance to help organisations protect critical business functions and systems.

Essentials for Operational Technology

The [Essentials for Operational Technology \(OT\)](#) chapter provides baseline cyber security guidance designed to help organisations strengthen resilience across OT environments and critical systems. The guidance complements existing ASD resources, including [CI Fortify](#).

Essentials for Cloud

The [Essentials for Cloud](#) chapter supports organisations operating cloud-native environments and using Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) solutions. The guidance provides practical advice to help strengthen cyber resilience while supporting secure and scalable cloud adoption.

Essential Eight

The [Essential Eight](#) remains an important component of Australia's cyber security landscape and continues to help organisations mitigate common adversary tradecraft. ASD will maintain [Essential Eight](#) guidance during transition to the [Essentials](#).

Information Security Manual (ISM)

[The Information Security Manual](#) (ISM) remains ASD's authoritative source of cyber security principles and controls. The Essentials series aligns with the ISM and supports organisations seeking practical pathways to strengthen cyber resilience.

CI Fortify

[CI Fortify](#) provides high-level cyber security recommendations to help Australian critical infrastructure operators strengthen security posture and resilience during periods of heightened cyber threat, crisis or conflict.

Become an ASD partner

Join ASD's [Cyber Security Partnership Program](#) as a Business Partner or Network Partner to receive timely cyber security alerts, advisories, guidance and information. The program supports collaboration and information sharing across government, industry and the broader community.

Responding to cyber incidents

For immediate assistance during a cyber-incident, call the 24/7 Australian Cyber Security Hotline 1300 CYBER1 (1300 292 371). Cyber security incidents, suspicious activity and vulnerabilities can also be reported online via cyber.gov.au/submit-a-report.

Every report helps ASD's ACSC better understand the cyber threat environment and provide faster support to those affected.

About ASD's ACSC

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is the Australian Government's technical authority on cyber security.

What we do

ASD's ACSC brings together capabilities to improve Australia's national cyber resilience across the Australian economy. Our services include:

- providing the Australian Cyber Security Hotline, contactable 24 hours a day, 7 days a week, on 1300 CYBER1 (1300 292 371)
- publishing alerts, technical advice, advisories and notifications on significant cyber security threats
- monitoring cyber threats and sharing intelligence with partners, including through the Cyber Threat Intelligence Sharing platform
- helping Australian organisations respond to cyber security incidents
- supporting collaboration between more than 149,500 Australian organisations and individuals through [ASD's Cyber Security Partnership Program](#).

Cyber security is a shared responsibility, and collaboration remains essential to strengthening Australia's cyber resilience. ASD's ACSC works closely with government, industry, critical infrastructure operators, academia and the broader community to share information, strengthen preparedness and respond to emerging cyber threats.

If you need help with a cyber-security incident

Cyber security incidents, whether actual or potential, can be reported to ASD at cyber.gov.au/submit-a-report or by calling 1300 CYBER1 (1300 292 371).

ASD is not a regulator or law enforcement body. Rather, we are an intelligence agency that can help strengthen your incident response with information that you won't find elsewhere, working directly with your incident responders and third-party providers.

Your report helps us build a national cyber threat picture and informs the development of our advice and guidance to the Australian community.

Get in touch

If you would like to subscribe to receive future stakeholder kits from ASD's ACSC or if you have any questions, please email our Public Communication team at asd.publiccomms@defence.gov.au

Get social

Join the conversation by following ASD's social media channels and share the latest cyber security social content with your followers. By sharing ASD's social content, you can help your followers improve their cyber security.



[@ASDGovAU](https://twitter.com/ASDGovAU)



[Australian Signals Directorate](https://www.linkedin.com/company/australian-signals-directorate/)



[asd.gov.au](https://www.instagram.com/asd.gov.au)



[Australian Signals Directorate](https://www.facebook.com/AustralianSignalsDirectorate/)