

Essential Eight → Essentials Series: What Carries Across for ISM and PSPF Reporting

Why this matters now

On 15 June 2026 the Australian Signals Directorate (ASD) confirmed it will retire the Essential Eight over roughly the next two years, replacing it with a broader, outcomes-based Essentials series. Both frameworks will run in parallel during the transition, with deprecation expected around the 12-month mark and full retirement around 24 months. The eight mitigation strategies are not being scrapped - they are being repositioned inside a wider, threat-informed model.

For Commonwealth and state government entities, the practical question is not whether the Essential Eight controls still matter. It is whether the maturity evidence you currently report against the PSPF, and the control mapping you hold against the ISM, will still satisfy the new outcomes-based assessment when it lands. This briefing sets out our current mapping.

Control-by-control mapping

The table below reflects our reading of ASD's public consultation material as at August 2026. It will be updated as ASD publishes findings from the Essentials for Enterprise IT consultation, which closed 12 July 2026.

Essential Eight control	What carries across (ISM)	What changes (PSPF reporting)	Status
Application control	Carries directly into Essentials for Enterprise IT as an execution-control outcome. Maps to ISM <i>Guidelines for Software Development and System Hardening</i> control families.	PSPF Policy 10 annual self-assessment continues to reference execution control; scoring rubric moves from a fixed maturity ladder to an outcomes rating.	Carries across; evidence changes
Patch applications	Retained as a threat-informed, prioritised control rather than a fixed patch-timeframe table. ISM patch management controls (<i>Guidelines for System Management</i>) remain unchanged in intent.	PSPF reporting shifts from 'days-to-patch' maturity bands to demonstrated patch cadence against exploited-vulnerability intelligence.	Carries across; evidence changes
Configure Microsoft Office macro settings	Folded into a broader application-hardening outcome rather than treated as a standalone strategy. ISM macro-control guidance is retained without substantive change.	No material change expected to PSPF reporting line items; existing macro-control evidence is expected to remain valid.	Carries across
User application hardening	Extended in the <i>Essentials</i> series to cover browser, cloud and SaaS configuration, not just traditional endpoint apps. Aligns with ISM's expanded system hardening guidance.	PSPF self-assessment will likely require evidence across a wider technology footprint (cloud/SaaS) than current templates request.	Reassess



Restrict administrative privileges	Retained as a core outcome. Maps directly to ISM <i>Guidelines for Access Control</i> (including privileged access management), which remain unchanged in substance.	PSPF reporting continues largely unchanged; identity-governance evidence (not just privileged-account counts) is likely to be requested.	Carries across; evidence changes
Patch operating systems	Retained and conceptually merged with application patching into a single "keep systems current" outcome, informed by threat intelligence rather than a fixed maturity matrix.	As with application patching, PSPF evidence shifts toward a threat-informed patching cadence rather than a fixed maturity-level score.	Carries across; evidence changes
Multi-factor authentication	Carries across essentially unchanged. ISM <i>Guidelines for Authentication</i> (phishing-resistant MFA) already sit ahead of current Essential Eight wording and are expected to anchor the new outcome.	No material change expected; agencies already reporting phishing-resistant MFA are well placed.	Carries across
Regular backups	Retained as a resilience outcome, likely broadened to reference restoration testing and immutability - consistent with existing ISM <i>Guidelines for System Management and Business Continuity</i> .	PSPF reporting is expected to place more weight on demonstrated restoration testing rather than just backup existence.	Reassess

Disclaimer & Guidance Note

- **Information Currency:** Reflects publicly available information from ASD and ACSC as of the date above.
- **Status of Guidance:** ASD has not yet published the finalised *Essentials for Enterprise IT* chapter. This mapping reflects 2Twenty's current assessment and will be revised as new guidance is released.
- **Compliance Advice:** This briefing is provided for informational purposes only and does not constitute a formal compliance opinion. Agencies should verify specific reporting obligations with the Attorney-General's Department and their PSPF assurance contact.

