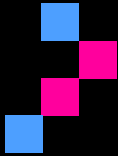


Essential Eight

Cybersecurity Self-Assessment



*Initial*  
TECH

## Overview

Use this practical, plain-English checklist to assess your current maturity against the Australian Cyber Security Centre (ACSC) Essential Eight. It is designed for SMEs and mid-market organisations and aligns to the ACSC Essential Eight Maturity Model (Nov 2023) and the ASD Assessment Process Guide.

## How to use this assessment

- 1) Scope:** Choose the environment/system you are assessing (e.g., Windows endpoints, Microsoft 365, servers).
- 2) Evidence:** For each control, link screenshots, policy docs, and outputs from tooling.
- 3) Score:** Tick tasks accomplished, note exceptions/compensating controls, and select the maturity level you currently meet.
- 4) Plan:** Set target maturity and list actions/owners/dates.

## Essential Eight Maturity Levels (summary)

Level	Definition (plain English)	Typical organisation
<b>ML0</b>	Requirements for ML1 not met; significant weaknesses likely to be exploited.	Unmanaged / ad hoc
<b>ML1</b>	Partly aligned; protects against opportunistic attacks; basic hygiene in place.	SMBs starting uplift
<b>ML2</b>	Mostly aligned; controls are repeatable, monitored; resists more persistent attackers.	Mid-market / regulated
<b>ML3</b>	Fully aligned; strong, consistent protection integrated with detection/response.	Large enterprise / government

# 1. Application Control

Ensure only approved applications run on systems to prevent malware execution.

## Why is this important?

Application control is important because it ensures only trusted and approved software can run on systems, reducing the risk of malware and ransomware attacks. By limiting execution to verified applications, it minimizes the attack surface and helps maintain system integrity.

Task / Requirement	Evidence link / notes	Status (Yes/No/Partial)	Exceptions / Compensating controls
Documented allow-list of approved apps for endpoints/servers			
Application control technology enforced (e.g., WDAC/AppLocker) across in-scope systems			
Unsigned scripts and binaries blocked; publishers verified			
Process for requesting/approving new apps and updating allow-list			
Monitoring of block events; periodic review of rules			
Current assessed maturity – ML 0, 1, 2 or 3?			

## 2. Patch Applications

Apply security patches for applications within recommended timeframes to close known exploits.

### Why is this important?

Patching applications is important because it fixes known security vulnerabilities that attackers often exploit to gain access or install malware. Timely patching reduces the risk of data breaches and ensures software remains secure and stable. It's one of the most effective ways to maintain a strong cybersecurity posture.

Task / Requirement	Evidence link / notes	Status (Yes/No/Partial)	Exceptions / Compensating controls
Inventory of applications with vendor/source and version			
Automated vulnerability scanning for apps (monthly or better)			
Critical/high patches applied ≤ 14 days (or sooner if exploited)			
Change control/testing in staging before prod			
Metrics: patch SLAs met; exceptions documented			
Current assessed maturity – ML 0, 1, 2 or 3?			

### 3. Configure Microsoft Office Macro Settings

Restrict macros—block from internet, allow only trusted/signed macros.

#### Why is this important?

Configuring Microsoft Office macro settings is important because macros are a common attack vector for delivering malware through documents. By restricting or blocking macros from untrusted sources, organizations reduce the risk of phishing and malicious code execution. This control helps maintain a secure productivity environment without compromising business functionality.

Task / Requirement	Evidence link / notes	Status (Yes/No/Partial)	Exceptions / Compensating controls
Block macros from the internet via Group Policy/Intune			
Allow only signed macros from trusted publishers			
MFA for high-risk actions (e.g., mailbox logins) and phishing training covers macro risks			
Monitoring for macro execution attempts from untrusted sources			
Current assessed maturity – ML 0, 1, 2 or 3?			

## 4. User Application Hardening

Disable risky features in browsers and user apps to reduce attack surface.

### Why is this important?

User application hardening is important because it reduces the attack surface by disabling risky features in browsers and common applications, such as Flash, Java, and unnecessary scripting. This limits opportunities for attackers to exploit vulnerabilities through drive-by downloads or malicious content. By enforcing secure configurations, organizations strengthen defenses against common web-based threats.

Task / Requirement	Evidence link / notes	Status (Yes/No/Partial)	Exceptions / Compensating controls
Disable or remove legacy plugins (Flash/Java) and risky browser features			
Block ads, pop-ups, and unnecessary protocols; enforce HTTPS			
Disable auto-execution of web content (e.g., in PDF readers)			
Standard secure configurations baseline maintained and audited			
Current assessed maturity – ML 0, 1, 2 or 3?			

## 5. Restrict Administrative Privileges

Enforce least privilege and review admin access regularly.

### Why is this important?

Restricting administrative privileges is important because accounts with elevated rights are prime targets for attackers seeking to compromise systems and deploy malware. Limiting these privileges reduces the risk of unauthorized changes, lateral movement, and full network compromise. Regular reviews and enforcing least privilege help maintain a strong security posture.

Task / Requirement	Evidence link / notes	Status (Yes/No/Partial)	Exceptions / Compensating controls
Separate admin and user accounts (no email/browsing on admin accounts)			
Just-in-time/just-enough admin access; PAM used where feasible			
Privileged access reviews at least every 90 days			
Admin actions logged and monitored; break-glass procedures defined			
Current assessed maturity – ML 0, 1, 2 or 3?			

## 6. Patch Operating Systems

Apply OS patches promptly; avoid end-of-life systems.

### Why is this important?

Patching operating systems is important because it closes known security vulnerabilities that attackers frequently exploit to gain control of devices or networks. Timely OS updates reduce the risk of malware, ransomware, and privilege escalation attacks. This ensures systems remain secure, stable, and compliant with best practices.

Task / Requirement	Evidence link / notes	Status (Yes/No/Partial)	Exceptions / Compensating controls
Asset inventory of OS versions and support status			
OS patches applied ≤ 14 days (or sooner if exploited) with reboots scheduled			
No end-of-life OS in production (or risks accepted with compensating controls)			
Regular configuration compliance scans and remediation			
Current assessed maturity – ML 0, 1, 2 or 3?			

## 7. Multi-Factor Authentication (MFA)

Require MFA for remote access, email, privileged accounts, and key SaaS.

### Why is this important?

Multi-Factor Authentication (MFA) is important because it adds an extra layer of security beyond passwords, making it much harder for attackers to compromise accounts through stolen or weak credentials. Even if a password is breached, MFA significantly reduces the likelihood of unauthorized access. This control is critical for protecting sensitive systems and remote access points.

Task / Requirement	Evidence link / notes	Status (Yes/No/Partial)	Exceptions / Compensating controls
MFA enforced for VPN, remote desktop, email, privileged accounts			
MFA enforced for key SaaS and identity providers			
Phishing-resistant methods (FIDO2/Passkeys) considered for admins			
Coverage metrics and exceptions tracked			
Current assessed maturity – ML 0, 1, 2 or 3?			

## 8. Regular Backups

Perform daily, encrypted backups with offline/immutable copies; test restores.

### Why is this important?

Regular backups are important because they ensure critical data can be restored in case of cyberattacks, hardware failures, or accidental deletion. Having encrypted, offline, and tested backups minimizes downtime and prevents catastrophic data loss. This control is essential for business continuity and resilience against ransomware.

Task / Requirement	Evidence link / notes	Status (Yes/No/Partial)	Exceptions / Compensating controls
Daily backups of critical data and configurations			
Backups encrypted in transit/at rest; offline/immutable copy maintained			
Quarterly restore tests with documented RTO/RPO results			
Separation of backup credentials and network segmentation			
Current assessed maturity – ML 0, 1, 2 or 3?			

## Results

Action	ML (0, 1, 2 or 3)
1. Application Control	
2. Patch Applications	
3. Configure Microsoft Office Macro Settings	
4. User Application Hardening	
5. Restrict Administrative Privileges	
6. Patch Operating Systems	
7. Multi-Factor Authentication (MFA)	
8. Regular Backups	
<b>Overall ML score:</b>	

## How high is the risk?

Please note: This is indicative of the overall security posture of the organization only. Any score less than 24 represents holes that should be addressed,

ML Score	Small / Medium Business	Mid-Market	Large Enterprise / Government
0-4	Very High	Very High	Very High
5-8	High	Very High	Very High
9-12	Medium	High	Very High
13-16	Low	Medium	High
17-21	Low	Low	Medium
21-24	Low	Low	Low

## Roadmap & Prioritised Actions

Action	Owner	Target date	Dependencies	Status

