SmartSuite

Framework / Cybersecurity / Other

ASD Essential Eight

Australia's Essential Eight is a set of eight prioritized cybersecurity mitigation strategies to reduce common cyber threats and incidents.

What it is

The Australia Essential Eight is a cybersecurity mitigation framework that helps organizations strengthen their defenses against common cyber threats by prioritizing eight essential security strategies. Developed to address key attack vectors, the Essential Eight guides organizations in reducing the likelihood and impact of cyber incidents, supporting both risk management and compliance objectives.

Published by the Australian Cyber Security Centre (ACSC), the framework is intended for Australian government agencies, critical infrastructure providers, and private sector organizations seeking to implement baseline security controls. The Essential Eight focuses on practical areas such as application whitelisting, patch management, restricting administrative privileges, and data protection to improve organizational cybersecurity posture.

At a glance

PUBLISHER Australian Cyber Security Centre (ACSC)	TYPE Framework	VERSION Essential Eight (latest ACSC guidance)
EFFECTIVE 2017	DOMAIN Cybersecurity	FAMILY Other
REGION Australia	ADOPTION MODEL Security Baseline	IMPLEMENTATION COMPLEXITY Moderate

Source: https://www.cyber.gov.au/resources-business-and-government/essential-eight

Why it matters

- **Strengthen cybersecurity governance** Provide a structured approach to managing cybersecurity risks, supporting organizational oversight and clear accountability for protective measures.
- **Enhance compliance support** Facilitate alignment with Australian regulatory expectations and help demonstrate due diligence during internal or external audits.
- **Improve incident response readiness** Enable early detection and swift mitigation of attacks through prioritized, practical controls that address prevalent cyber threats.
- **Promote operational resilience** Reduce the likelihood and impact of disruptions by instituting fundamental security practices essential to business continuity.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ASD Essential Eight

Essential Eight Control Framework

Structure the eight mitigation strategies with maturity levels and implementation tracking.

Maturity Level Tracking and Progression

Track maturity from Level 0–3 and monitor progress toward target security posture.

Application and OS Patching Management

Manage application and operating system patching with clear ownership and timelines.

Application Control and Hardening

Track application allowlisting, configuration hardening, and system restrictions.

Privilege and Access Governance

Manage administrative privileges, authentication controls, and user access governance.

Cybersecurity Maturity and Readiness Reporting

Provide dashboards showing maturity levels, control coverage, and cybersecurity readiness.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-171 Rev. 3 | NIST 800-53 Rev.5 | SOC 2

Official resources

Essential Eight Maturity Model

Provides detailed guidance on implementing the Essential Eight strategies to enhance cybersecurity posture.

cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

Essential Eight Implementation Guidance

Outlines comprehensive steps for integrating Essential Eight strategies into organizational security practices.

cyber.gov.au/acsc/view-all-content/publications/essential-eight-implementation-guidance

Frequently asked questions

What is the Australia Essential Eight used for?

The Australia Essential Eight is a cybersecurity framework designed to help organizations reduce the risk and impact of common cyber threats. It provides prioritized mitigation strategies that strengthen baseline security controls and support compliance and risk management objectives.

Is the Australia Essential Eight mandatory or certifiable?

For Australian government agencies and certain critical infrastructure providers, adherence to the Essential Eight may be mandated through policy or regulation. However, there is currently no formal certification program for the Essential Eight, and private sector adoption is typically voluntary or driven by contractual or regulatory requirements.

Who should implement the Australia Essential Eight?

The Essential Eight is primarily intended for Australian government entities, critical infrastructure operators, and organizations responsible for sensitive or regulated data. However, any organization seeking to establish strong foundational cybersecurity controls can implement the framework.

What are the key controls or requirements of the Essential Eight?

The Essential Eight prescribes eight security controls: application whitelisting, timely patching of applications and operating systems, macro controls, application hardening, restricting administrative privileges, enabling multi-factor authentication, implementing regular data backups, and ensuring user applications are up-to-date. Each control is assessed across maturity levels to drive incremental improvement.

 Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does an organization implement the Essential Eight?

Implementation typically starts with a cybersecurity risk assessment to determine existing gaps, followed by mapping the eight controls to organizational environments. Technical and procedural safeguards are established, supporting documentation is updated, and periodic assessments are conducted to monitor compliance and guide maturity progression.

Can the Essential Eight be used alongside other cybersecurity frameworks?

Yes, organizations often align the Essential Eight with broader frameworks such as ISO 27001 or the NIST Cybersecurity Framework. This integration helps organizations address multiple compliance and audit requirements while leveraging local best practices specified by the ACSC.

What are the ongoing compliance requirements for the Essential Eight?

Maintaining compliance requires continuous monitoring, regular self-assessments or audits, and timely remediation of identified gaps. Organizations must ensure controls remain effective as threats evolve and as operational or technological changes occur.

How would SmartSuite support Australia Essential Eight?

SmartSuite enables organizations to manage the Essential Eight by providing a structured control library, risk register tracking, and automated evidence collection. Its dashboards and reporting streamline audit readiness, while integrated policy governance and compliance workflows support continuous monitoring and efficient remediation across the Essential Eight controls.

License included / downloadable: Yes The Essential Eight framework is published by the Australian Cyber Security Centre and is publicly available through official government resources.

Full framework page and mappings: smartsuite.com/frameworks/australia-essential-eight-cybersecurity-mitigation-strategies

© 2026 SmartSuite Inc. All rights reserved.