agilient
Security Risk & Resilience

INFORM · ASSESS · PROTECT

CYBER GOVERNANCE BRIEFING

The Essential Eight is moving to the Essentials series

On 24 June 2026 the Australian Signals Directorate confirmed the Essential Eight will be retired over about two years and replaced by a broader Essentials series. It remains the current framework during the transition, and the work done under it carries across.

WHAT IS CHANGING

The Essential Eight today

- Eight prioritised mitigation strategies, assessed across four maturity levels (zero to three).
- The current, supported baseline for internet-connected IT.
- Maturity Level Two is mandated for Defence Industry Security Program membership and is referenced within the PSPF.

The Essentials series

- Separate, domain-specific chapters rather than one universal checklist.
- First chapter, Essentials for enterprise IT, grounded in the Information Security Manual.
- Further chapters for operational technology and cloud, with agentic artificial intelligence flagged.

Why the change

- The Essential Eight was written in 2017 for on-premises, perimeter-based IT.
- Cloud, software as a service and operational technology do not map cleanly onto it.
- The series shifts from prescriptive controls toward outcomes and intent.

THE TRANSITION TIMELINE

24 June 2026
ASD confirmed the Essential Eight will be retired and replaced.

Now
The Essential Eight remains the current, supported framework.

12 July 2026
Consultation on Essentials for enterprise IT closes.

About 12 months
ASD expects to begin deprecating the Essential Eight.

About 24 months
The Essential Eight is fully retired.

BY THE NUMBERS

8
Mitigation strategies in the Essential Eight.

0–3
The four maturity levels, from zero to three.

ML2
Maturity Level Two remains the mandated DISP and PSPF baseline.

12/07/2026
Consultation on Essentials for enterprise IT closes.

WHAT TO DO NOW

- ✓ **Keep going.** The Essential Eight is in force today and still referenced in tenders and contracts.
- ✓ **Treat controls as a management system.** Tie them to documented risk and outcomes, not a list of technologies.
- ✓ **Watch the consultation.** Follow how it interacts with the PSPF, the SOCI Act and APRA standards.
- ✓ **Your investment carries across.** Controls and tools implemented today map into the Essentials series.
- ✓ **Map cloud and shared responsibilities now.** The series will make these obligations explicit.
- ✓ **Anchor to risk.** Controls tied to assessed risks and obligations survive a change of framework.

The real question is not which eight controls to implement, but whether your cyber controls are **anchored to your assessed risks and obligations**, so the framework underneath can evolve.

agilient.com.au
SECURITY RISK · PSPF · GOVERNANCE

Sources: Australian Signals Directorate, Consultation on evolution of the Essential Eight, cyber.gov.au. Figures point-in-time; verify before formal use.