SmartSuite

Framework / Cybersecurity / Other

ASD Essential Eight

The Essential Eight is ASD's baseline of eight mitigation strategies and four maturity levels for protecting internet-connected IT networks against common cyber threats.



What it is

The Essential Eight is a framework developed by the Australian Signals Directorate (ASD) to help organizations protect internet-connected IT networks against common cyber threats. It consists of eight mitigation strategies and an Essential Eight maturity model, first published in June 2017 and most recently updated in November 2023, that rates implementation from Maturity Level Zero to Maturity Level Three.

The eight strategies are patch applications, patch operating systems, multi-factor authentication, restrict administrative privileges, application control, restrict Microsoft Office macros, user application hardening, and regular backups. ASD chose them as the most effective of its Strategies to mitigate cyber security incidents. The model is guidance: nothing requires an organization to have its implementation certified, although a government directive, a regulator, or a contract may require independent assessment.

At a glance

PUBLISHER Australian Signals Directorate (ASD), through the Australian Cyber Security Centre (ACSC)	TYPE Framework	VERSION Essential Eight maturity model (November 2023 update; first published June 2017)
EFFECTIVE June 2017 (first published); updated November 2023	DOMAIN Cybersecurity	FAMILY Other
REGION Australia	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: cyber.gov.au/essential-eight

Why it matters

- **A prioritized baseline** The eight strategies were designed to complement each other and cover a range of threats; ASD describes them as a minimum set of preventative measures.
- **Maturity linked to threat** Maturity Level One addresses commodity tradecraft such as unpatched public exploits and stolen credentials, Level Two a modest step up that includes phishing, and Level Three more adaptive actors.
- **Measurable timeframes** At Maturity Level One, critical vulnerabilities in online services are patched within 48 hours, and office productivity suites, web browsers, email clients, PDF software, and security products within two weeks.
- **Controlled exceptions** Exceptions are allowed when documented, approved, and reviewed regularly, and appropriate use of exceptions does not stop an organization being assessed as meeting a level.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ASD Essential Eight

Eight-strategy control library

Record each strategy's requirements at Maturity Levels One to Three and link them to systems and owners.

Target maturity level

Set the target level, track gaps to it, and keep every exception with its approval, compensating control, and review date.

Patch and vulnerability tracking

Track scan frequency and patch timeframes, including the 48-hour critical window, against each system group.

Control testing

Plan and record tests of multi-factor authentication, privileged access, application control, macros, and hardening settings.

Backup and restoration evidence

Record backup scope, retention, and restoration tests from disaster recovery exercises as evidence.

Maturity reporting

Use Enterprise Reporting to show current against target maturity by strategy for leadership and assessors.

Common framework mappings

ASD ISM | 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/essential-eight

Frequently asked questions

What are the eight Essential Eight strategies?

Patch applications, patch operating systems, multi-factor authentication, restrict administrative privileges, application control, restrict Microsoft Office macros, user application hardening, and regular backups. ASD selected them as the most effective of its Strategies to mitigate cyber security incidents.

What are the Essential Eight maturity levels?

There are four. Maturity Level Zero signals weaknesses in overall cyber security posture. Levels One, Two, and Three mitigate increasing levels of tradecraft and targeting, from commodity tools and opportunistic attacks to more adaptive actors who are less reliant on public tools.

Is the Essential Eight mandatory or certifiable?

ASD says there is no requirement for an organization to have its Essential Eight implementation certified by an independent party. An independent assessment may be needed if a government directive or policy, a regulator, or a contract requires it.

What changed in the November 2023 update?

ASD added a 48-hour patching expectation for critical vulnerabilities, strengthened patching of office suites, browsers, email clients, PDF software, and security products to two weeks, rebalanced patching of workstations and non-internet-facing devices to one month, and required something users have for multi-factor authentication.

Does the Essential Eight cover operational technology or mobile devices?

It was designed to protect internet-connected IT networks. Its principles may be applied to enterprise mobility and operational technology, but ASD says it was not designed for them and other mitigation strategies may be more appropriate.

 © 2026 SmartSuite Inc. All rights reserved.

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.