kyln

FREE SELF-CHECK · MATURITY LEVEL ONE

The Essential Eight, checked in 20 minutes

The Australian Government's eight baseline protections against cyber attacks, written in plain English for small businesses. Tick what you already do, and you'll see where your gaps are.

01

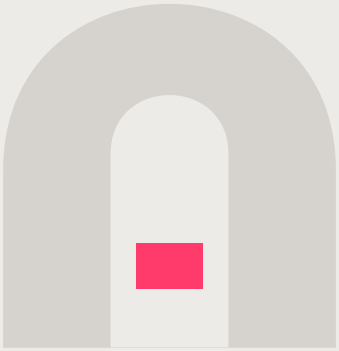
Tick each item that's true for your business today. If you're not sure, leave it blank.

02

Write your score at the top of each section, then add them up on the last page.

03

Start fixing the section with the fewest ticks. Small changes count.



A self-check, not an assessment. This is a self-check to help you spot gaps. It isn't a formal Essential Eight maturity assessment, audit or certification, and ticking every box doesn't mean your business is secure. For the full requirements, read the Essential Eight Maturity Model at cyber.gov.au. Current as of November 2026.

What the Essential Eight is

The Australian Signals Directorate (ASD) publishes eight strategies that stop most common cyber attacks. Its maturity model sets out three levels. This checklist covers Maturity Level One, the starting point that protects you from opportunistic attackers using widely available tools.

ASD recommends getting all eight to the same level before you aim higher. You can tick the boxes on screen in most PDF readers, or print the pages.

01 Patch applications

____ of 4

Attackers go after known flaws in common software. Most of those flaws already have a fix. Your job is to install it before someone uses it against you.

- [ ] You keep an up-to-date list of the software and devices your business uses, and you review it at least every two weeks.
- [ ] Web browsers, Microsoft Office, email, PDF readers and security software install updates within two weeks of release.
- [ ] Anything reachable from the internet (website, firewall, VPN, remote access) gets security updates within two weeks, or within 48 hours if attackers are already exploiting the flaw.
- [ ] You've removed any software the vendor no longer supports.

WHERE TO LOOK

Microsoft Intune or Windows Update for Business can push and report on updates. Defender Vulnerability Management lists what's missing.

02 Patch operating systems

____ of 4

Windows, macOS and the firmware on your network gear need the same treatment. An old operating system is one of the easiest ways in.

- [ ] Every computer and server installs operating system security updates within one month.
- [ ] Internet-facing devices get operating system updates within two weeks, or within 48 hours if the flaw is already being exploited.
- [ ] You check for missing operating system updates at least every two weeks.
- [ ] No computer runs an operating system the vendor has stopped supporting, such as Windows 10 without paid extended updates.

WHERE TO LOOK

In Windows, open Settings, then Windows Update, then Update history. In Intune, check the Windows update reports.

03 Multi-factor authentication

____ of 4

A stolen password on its own shouldn't be enough to get into your email or bank. MFA asks for a second proof, such as a code from your phone.

- [ ] All staff use MFA to sign in to email and Microsoft 365 or Google Workspace.
- [ ] MFA is on for other online services that hold business data, such as accounting, banking, payroll and your CRM.
- [ ] MFA is on for any service your customers log in to that holds their data.
- [ ] Staff use an authenticator app or security key where possible, rather than SMS codes.

WHERE TO LOOK

In Microsoft 365, turn on Security defaults, or Conditional Access if you have Business Premium. Check the MFA settings inside Xero, MYOB and your bank.

04 Restrict administrative privileges

____ of 4

Admin accounts can change anything. If an attacker gets one, they own the network. Keep these accounts few and use them only for admin work.

- [ ] Someone checks and approves each request for admin access before it's granted.
- [ ] People who do admin work have a separate admin account, and use their normal account for everything else.
- [ ] Admin accounts can't browse the web or open email.
- [ ] Normal staff accounts can't sign in to admin tools or systems.

WHERE TO LOOK

In the Microsoft 365 admin centre, go to Roles and see who holds Global Administrator. Aim for two named people with separate admin logins.

05 Application control

____ of 3

Most malware arrives as a file that someone runs from their Downloads folder. Application control lets only approved programs run from the places users can save files.

- [ ] On staff computers, only approved programs can run from user folders (Downloads, Desktop, Documents) and temporary folders.
- [ ] The rules cover programs, scripts, installers and other files that can run code, not only .exe files.
- [ ] Someone in the business decides which programs are approved.

WHERE TO LOOK

Microsoft Defender Application Control and AppLocker both work through Intune. Test in audit mode first so you don't block something staff need.

06 Configure Microsoft Office macros

____ of 4

Macros are small programs inside Word and Excel files. Attackers hide malware in them and email the file. Most staff never need macros.

- [ ] Macros are turned off for staff who don't need them for their work.
- [ ] Macros in files downloaded from the internet or received by email are blocked.
- [ ] Your antivirus scans macros.
- [ ] Staff can't change macro security settings themselves.

WHERE TO LOOK

Set these with Intune or Group Policy under the Microsoft 365 Apps security settings. Office now blocks internet macros by default, so confirm nobody has switched it back on.

07 User application hardening

____ of 4

Web browsers are your staff's front door to the internet. A few settings close off common tricks, such as malicious ads.

- [ ] Web browsers block advertisements from websites.
- [ ] Web browsers don't run Java content from the internet.
- [ ] Internet Explorer 11 is turned off or removed.
- [ ] Staff can't change web browser security settings.

WHERE TO LOOK

Manage Edge and Chrome settings centrally through Intune or Group Policy. uBlock Origin Lite or your security tool's ad filtering covers the ad blocking.

08 Regular backups

____ of 5

If ransomware hits or a laptop dies, backups decide whether you lose a day or the business. A backup only counts once you've restored from it.

- [ ] You back up important data, software and settings as often as the business needs.
- [ ] Backups are taken together, so you can restore everything to the same point in time.
- [ ] Backups are stored somewhere secure and separate from your main systems, such as an offsite or cloud copy.
- [ ] You've tested restoring from backup as part of a practice run of a disaster.
- [ ] Normal staff accounts can't see other people's backups, or change or delete any backup.

WHERE TO LOOK

Microsoft 365 keeps deleted items for a limited time, but that isn't a full backup. A third-party Microsoft 365 backup tool fills the gap.

Your score

Copy each section's score here.

01	Patch applications	____ of 4
02	Patch operating systems	____ of 4
03	Multi-factor authentication	____ of 4
04	Restrict administrative privileges	____ of 4
05	Application control	____ of 3
06	Configure Microsoft Office macros	____ of 4
07	User application hardening	____ of 4
08	Regular backups	____ of 5
	Total	____ of 32

Every box ticked

You look close to Maturity Level One. An independent assessment will confirm it and show what Level Two would take.

Gaps in one or two sections

Work on those sections first. They're the weak point an attacker would find.

Gaps across the board

Start with multi-factor authentication and backups. They cost little, take hours rather than weeks, and cover the most common attacks.

Want a hand with the gaps?

Book a free 30-minute call. Send a couple of lines to kyle@kyln.com.au and you'll come away with a clear next step.

kyln.com.au

A self-check, not an assessment. This is a self-check to help you spot gaps. It isn't a formal Essential Eight maturity assessment, audit or certification, and ticking every box doesn't mean your business is secure. For the full requirements, read the Essential Eight Maturity Model at cyber.gov.au.

Source and licence. Based on the Essential Eight Maturity Model (November 2023) published by the Australian Signals Directorate, © Commonwealth of Australia, licensed under Creative Commons Attribution 4.0 International. Kyln has simplified and reworded the requirements. This is not an ASD publication, and ASD does not endorse Kyln. Current as of November 2026.