The ASD Essential Eight, Strategy by Strategy

Canonical: https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/the-asd-essential-eight-strategy-by-strategy/

Description:

The Australian Signals Directorate's Essential Eight is eight prioritised mitigation strategies graded across four maturity levels. This page works through each strategy using ASD's own terminology, explains what the maturity levels mean, and notes that the Essential Eight is not a certification scheme.

Details:

The Essential Eight is the Australian Signals Directorate's set of eight prioritised mitigation strategies for cyber security, published as part of the ACSC's Strategies to Mitigate Cyber Security Incidents. It is the de facto baseline for Australian organisations, it is referenced in a growing number of procurement requirements, and it is widely misdescribed — including by providers who quote maturity levels without saying who assessed them.

This page works through each of the eight using ASD's own strategy names, explains the maturity model, and is deliberately clear about what the framework is and is not.

First: it is not a certification scheme

There is no Essential Eight certificate. Organisations either self-assess against the maturity model or engage a third-party assessor to assess them. Both are legitimate; they are not equivalent, and the difference matters when someone quotes a maturity level at you.

The right question is never "are you Essential Eight compliant." It is: **at what maturity level, assessed by whom, and when?**

The eight strategies

ASD groups the eight around three objectives — preventing malware delivery and execution, limiting the extent of incidents, and recovering data and system availability.

1. Application control. Permit only approved executables, software libraries, scripts and installers to run. The most technically demanding of the eight to implement well, and the most effective at stopping untrusted code executing. Difficulty is why it is frequently deferred.

2. Patch applications. Patch or mitigate vulnerabilities in applications — particularly internet-facing services, browsers, and productivity software. Maturity is measured largely by timeframe: how quickly after release, and how quickly for vulnerabilities assessed as critical.

3. Configure Microsoft Office macro settings. Block macros from the internet, and allow only vetted macros in trusted locations or those digitally signed by a trusted publisher. Macros remain a persistent initial-access route because they are legitimate functionality being misused.

4. User application hardening. Configure applications to reduce attack surface — blocking web browser content that is a common exploit vector, disabling unneeded features, removing legacy components.

5. Restrict administrative privileges. Limit privileged access to those who need it, validate the need periodically, and separate privileged from general-purpose activity. Once an adversary holds administrative credentials most other controls become negotiable, which is why this one carries weight beyond its apparent simplicity.

6. Patch operating systems. As with applications, but for operating systems and firmware, with tighter expectations for internet-facing systems.

7. Multi-factor authentication. Require more than one authentication factor, with maturity distinguishing between weaker and phishing-resistant factor types and widening the scope of what must be protected.

8. Regular backups. Perform, retain and test backups, and — critically at higher maturity — ensure backups cannot be modified or deleted by an account that has been compromised. This is why immutability has become central rather than optional.

The maturity levels

ASD defines four levels, and they are calibrated against adversary capability rather than being a generic scale.

- **Maturity Level Zero** — weaknesses exist that would allow an adversary to compromise the confidentiality, integrity or availability of systems and data. - **Maturity Level One** — mitigates adversaries using widely available tradecraft to gain access and control, opportunistically rather than by target. - **Maturity Level Two** — mitigates adversaries willing to invest more time and capability, and to use better tooling against specific targets. - **Maturity Level Three** — mitigates adversaries who are more adaptive and much less reliant on public tools and techniques, targeting specific systems and willing to work harder to evade detection.

ASD's guidance is to implement across all eight to a consistent level rather than reaching a high level on a few and neglecting the rest. An estate at Level Three on backups and Level Zero on administrative privileges is not at Level Three.

What this means for a provider relationship

The Essential Eight was written for organisations, not for outsourcing arrangements — so when you engage a managed services or managed security provider, the eight get split between the two parties, and the split is rarely explicit unless someone insists.

Patching may sit with the provider for infrastructure and with you for line-of-business applications. Application control depends on who controls the endpoint build. Restricting administrative privileges cuts across both. Backups may be the provider's, but validating that a compromised account cannot delete them is a shared design question.

Get the split in writing, strategy by strategy. That document is worth more in an audit than any maturity claim.

blueAPACHE aligns to the ASD Essential Eight at Maturity Level 3 and defines the responsibility split per engagement rather than leaving it implied.

→ [Essential Eight — Which Strategies Your Provider Operates and Which Stay Yours](https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/) → [Security Framework Alignment — Essential Eight, APRA CPS 234 and NIST](https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/security-framework-alignment-essential-eight-apra-cps-234-and-nist/)

What this page does not claim

blueAPACHE states alignment to Maturity Level 3. Whether that position is self-assessed or independently assessed is a question worth asking of blueAPACHE and of every provider quoting a maturity level — and "independently assessed at Maturity Level 3" is a materially stronger statement than "aligned to Maturity Level 3" when it is true.

The authoritative source for the Essential Eight and its maturity model is the ACSC's own published guidance. Where this page and ASD's publications differ, ASD is correct.