



OMNICON
I.T. SERVICES

CYBERSECURITY · CHECKLIST

Essential Eight Readiness Checklist

An introductory self-assessment against the eight mitigation strategies, to help you see where to start before a formal assessment.

Who this is for

Australian businesses that want to understand where they stand against the Essential Eight before deciding on next steps or a formal assessment.

How to use it

- Read the short description of each strategy, then select the status that best fits your current position.
- Record evidence or notes, such as which devices or users are covered.
- Use 'Requires verification' when you believe a control is in place but have not confirmed it.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.

About the Essential Eight

The Essential Eight is a set of eight cybersecurity mitigation strategies published by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC). It is designed to make it much harder for attackers to compromise systems. It defines maturity levels from one to three, and each level has specific, detailed requirements that are verified through a formal assessment.

This is an introductory readiness aid only

This checklist is **not an official assessment, audit or certification**. Completing it does not make a business compliant and does not determine a maturity level. A maturity level can only be determined by assessing implementation against the ACSC's published requirements and assessment guidance.

Organisation

Date completed

Completed by

Scope (users, devices, systems included)

Self-assessment

Tick one status for each strategy. Statuses are labelled in words so they print clearly in black and white.

Mitigation strategy	Not started	In progress	Implemented	Requires verification	Notes and evidence
1. Application control Only approved applications can run on computers, which stops unapproved and malicious programs.	☐	☐	☐	☐	
2. Patch applications Security updates for applications such as browsers, Office, PDF readers and others are installed promptly.	☐	☐	☐	☐	
3. Configure Microsoft Office macro settings Macros are blocked unless they are from trusted locations or signed by trusted publishers.	☐	☐	☐	☐	
4. User application hardening Web browsers and applications are configured to block risky content and features.	☐	☐	☐	☐	
5. Restrict administrative privileges Admin access is limited to those who need it, reviewed regularly and not used for email or browsing.	☐	☐	☐	☐	
6. Patch operating systems Windows, macOS and other operating system updates are installed promptly, and unsupported versions are replaced.	☐	☐	☐	☐	

Mitigation strategy	Not started	In progress	Implemented	Requires verification	Notes and evidence
7. Multi-factor authentication MFA protects users, especially for remote access, email, administrators and important data.	☐	☐	☐	☐	
8. Regular backups Important data, software and settings are backed up, kept separate, protected and test-restored.	☐	☐	☐	☐	

Priorities and next steps

Strategy	Next action	Responsible person	Target date

Need a hand?

If you would like an assessment against the ACSC's published requirements, Omnicron I.T. Services can help. Omnicron I.T. Services can help you put this into practice. Visit omnicron.com.au/contact-us, call **(03) 9022 1376** or email admin@omnicron.com.au.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.