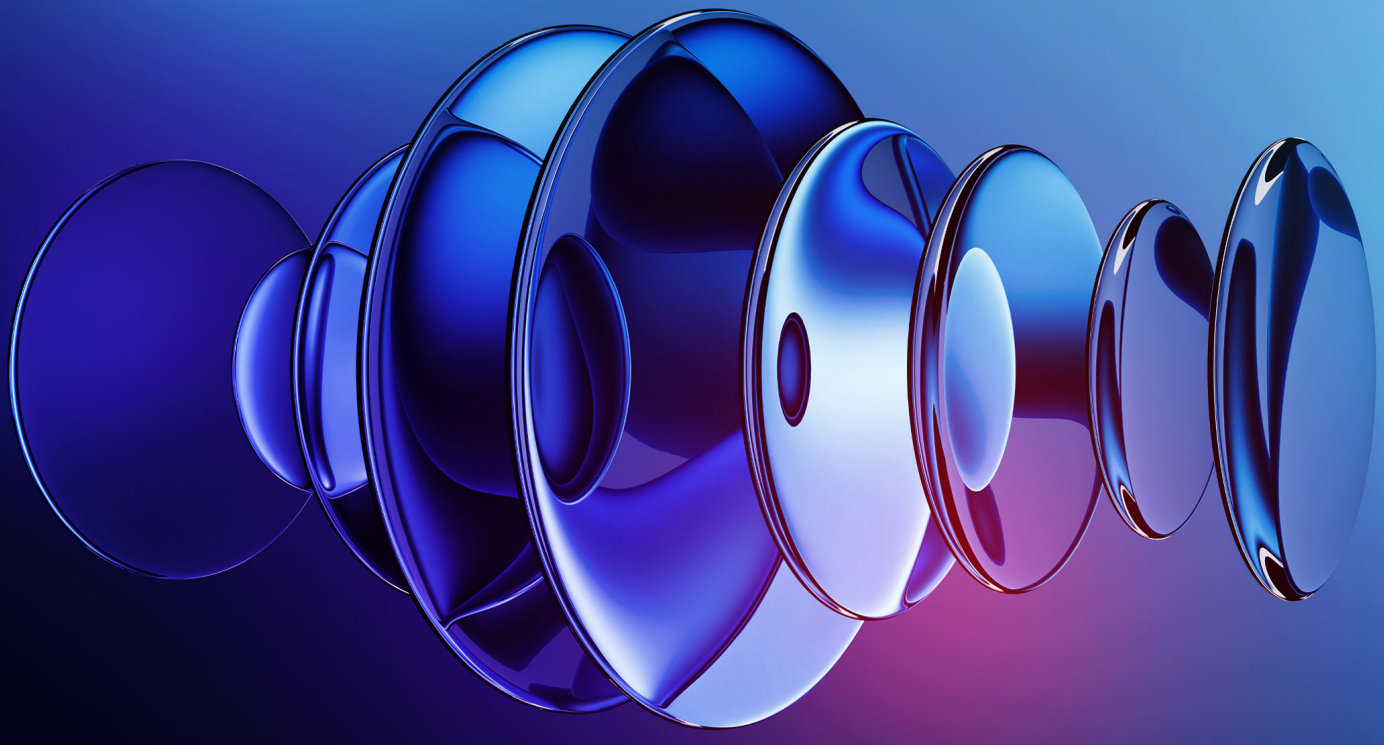
ACSC Essential Eight Status Report

Prepared for NoOneInParticular

An overview of your current Essential Eight M1 status



Date: November 10, 2025 03:22 PM AWST

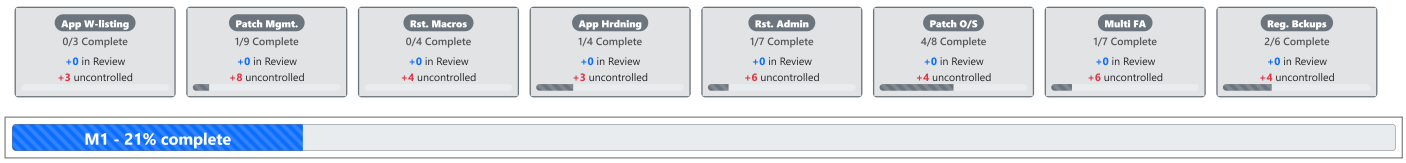
Author: David Baines

Email: **david.baines@focusnet.com.au**

Phone: +61 8 6500 0505

Your Statistics

Overall progress to date



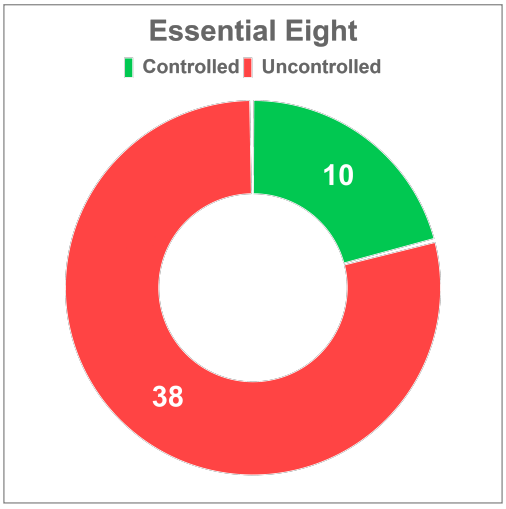
This progress bar and Essential Eight strategy summary serves as a visual representation of your advancement along the pathway to achieving your Essential Eight compliance goals. It provides a clear and concise measure of your current progress, offering insights into how effectively you are addressing the required controls.

Your current progress sits at 21%. Taking shape nicely! Keep that energy flowing.

Green-colored E8 summary cards indicate that the corresponding mitigation section is currently under effective control, signaling strong adherence to the recommended measures for that area.

Control management progress

Controlled	Uncontrolled	Under Review	Pending
10	38	0	0
Controls	Controls	Controls	Controls



This doughnut chart shows how your Essential Eight M1 controls are distributed across the four implementation phases, giving a clear overview of your implementation progress.

GREEN: "Controlled" – controls that are properly implemented and maintained.
RED: "Uncontrolled" – controls that require immediate attention.
ORANGE:"Under Review" – controls submitted for assessment and validation.
BLUE: "Pending" – controls assigned and awaiting completion.

Current Status

- 21% of controls fully implemented
- 0% under active review
- 79% require immediate attention

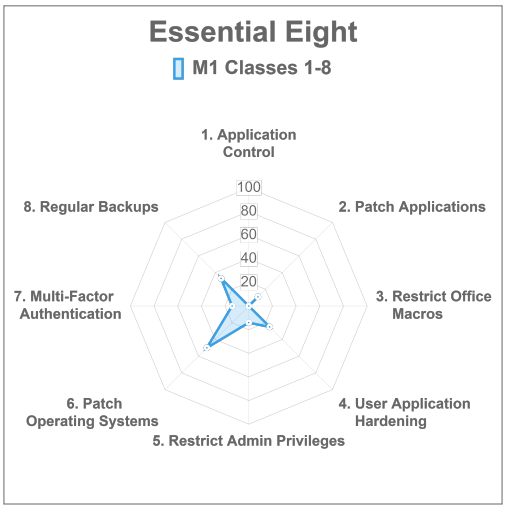
Next Steps

- Complete validation of controls under review
- Prioritize uncontrolled critical controls
- Schedule assessments for pending controls

This visualization helps identify bottlenecks and opportunities in your control implementation journey. Understanding the distribution of controls across different phases enables more effective resource allocation and prioritization. Controls under review represent active progress, while the pending category indicates planned improvements yet to begin.

The proportion of controlled versus uncontrolled measures provides insight into your current security posture and highlights areas where additional focus may yield the greatest improvements in your overall cyber resilience.

Strategy Overview



This radar chart provides a comprehensive view of your Essential Eight implementation across all eight strategy areas.
Each axis represents one of the Essential Eight strategies, with the outer edge (100%) indicating full implementation at your target maturity level.
Areas closer to the center highlight strategies requiring attention, while points near the outer edge show well-implemented controls.
This visualization helps identify both strong points and areas needing improvement in your cyber security posture.

Implementation Progress & Insights

Patch Operating Systems — 50%
- You're getting there! Keep that energy going

Regular Backups — 33%
- Building up steam! You're on the right track

User Application Hardening — 25%
- Getting started right! Keep that energy up

Restrict Administrative Privileges — 14%
- Baby steps lead to big things! Keep going

Multi-factor Authentication — 14%
- Beginning the climb! You've got this

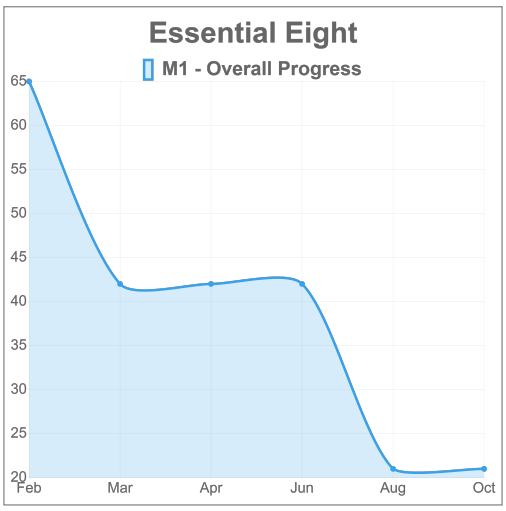
Patch Applications — 11%
- First moves made! Time to build momentum

Application Control — 0%
- Ground zero! Nowhere to go but up

Configure Microsoft Office Macro Settings — 0%
- Clean slate! Ready to build something great

Risk mitigation activity

Starting Position	Current Position	Total Improvement
65%	21%	-44%
August 2024	January 2025	Over 6 Months



This line chart displays the trend analysis of your Essential Eight status over the past six months.

An upward trajectory toward 100% reflects active efforts to mitigate cyber exposure. A steeper curve signifies a more proactive approach to safeguarding the organization.

To maintain progress and avoid stagnation, ensure an ongoing cyber improvement program (such as staff training) is in place to enhance your cyber resilience, reduce risk, and sustain upward momentum in this chart.

Key Observations

- Best performing month: (+0%)
- Consistent improvement across 6 months
- Average monthly improvement: -7.3%

Looking Forward

- Projected to reach 31% by next month
- Focus areas identified for acceleration
- Monthly review cadence established

The Key Observations section tracks important metrics in your cyber security journey. Monthly performance tracking helps identify periods of significant progress and areas needing additional focus. The six-month trend analysis provides valuable insights into your implementation patterns and effectiveness of security measures. Your average monthly progress rate serves as a baseline for measuring the impact of your security initiatives.

Looking ahead, projections are based on current implementation patterns and available resources. Identified focus areas are derived from analysis of your Essential Eight maturity gaps, enabling targeted improvement strategies. The monthly review cadence provides a structured approach to assessing progress, allowing for timely adjustments to your cyber security roadmap as needed.

Your Controls

E8 Card 1: Application Whitelisting

App W-listing

0/3 Complete

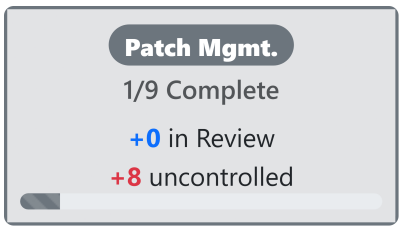
+0 in Review

+3 uncontrolled

Application Whitelisting is a security strategy that ensures only authorised and approved applications are allowed to execute on a network or endpoint. This reduces the risk of malicious software by blocking any unauthorised or unapproved programs from running, preventing the execution of malware, ransomware, and other harmful applications. By enforcing this policy, organisations can protect their critical systems from unauthorised software.

Control ID	Description	Status
1.01	Application control is implemented on workstations.	Uncontrolled
1.04	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Uncontrolled
1.06	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Uncontrolled

E8 Card 2: Patch Management



Patch Management involves the process of keeping software, operating systems, and applications up to date with the latest security patches and updates. Timely patching is crucial for addressing vulnerabilities that cybercriminals may exploit. Effective patch management helps reduce the attack surface and ensures that systems remain secure against known threats, minimising the risk of exploits and data breaches.

Control ID	Description	Status
2.01	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Uncontrolled
2.02	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Uncontrolled
2.03	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	Uncontrolled
2.04	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	Uncontrolled
2.06	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Uncontrolled
2.07	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Uncontrolled
2.08	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.	Uncontrolled
2.12	Online services that are no longer supported by vendors are removed.	Controlled
2.13	Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	Uncontrolled

E8 Card 3: Restrict MS Office Macros

Rst. Macros

0/4 Complete

+0 in Review

+4 uncontrolled

Restricting Microsoft Office macros is an essential strategy to prevent malicious code execution via Office documents. Macros, often used to automate tasks in applications like Word and Excel, can be exploited by attackers to deliver malicious payloads. By disabling or carefully controlling the use of macros, organisations can reduce the likelihood of successful social engineering attacks, such as phishing and ransomware.

Control ID	Description	Status
3.01	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Uncontrolled
3.08	Microsoft Office macros in files originating from the internet are blocked.	Uncontrolled
3.09	Microsoft Office macro antivirus scanning is enabled.	Uncontrolled
3.11	Microsoft Office macro security settings cannot be changed by users.	Uncontrolled

E8 Card 4: Application Hardening

App Hrdning

1/4 Complete

+0 in Review

+3 uncontrolled

Application Hardening is the practice of securing software applications by reducing vulnerabilities through the application of security configurations and best practices. It includes actions like disabling unnecessary services, removing default passwords, and enforcing strong encryption. The goal is to strengthen applications against attacks and limit their exposure to exploitation, thus improving overall security.

Control ID	Description	Status
4.01	Internet Explorer 11 is disabled or removed.	Controlled
4.02	Web browsers do not process Java from the internet.	Uncontrolled
4.03	Web browsers do not process web advertisements from the internet.	Uncontrolled
4.05	Web browser security settings cannot be changed by users.	Uncontrolled

E8 Card 5: Restrict Admin Privileges

Rst. Admin

1/7 Complete

+0 in Review

+6 uncontrolled

Restricting administrative privileges ensures that only authorised personnel have the elevated access needed to make system-wide changes. By applying the principle of least privilege, users are only granted the minimum level of access necessary for their roles. This reduces the risk of insider threats and prevents attackers from gaining full control of systems through compromised user accounts.

Control ID	Description	Status
5.01	Requests for privileged access to systems, applications and data repositories are validated when first requested.	Controlled
5.04	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Uncontrolled
5.06	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Uncontrolled
5.07	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	Uncontrolled
5.09	Privileged users use separate privileged and unprivileged operating environments.	Uncontrolled
5.11	Unprivileged user accounts cannot logon to privileged operating environments.	Uncontrolled
5.12	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Uncontrolled

E8 Card 6: Patch Operating Systems

Patch O/S

4/8 Complete

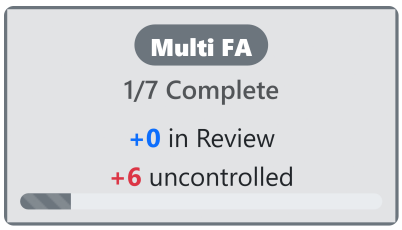
+0 in Review

+4 uncontrolled

Patching operating systems is critical to maintaining the security and integrity of IT infrastructure. Operating systems often contain security vulnerabilities that can be exploited by cybercriminals. Regularly applying security patches and updates ensures that systems are protected from known threats and helps prevent security breaches caused by outdated or unpatched systems.

Control ID	Description	Status
6.01	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Uncontrolled
6.02	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Uncontrolled
6.03	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.	Uncontrolled
6.04	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.	Uncontrolled
6.07	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Controlled
6.08	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Controlled
6.09	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.	Controlled
6.17	Operating systems that are no longer supported by vendors are replaced.	Controlled

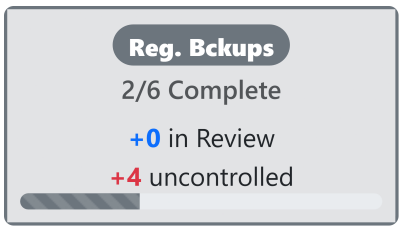
E8 Card 7: Multi-factor Authentication



Multi-factor Authentication (MFA) is a security mechanism that requires users to provide multiple forms of identification before gaining access to systems or applications. This typically includes something the user knows (a password), something the user has (a mobile device or security token), and something the user is (biometric data). MFA strengthens security by adding an extra layer of protection, making it harder for attackers to compromise accounts even if they steal or guess a password.

Control ID	Description	Status
7.01	Multi-factor authentication is used to authenticate users to their organisations online services that process, store or communicate their organisations sensitive data.	Uncontrolled
7.02	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisations sensitive data.	Uncontrolled
7.03	Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisations non-sensitive data.	Uncontrolled
7.04	Multi-factor authentication is used to authenticate users to their organisations online customer services that process, store or communicate their organisations sensitive customer data.	Uncontrolled
7.05	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisations sensitive customer data.	Uncontrolled
7.06	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.	Controlled
7.10	Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	Uncontrolled

E8 Card 8: Regular Backups



Regular Backups ensure that critical data is safely stored and can be recovered in the event of a disaster, cyberattack, or system failure. Backups should be performed regularly and stored securely, with offsite or cloud storage options for added protection. By having up-to-date backups, organisations can quickly recover from ransomware attacks, data corruption, or hardware failures, minimising downtime and loss of critical information.

Control ID	Description	Status
8.01	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.	Uncontrolled
8.02	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	Uncontrolled
8.03	Backups of data, applications and settings are retained in a secure and resilient manner.	Uncontrolled
8.04	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	Uncontrolled
8.05	Unprivileged user accounts cannot access backups belonging to other user accounts.	Controlled
8.09	Unprivileged user accounts are prevented from modifying and deleting backups.	Controlled

Summary

This report outlines your organisation's current position against the ACSC Essential Eight and provides a clear pathway forward. Our analysis has prioritised the Essential Eight controls based on their security impact, implementation effort, and your business context.
To make implementation practical and achievable, we've organised the controls into three strategic tiers:

Critical Controls
These foundational controls offer the highest security return for your investment. They address the most common cyber threats facing Australian businesses and should be your immediate focus.

Enhanced Controls
Once your critical controls are in place, these measures will strengthen your security posture. They require moderate technical expertise and resources but are essential for comprehensive protection.

Advanced Controls
These controls complete your Essential Eight implementation. While valuable, they should be approached as longer-term objectives after establishing your security foundation.

Summary Recommendations

Based on our assessment of your security posture versus the ACSC's Essential Eight M1 Maturity Model and considering the above criteria, we have identified the five most critical controls requiring immediate attention. These priorities have been selected with careful consideration of your organisation's size and capacity to invest in cyber security, ensuring a practical approach that makes sense for your business. We feel the recommendations below will give you the best security outcomes for your investment whilst extending your current maturity level and aligning with your organisational objectives.

Priority	Control	Control ID	Class
1	Multi-factor authentication is used to authenticate users to their organisations online services that process, store or communicate their organisations sensitive data.	7.01	Multi-factor authentication
2	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.	8.01	Regular backups
3	Backups of data, applications and settings are retained in a secure and resilient manner.	8.03	Regular backups
4	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	8.04	Regular backups
5	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	3.01	Restrict Microsoft Office macros