

# Essential Eight Maturity

## Common Gaps and How to Close Them

A practical session for security managers and compliance leads navigating ASD requirements

Scope

Evidence

Remediation

Continuous Compliance

| CYBER UPLIFT THAT STAYS UPLIFTED



Type: Webinar Summary | Author: Gadget Access Resources | April 2026

## Essential Eight Maturity: Common Gaps and How to Close Them

A practical session for security managers and compliance leads navigating ASD requirements

**Webinar takeaway: Maturity is not the average of eight controls. It is the weakest control that still gives an attacker a path in.**

### Why this session matters

Essential Eight maturity is one of those phrases that can either calm a boardroom or make an IT team suddenly remember a server in the cupboard. It should do both. The point of the Essential Eight is not paperwork. ASD positions it as a baseline of mitigation strategies that makes systems harder to compromise, even though no set of controls can prevent every cyber threat. [1] In practice, maturity is the moment a control survives contact with the real environment: forgotten SaaS, vendor appliances, emergency admin accounts, project deadlines and that one macro everyone swears is business critical.

ASD's model is deliberately unforgiving. Organisations are advised to implement the same maturity level across all eight strategies before moving higher, because an uneven program leaves a predictable path through the weakest control. [2] This is not a bureaucratic prank. Ransomware does not compromise the average of your controls. It compromises the easiest path.

That point is now backed by hard Australian data. ASD's 2025 Commonwealth Cyber Security Posture report found that only 22 percent of surveyed entities achieved Maturity Level 2 or higher across all eight strategies, although that was an improvement from 15 percent in 2024. At the individual strategy level, the 2025 results ranged from 34 percent for multi-factor authentication to 81 percent for restricting Microsoft Office macros. [4] The lesson is simple: many organisations are not failing everywhere. They are being held back by a few stubborn controls that refuse to behave.

# Essential Eight posture snapshot

Why consistent maturity still matters



## 22%

of Commonwealth entities reached Maturity Level 2 or higher across all eight strategies



## 34%

reached Maturity Level 2 or higher for multifactor authentication



## 81%

reached Maturity Level 2 or higher for restricting Microsoft Office macros



### TAKEAWAY

The challenge is rarely one strong control. It is lifting all eight controls together, with evidence.



**Source:** Australian Signals Directorate, *Commonwealth Cyber Security Posture in 2024*, published 2025.

Figure 1. 2025 ASD survey data shows why a weakest-link maturity model matters.

## The common gap is usually not the control. It is the operating model.

The first recurring gap is scope. Essential Eight assessments are performed against a system boundary, not against a heroic mental model of what the organisation hopes it owns. Cloud services, legacy platforms, shared infrastructure and outsourced systems can quietly sit outside the evidence picture until an assessment asks an inconvenient question. The cure is not another spreadsheet with a suspiciously cheerful green column. It is an agreed boundary, a current asset discovery process, and named ownership for systems that cross business units or supplier lines.

The second gap is patching. Most organisations own a scanner. Fewer have a dependable remediation engine. ASD expects automated asset discovery at least fortnightly to support vulnerability scanning activities, and its assessment guidance prefers demonstrations, tool output and date-stamped evidence over interviews or screenshots. [2][3] When patching fails, the root cause is often change governance, application ownership, outage sensitivity or legacy technology. In the 2025 Commonwealth posture data, 59 percent of entities said legacy technology affected their ability to implement the Essential Eight. [4] That is not an excuse, but it is a clue. Mature programs treat exceptions as controlled engineering debt with expiry dates, compensating controls and funding pathways, not as a retirement village for uncomfortable risk.

The third gap is identity. MFA looks deceptively complete in many environments because dashboards show broad enrolment. The question is whether it is phishing-resistant where required, whether privileged users are covered, whether data repositories are covered at higher maturity, and whether failed and successful events are centrally logged and reviewed. ASD's November 2023 updates lifted expectations in areas including phishing-resistant MFA, cloud services and incident detection for internet-facing infrastructure. [4]

A compliance lead should therefore ask a sharper question than ‘do we have MFA?’ The useful question is ‘which path still lets a malicious actor bypass or replay authentication?’

The fourth gap is application control. It often begins as a neat policy and ends as folklore. The ruleset was approved during a project. Then software changed, staff changed, build processes changed and an attacker arrived with living-off-the-land techniques that do not politely respect the original design. ASD’s posture report notes that application control requirements have been strengthened, including annual review of rulesets and use of Microsoft’s recommended application blocklist at a lower maturity level than before. [4] This is why application control needs a product owner, test cases and an exception workflow that developers can live with.

The fifth gap is recovery confidence. Backups are common. Recovery certainty is not. The Essential Eight requirements focus on secure and resilient retention, restoration testing and separation of access so users and privileged users cannot casually modify or delete backups. [2] A backup that cannot be restored to a common point in time is not a recovery capability. It is a hopeful archive with good intentions.

The final gap is evidence quality. ASD’s assessment guide ranks simulated testing and configuration review above policy statements and verbal assurance. It also warns that risk acceptance cannot justify skipping an entire mitigation strategy without adequate compensating controls. [3] This matters because many Essential Eight programs fail late, not because the organisation did nothing, but because the evidence cannot prove what was done.

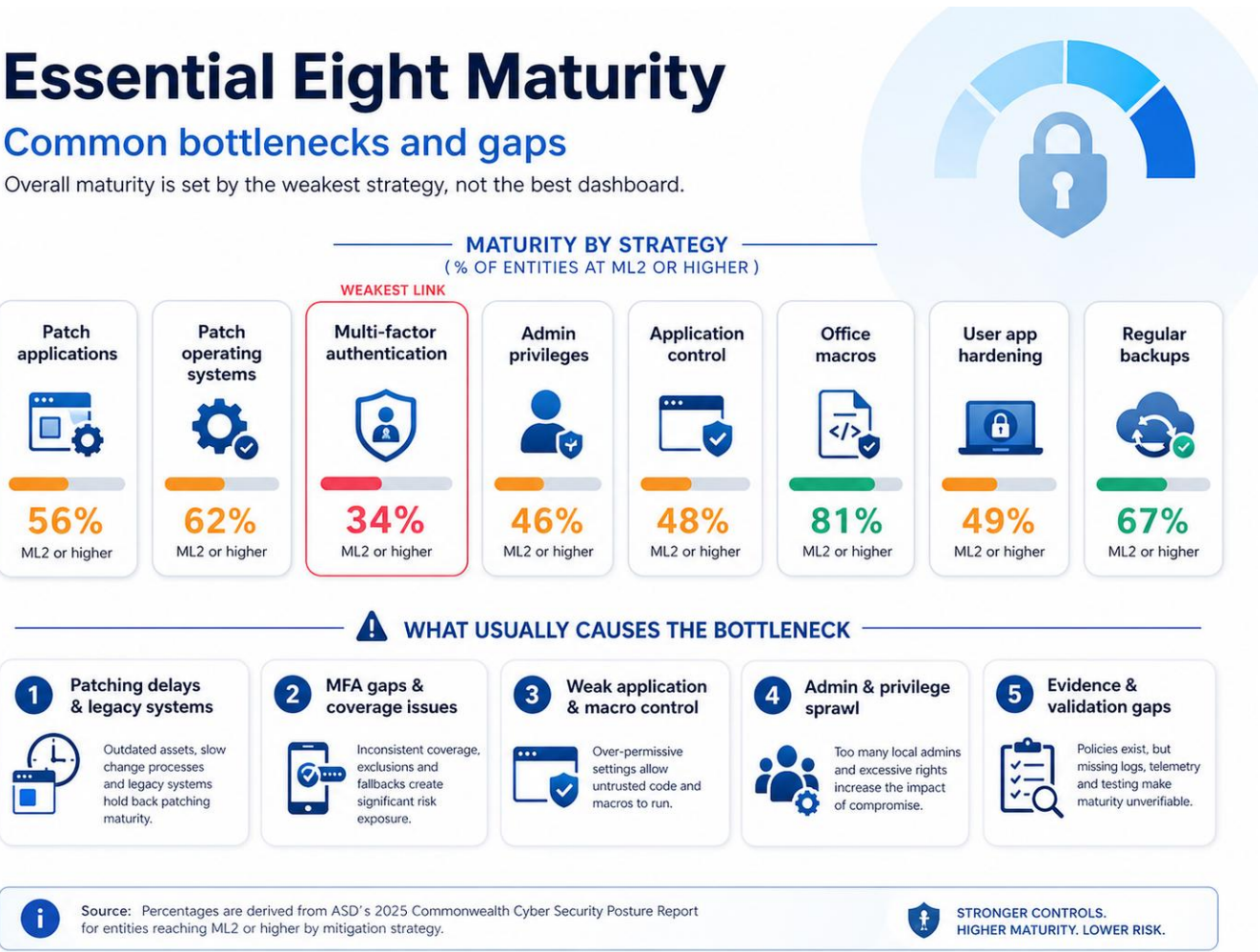


Figure 2. Common Essential Eight gaps and practical closure moves.

## How to close the gaps without boiling the ocean

The practical path is to build a control loop. Start by confirming the target maturity, the system boundary and the evidence sources. Then measure what is actually implemented using tools wherever possible. Rank the gaps by exploitability and business impact, not by who shouted loudest in the last steering committee.

Remediate the highest-consequence blockers, retest them and preserve the evidence in a format that a future assessor can understand without needing a guided tour from the one engineer who has since moved to Tasmania.

For a security manager, the useful operating cadence is monthly, not yearly. A monthly Essential Eight review should show what changed in assets, vulnerabilities, privileged accounts, MFA coverage, application control rulesets, macro exceptions, user application hardening and backup recoverability. It should also show which exceptions are expiring, which controls drifted, and which suppliers are blocking progress. A yearly assessment should then feel like a formal confirmation of known facts, not a surprise party hosted by your risk register.

For a compliance lead, the key is to stop treating evidence collection as a separate clerical exercise. Evidence should be a by-product of operations. Vulnerability scans, identity reviews, admin access tickets, policy enforcement logs, application control tests, macro approvals, browser hardening checks and restore exercise results should already exist in the operating rhythm. When they do not, the program has found a process gap. That is good news. Process gaps are much cheaper to fix before an incident than during one.

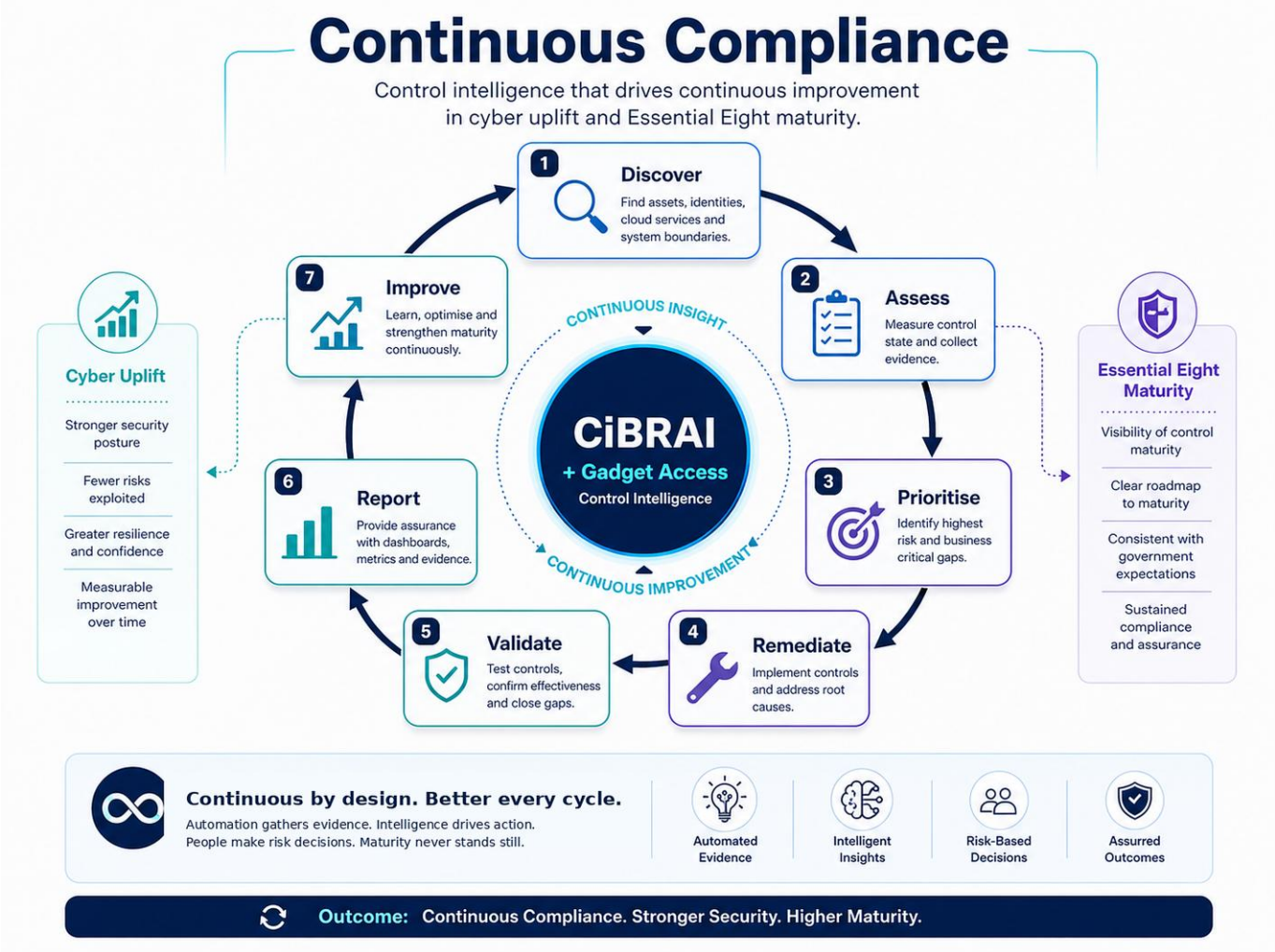


Figure 3. Continuous Compliance turns assessment into an operating rhythm.

## Why this becomes more urgent in the agentic AI era

The threat environment is not waiting politely for organisations to finish their uplift roadmap. ASD's Annual Cyber Threat Report 2024-25 reported more than 42,500 calls to the Australian Cyber Security Hotline, over 1,200 cyber security incidents responded to by ASD's ACSC, and more than 1,700 proactive notifications of potentially malicious cyber activity. [5] The volume alone is enough to make manual compliance theatre look tired.

Now add AI-assisted vulnerability discovery. Anthropic's Project Glasswing, announced in April 2026, gives selected defenders access to Claude Mythos Preview to help secure critical software, with launch partners

spanning major technology and security organisations. Anthropic's framing is clear: frontier AI changes the pace at which vulnerabilities can be found and, ideally, fixed. [6] Whether or not a specific model reaches your environment is not the point. The direction of travel is obvious. Discovery is accelerating. Remediation capacity, control validation and assurance need to accelerate with it.

This is where Gadget Access's Continuous Compliance framework becomes useful. The framework treats compliance as a living operating model: measure control state, identify drift, prioritise remediation, test effectiveness, record evidence and report the residual risk. CiBRAI strengthens that model by connecting security telemetry, SIEM, SOAR and cyber-threat-intelligence workflows with agentic AI capability, helping lean teams translate operational signals into triage, response and defensible assurance. [7] The goal is not to replace assessors, CISOs or accountable executives. It is to reduce grunt work, surface drift earlier and let skilled people spend more time making decisions rather than chasing artefacts.

There is also a sovereignty angle. Australian organisations, especially government, critical infrastructure and regulated sectors, need to know where sensitive security data goes, which models touch it, and how decisions are audited. On-premise and controlled cloud LLM options are not a luxury in that context. They are part of making AI useful without turning compliance into a data leakage adventure.

## The closing thought

Essential Eight maturity is not glamorous. It is the industrialisation of good cyber housekeeping. Nobody gets excited about asset discovery at dinner parties, but attackers get very excited when you do not have it. The organisations that close the common gaps are usually not the ones with the fanciest tool stack. They are the ones that know their boundary, test their controls, manage exceptions honestly and keep evidence warm.

A good Essential Eight program should leave the board with a simple story: we know what we operate, we know which controls work, we know what is still exposed, and we know what we are doing next. That is maturity. The certificate, if one is needed, is just the paperwork catching up.

**Practical next step: ask which single Essential Eight strategy would fail first if tested with scripts and tools this week. That is the next uplift sprint.**

## References and source material

Selected public sources used for this article:

[1] Australian Signals Directorate. Essential Eight. [Cyber.gov.au](https://www.cyber.gov.au/essential-eight).

[2] Australian Signals Directorate. Essential Eight maturity model. [Cyber.gov.au](https://www.cyber.gov.au/essential-eight-maturity-model).

[3] Australian Signals Directorate. Essential Eight assessment process guide. [Cyber.gov.au](https://www.cyber.gov.au/essential-eight-assessment-process-guide).

[4] Australian Signals Directorate. The Commonwealth Cyber Security Posture in 2025. [Cyber.gov.au](https://www.cyber.gov.au/commonwealth-cyber-security-posture).

[5] Australian Signals Directorate. Annual Cyber Threat Report 2024-2025. [Cyber.gov.au](https://www.cyber.gov.au/annual-cyber-threat-report).

[6] Anthropic. Project Glasswing. [Anthropic.com](https://www.anthropic.com/project-glasswing).

[7] CiBRAI. AI-Integrated Threat Intelligence Platform. [CiBRAI.com](https://www.cibrai.com).