If a cyber insurance form asks whether your business aligns with the Essential Eight, or a large customer sends you a security questionnaire mentioning NIST, it can be hard to know what you are actually being asked to do.

They are related in purpose: both help organisations manage cyber risk. But they are not interchangeable checklists. The Australian Signals Directorate's (ASD) Essential Eight is a focused set of eight mitigation strategies, supported by a maturity model. "NIST" can refer to several much broader US frameworks, including the NIST Cybersecurity Framework (CSF) and NIST Special Publication 800-53.

For a small Australian business, the practical question is not "Which framework is best?" It is: "What baseline controls are relevant to our risks, and what implementation effort can we sustain?"

What is the Essential Eight?

The Essential Eight is a set of mitigation strategies developed by ASD, Australia's national signals intelligence and cyber security agency. The Australian Cyber Security Centre (ACSC), which is part of ASD, provides cyber security guidance and publishes material on the strategies and their implementation.

The Essential Eight is designed to reduce the likelihood and impact of common cyber incidents, including malware and ransomware attacks. It focuses mainly on securing Windows computers, applications, user privileges, authentication and backups. That makes it particularly relevant to businesses running Microsoft Windows and Microsoft 365—but it does not cover every part of a business's security program.

Each strategy has maturity levels from 0 to 3. These describe how consistently and effectively the controls are implemented. The levels are not a simple pass/fail score, nor do they automatically prove that an organisation is secure. A business should choose a target based on its threat exposure, customers, regulatory obligations and capacity to implement and maintain controls.

It is worth being precise when describing your position. "We are basically Level Two" is not a useful assurance claim. Say which maturity level you have assessed, for which strategies, against which version of the guidance, and what gaps remain.

What does "NIST" mean?

NIST is the US National Institute of Standards and Technology. It publishes many standards and guidance documents, so a questionnaire that says "Do you follow NIST?" is incomplete unless it identifies the specific framework or publication.

- **NIST Cybersecurity Framework (CSF):** A flexible way to organise cyber risk management around outcomes such as identifying, protecting, detecting, responding and recovering. It can suit organisations of different sizes and sectors.
- **NIST SP 800-53:** A large catalogue of security and privacy controls, commonly used in US government and higher-assurance environments.
- **NIST SP 800-171:** A set of requirements for protecting certain types of controlled information in non-federal systems, particularly in US government supply chains.

These are not three names for the same checklist. Before answering a supplier questionnaire, ask which NIST publication, version and assessment method the customer means. "NIST compliant" is not a meaningful claim on its own.



Essential Eight vs NIST: the practical difference

Question Essential Eight NIST frameworks What is it? Eight mitigation strategies with a maturity model. A family of frameworks and control publications; the scope depends on which one is specified. Typical focus Practical controls that reduce common attack paths, especially on Windows environments. Risk management outcomes or extensive control requirements, depending on the publication. How is progress described? Maturity Levels 0–3 for each strategy. Varies. CSF uses outcomes and profiles; other publications use control requirements and assessment methods. Useful for a small business when… You need a clear Australian baseline and a way to prioritise core technical controls. A customer, regulator or contract names a particular NIST framework, or you need a broader risk-management structure.

The Essential Eight can be a practical starting point for improving technical safeguards. NIST CSF can help structure a wider program, including governance, incident response and recovery. A business may use both: for example, the Essential Eight to drive specific technical work and NIST CSF to organise responsibilities and risk discussions.

Neither framework should be treated as a guarantee against compromise. Nor does adopting one automatically satisfy every legal, contractual or insurance requirement.

Are you required to adopt the Essential Eight?

For many small businesses, adopting the Essential Eight is not a blanket legal requirement. Requirements depend on the business's industry, the information it handles, applicable Australian laws and regulations, and the terms of its contracts. Some government or regulated environments may set specific requirements. A supplier agreement may also impose controls that go beyond a general baseline.

Even where adoption is voluntary, market pressure can make it expected in practice. Common sources include:

- **Cyber insurance forms:** Insurers may ask about MFA, backups, patching, privileged access and endpoint protection. A positive answer should reflect a control that is enabled and maintained—not a plan or a capability you have not tested.

- **Supplier questionnaires:** A large client may ask for evidence of security controls or a named framework. Its answers can affect onboarding, contract renewal or access to customer systems.
- **Tenders and procurement:** Government buyers and larger organisations may require security attestations, documented policies or evidence that risks are being managed.
- **Customer expectations:** Accountants, engineering firms and hospitality groups may hold payroll, financial, design or customer data that clients expect them to protect.

Answer questionnaires carefully. If asked whether backups exist, ask **australian signals directorate ASD** yourself: **can you restore it?** A backup that has never been restored is an assumption, not proven recovery capability.



The eight strategies in plain language

1. ### Application control

   Allow only approved software to run on computers where it is practical to do so. This can stop unauthorised or malicious programs, but requires a process for approving legitimate business applications and updates.

2. ### Patch applications

   Keep applications—especially internet-facing and commonly targeted software—up to date. Browsers, PDF readers and business applications need an owner and a repeatable update process. Patching is inconvenient, but leaving known vulnerabilities open is not a sustainable shortcut.

3. ### Configure Microsoft Office macro settings

   Restrict macros from untrusted sources and allow only those that are genuinely needed and appropriately controlled. A business should not leave risky macro behaviour enabled simply because “someone might need it”.

4. ### User application hardening

Reduce risky features in everyday applications—for example, block or limit content and behaviours that attackers commonly abuse. The aim is to make routine browsing and document handling less hazardous without disrupting essential work.

5. **Restrict administrative privileges**

   Give people standard user accounts for everyday work and separate, tightly controlled admin accounts for tasks that need them. Remove unnecessary administrator access and review who still needs it. Convenience is not a good reason to leave admin rights on for everyone.

6. **Patch operating systems**

   Keep Windows and other supported operating systems current, and replace systems that have reached end of support. Define how quickly important updates are applied, how exceptions are approved and who checks that devices are actually compliant.

7. **Multi-factor authentication (MFA)**

   Require more than a password to access important systems. Prioritise administrator accounts, email, remote access and cloud services such as Microsoft 365. MFA reduces the value of a stolen password, although it does not eliminate phishing or account takeover risk.

8. **Regular backups**

   Back up important information and systems, protect backup access from ordinary user accounts and test restoration. Decide how much data loss and downtime the business can tolerate, then check that the recovery process meets those needs. Confirm who can initiate a restore and how long it takes.

What does implementation effort look like for an SMB?

Implementation effort depends less on headcount than on how consistently the business manages its devices, identities and data. A small office with a standard Windows build and centrally managed Microsoft 365 environment may be able to roll out several controls efficiently. A business with old equipment, specialist software, shared logins or many unmanaged devices will need more preparation.

Control area Common effort or obstacle Practical first step MFA and admin access Finding exceptions, old accounts and business processes tied to shared credentials. Inventory accounts, protect administrator access, then enable MFA for all users with a managed exception process. Patching and application control Unmanaged devices, specialist applications and concern about business disruption. List devices and software, assign an owner, test updates on a small group and track exceptions with expiry dates. Macro settings and hardening Legacy spreadsheets or workflows that rely on macros or older features. Identify what is genuinely required, test safer settings and replace unsupported workflows where possible. Backups Unclear recovery priorities or backups that are accessible from compromised accounts. Identify critical data, protect backup access and schedule a documented restore test.

Do not try to claim maturity across all eight strategies before you know what is installed, managed and working. Start with an inventory of devices, users, applications and critical data. Then assess the current state, choose a realistic target and prioritise the gaps that present the greatest risk.

A sensible approach to frameworks and questionnaires

1. **Clarify the request.** Ask which version, maturity level, NIST publication or evidence standard the customer expects.
2. **Assess what is in place.** Check configuration and coverage—not just whether a licence or product is available.
3. **Prioritise baseline controls.** Start with high-impact gaps such as MFA, unpatched systems, excessive admin access and untested backups.
4. **Document exceptions.** Record why a control is not yet implemented, the risk, the owner and a review date.
5. **Keep evidence.** Retain policies, configuration records, update reports, access reviews and restore-test results that support questionnaire answers.

The bottom line

For a small Australian business, the Essential Eight offers a focused set of baseline controls and a maturity model that can help turn cyber security into practical work. NIST is broader, but you need to know which NIST framework a customer means before comparing it or claiming alignment.

Neither label replaces good operational habits. Keep systems patched, remove unnecessary administrator access, use MFA, and test your backups. If an insurer or client asks for a framework claim, be specific about what you have assessed and what remains. Honest, evidence-backed answers are more useful than saying you are “basically Level Two”.