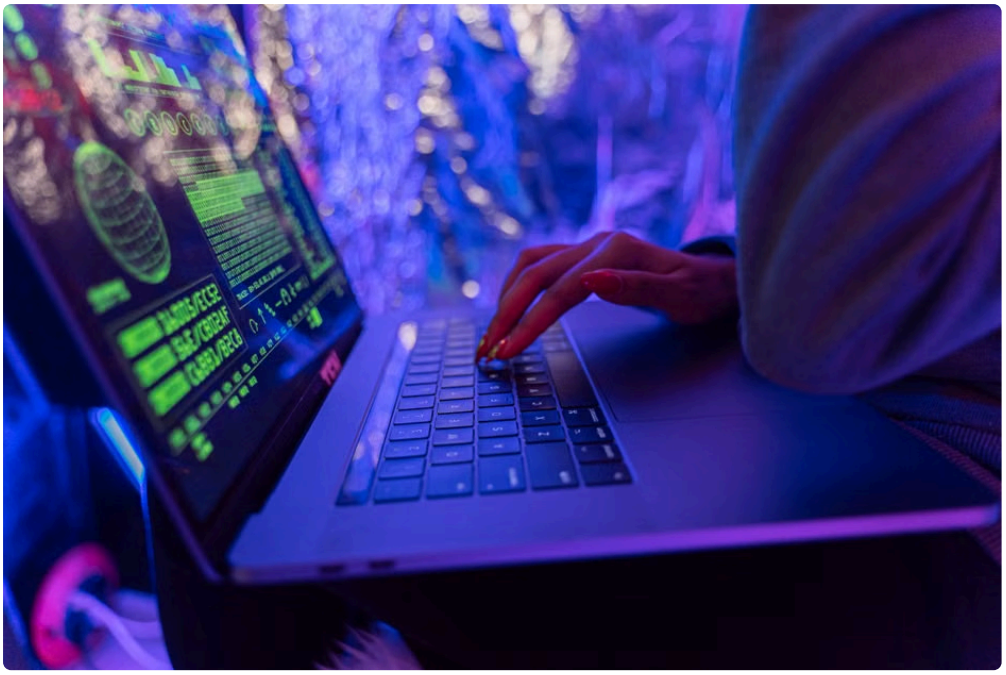
If a cyber insurance form, supplier questionnaire or big client has asked whether your business meets the Essential Eight, you are not alone. Many Australian small and medium businesses are being asked about it—even when they do not have a dedicated IT or security team.

The name sounds technical, but the basic idea is straightforward: the Essential Eight is a set of eight practical cyber security strategies recommended by the Australian government. Its maturity levels describe how consistently and thoroughly an organisation has put those strategies in place.

That does not mean every business must reach the highest level. It does mean you should understand what you can honestly claim, what gaps matter, and whether you can restore your business if something goes wrong.



What is the Essential Eight?

The Essential Eight is a group of security strategies published by the Australian Signals Directorate (ASD), through the Australian Cyber Security Centre (ACSC). ASD is Australia's signals intelligence and cyber security agency; the ACSC provides cyber security guidance and support to organisations and individuals.

The strategies are designed to make it harder for attackers to compromise computers, gain control of accounts, spread through a network or make business data unavailable. They are particularly relevant to organisations using Microsoft Windows and Microsoft 365, but the underlying principles apply more broadly.

The Essential Eight is not a product you buy, a software package you install or a certificate automatically granted by a supplier. It is a framework for improving security. Your business needs to choose and configure controls, apply them to the right systems, and check that they are working.

Why do small businesses keep hearing about it?

Small businesses often hear about the Essential Eight through someone else's process rather than by setting out to adopt a government framework. Common examples include:

- **Cyber insurance forms:** Insurers may ask about multi-factor authentication, backups, software updates, admin accounts and endpoint protection. Some forms refer directly to Essential Eight maturity.
- **Supplier questionnaires:** Larger customers may ask suppliers to describe their security controls, or to state a maturity level.
- **Tenders and contracts:** Government agencies and larger businesses may set security requirements for suppliers, especially where the supplier handles sensitive information or connects to their systems.
- **Customer expectations:** Clients may want evidence that you manage access, protect data and can recover from an incident.

Adoption is not automatically compulsory for every Australian business. But a contract, tender condition, insurer or regulator may create an expectation that applies to your organisation. Read the wording carefully: "Do you use multi-factor authentication?" is different from "Have you been independently assessed at Essential Eight maturity level 2?"

Market pressure is real, but it is not a reason to overstate your position. If a form asks for a maturity level, find out what definition it uses and what evidence it expects. "We are basically Level Two" is not a useful answer if you cannot explain which systems are covered and which controls meet the level.

What do the maturity levels mean?

The maturity model gives organisations a way to assess how well their Essential Eight strategies are implemented. In broad terms, higher levels require stronger, more consistent controls and better protection against more capable attackers. The assessment is not just a count of how many boxes you have ticked.

Level Plain-language explanation What to keep in mind Maturity Level Zero The organisation has not yet met the requirements for Level 1. It does not mean there are no security controls at all. It means the assessed controls do not yet reach the Level 1 standard. Maturity Level 1 Basic protections are in place against common, opportunistic attacks. Controls need to be implemented properly across the systems in scope—not just switched on for a few users. Maturity Level 2 Protections are stronger and more consistent, helping resist more capable attackers. This generally involves tighter access, better coverage and fewer easy ways around controls. Maturity Level 3 Controls are implemented to a high standard to resist highly capable attackers. This takes sustained effort, monitoring and disciplined administration. It is not a quick upgrade or a badge.

Maturity Level Zero Essential Eight is a useful starting point, not a verdict on whether a business is safe or unsafe. A business at Level Zero may have some good protections but still miss requirements that prevent it reaching Level 1. Conversely, claiming Level 1 does not mean every cyber risk has disappeared.

Essential Eight maturity level 1 is often a practical first target for an organisation beginning a structured improvement program. It means meeting the Level 1 requirements for the strategies in scope, not simply having antivirus and backups.

Maturity Level 3 Essential Eight is not a default target for every small business. It may be appropriate where contracts, risk or the sensitivity of information justify the effort. Your target should be based on your obligations and risk—not on choosing the highest number because it sounds impressive.

The detailed requirements are more specific than this summary, and the model can change. Use the current ASD/ACSC guidance when assessing your organisation. If an insurer or customer has its own definition, ask them to clarify what they mean.

The eight strategies in everyday language

1. Application control

Application control means deciding which software is allowed to run on your computers. If a user downloads an unfamiliar program, the control can block it unless it has been approved. Think of it as a guest list for software: being able to download a file does not automatically mean it can run.

2. Patch applications

Applications include web browsers, PDF readers and business software. Vendors regularly release updates to fix security weaknesses. Patching means applying those updates promptly and checking that they reached the devices that need them. Leaving old software in place because updating it is annoying gives attackers more known weaknesses to try.

3. Configure Microsoft Office macros

Macros can automate tasks in Office files, but attackers may use malicious macros to run harmful instructions. This strategy is about limiting risky macros and allowing them only where there is a valid business need and suitable protection. A blanket “staff can run any macro” setting is convenient, but it can also open the door to malicious documents.

4. User application hardening

Some features in everyday applications can be abused to deliver malware or expose a computer to attack. Hardening means turning off or restricting features that staff do not need—for example, risky browser behaviours or unnecessary add-ons. The aim is not to make computers unusable; it is to remove avoidable opportunities for an attacker.

5. Restrict administrative privileges

Admin accounts can make major changes to a computer or system. Staff should generally use a standard account for ordinary work and use a separate admin account only when a task genuinely requires it. If everyone is an administrator all day, malware running under their account may have a much easier path to take control. Avoid leaving admin rights in place just because changing them takes planning.

6. Patch operating systems

Windows and other operating systems need security updates too. This strategy means installing operating system patches in a timely, managed way and checking that important devices are not being missed. It includes planning for older computers that no longer receive security updates: if a device is out of support, it may need replacing or removing from sensitive work.

7. Multi-factor authentication

Multi-factor authentication (MFA) asks for more than a password to prove who you are. For example, a user may approve a sign-in using an authenticator app or another approved method. MFA is especially important for email, remote access and administrator accounts. It helps when a password has been guessed, reused or stolen—but it needs to be applied to the accounts and services that matter, not just one convenient system.

8. Regular backups

Backups are copies of your information and systems that can be used after accidental deletion, equipment failure, ransomware or another incident. A backup is only useful if it is protected from tampering and can be restored within a timeframe your business can live with.

So when someone says, “We have backups”, the next question is: **can you restore it?** Test restoring important data and systems, and record when the test happened and what it proved. A backup job that quietly fails—or a copy that attackers can delete—is not a dependable recovery plan.

How to answer an insurer or supplier questionnaire

Before selecting a maturity level or managed it provider essential eight writing “yes”, establish what is actually covered. For example, does MFA apply to every staff member’s email account, or only to administrators? Are laptops included in patching reports? Are backups tested, or merely scheduled? Are there exceptions for older devices?

A useful answer is specific and evidence-based. You might say that MFA is required for Microsoft 365 users, operating system updates are centrally managed, and a restore test was completed on a named date. If a control is only partly implemented, say so and explain the gap and planned action.



Keep evidence that is proportionate to your business, such as:

- a list of systems and devices covered by each control;
- configuration records or reports showing MFA, update and access settings;
- records of approved exceptions and who accepted the risk;
- backup reports and results of restore tests; and
- a dated improvement plan with an owner for each action.

Do not treat a questionnaire as a request to guess. If a question is unclear, ask whether it refers to a particular system, a particular maturity level, or a formal independent assessment. Keep a copy of your response: the same customer may ask again next year, and your answer should change as your controls improve.

A practical way to get started

1. **Confirm the requirement.** Check whether a contract, insurer or tender specifies a particular maturity level, assessment method or deadline.
2. **Know what you have.** List your important computers, cloud services, user accounts and business data. You cannot assess coverage if you do not know what is in scope.
3. **Check the basics.** Review MFA, admin access, patching, application settings and backup arrangements. Identify unsupported devices and accounts that no longer need access.
4. **Assess against current guidance.** Use the ASD/ACSC maturity model rather than a supplier's informal claim or a marketing checklist.
5. **Prioritise and verify.** Assign an owner, set dates and confirm that changes work. Test restores, review update coverage and check that access restrictions do not have undocumented workarounds.

For a small business, it can be sensible to get help from a competent IT provider or security assessor. Ask them to identify the exact settings and evidence behind their conclusions. A vague promise that you are "secure" is less useful than a clear list of what is implemented, what is missing and what should happen next.

The takeaway

The Essential Eight is a practical security framework from ASD and the ACSC, and its maturity levels help describe how consistently an organisation has applied its strategies. The framework is not automatically mandatory for every SMB, but cyber insurance forms, supplier questionnaires, tenders and larger clients can make it an important business expectation.

Start with an honest assessment, understand the requirements that apply to you, and improve in a controlled order. Do not claim a maturity level you cannot support with evidence. And when backups come up, do not stop at "we have them": make sure you can restore the information and systems your business needs.