Engineering firms handle more than drawings. Their systems may contain project plans, building and infrastructure details, cost estimates, client contact information, intellectual property and, in some cases, data about sensitive sites. That makes cybersecurity a practical business issue: a compromised account or unavailable file server can disrupt project delivery and affect clients as well as your own team.

When a client, insurer or prospective project partner asks about your security, the Australian Cyber Security Centre's Essential Eight is likely to come up. The questions may appear in a cyber insurance form, tender, contract review or **supplier questionnaire**. They may ask whether you "meet the Essential Eight", what **essential eight maturity level 1** means, or how you protect **client data**.

This guide explains the framework in plain language, what clients commonly want to know, and how an engineering firm can answer without making promises it cannot support.

What is the ASD Essential Eight?

The Essential Eight is a set of eight mitigation strategies published by the Australian Signals Directorate (ASD), through the Australian Cyber Security Centre (ACSC). It is intended to help organisations reduce the risk of common cyber attacks, especially attacks that target Windows computers and business networks.

The strategies are grouped into a maturity model. The model describes how consistently and effectively an organisation has implemented each strategy. Maturity Level 0 indicates limited implementation; Levels 1, 2 and 3 represent progressively stronger controls against more capable threats. The appropriate target depends on the organisation's risks, obligations and operating environment.

The Essential Eight is guidance, not a universal certification or a guarantee that an organisation is secure. A firm should not say it is "certified Essential Eight" unless it holds a specific, valid certification that actually supports that claim. In most client discussions, it is more useful to explain which controls are in place, how they are applied and what evidence is available.

Why do small and medium-sized firms keep hearing about it?

Many SMBs do not have a regulatory requirement to implement a particular Essential Eight maturity level. They still encounter it because clients and insurers use the framework as a practical shorthand for basic cyber controls.

- **Cyber insurance forms** may ask about multi-factor authentication, backups, privileged access, patching and endpoint protection. Some questions resemble Essential Eight controls, although an insurer's requirements are its own and may not map neatly to a maturity level.
- **Supplier questionnaires** can ask whether your business follows ASD or ACSC guidance, whether you have a target maturity level, and how you protect information shared by the client.
- **Tenders and contracts** may include security requirements, especially for government work, critical infrastructure, large construction projects or work involving sensitive client information.
- **Large clients** may assess suppliers because a supplier's compromised account or system can create a route into project data or business processes.

So adoption may be voluntary in a legal sense but expected in a commercial one. If a contract requires specific controls, those requirements are not optional for that engagement. Read the wording carefully: a

client asking for “alignment with the Essential Eight” may mean something different from one requiring a defined maturity level or a formal assessment.



The eight strategies in plain language

The Essential Eight focuses on controls that help prevent common attack paths and limit the damage if an attacker gets in. For an engineering firm, implementation should account for specialist design applications, project workflows, remote access and any equipment or systems that cannot be changed without testing.

Strategy What it means in practice An engineering-firm consideration Application control Control which software can run, rather than allowing any downloaded program to execute. Test controls against CAD, modelling, estimating and specialist engineering tools before broad deployment. Patch applications Apply security updates to business software and browsers within defined timeframes. Track third-party tools and confirm updates do not break plugins, licences or project workflows. Configure Microsoft Office macro settings Restrict risky macros, particularly those arriving from untrusted sources. Identify any legitimate macro-dependent templates and manage exceptions rather than leaving macros broadly enabled. User application hardening Reduce risky features in applications, such as web browsers and document readers. Apply secure settings to the tools staff use to open drawings, PDFs, emails and shared project documents. Restrict administrative privileges Give users only the access they need, and keep everyday accounts separate from admin accounts. Engineers generally should not have permanent local administrator rights just because installing software is convenient. Patch operating systems Keep supported operating systems updated and address security vulnerabilities promptly. Plan updates for workstations, servers and remote devices; investigate unsupported systems and document any exceptions. Multi-factor authentication (MFA) Require an additional proof of identity, not just a password, when users sign in. Prioritise email, Microsoft 365, remote access and administrator accounts, then check coverage and exceptions. Regular backups Keep protected copies of important data and systems so they can be recovered after loss, damage or ransomware. Include project files, key business systems and configuration information, and test recovery—not just backup jobs.

What clients usually ask in supplier questionnaires

Questionnaires vary, but the same practical themes come up repeatedly. A client may ask for a yes/no response, a maturity-level selection or a short explanation. Before answering, check exactly what the question refers to: all systems, a particular project environment, or only the systems that access client data.

“Do you follow the Essential Eight? What maturity level are you?”

Be precise. If you have not completed an assessment https://www.techguide.com.au/news/computers-news/the-essential-eight-explained-for-small-and-medium-australian-businesses/ against the ASD maturity model, do not imply that you have. You can explain that you are assessing the controls, state your target if one has been formally chosen, and describe the current evidence. **Essential eight maturity level 1** is a common reference point for organisations building a baseline, but it is not a magic label or proof that every risk has been addressed.

“How do you protect our data?”

Describe controls that apply to the relevant systems: access restrictions, MFA, secure sharing, device protection, patching, backups and staff processes. Explain where client data is stored and who can access it. If you use cloud services or subcontractors, be ready to describe how access and responsibilities are managed. Avoid claiming that all information is “fully secure”; security depends on the systems, configurations and operating practices in scope.

“Do you have MFA and restricted administrator access?”

Give a coverage-based answer rather than a broad assurance. For example, state which accounts and services require MFA, how exceptions are approved, and whether administrator accounts are seperate from everyday user accounts. Name the setting or control where possible. “We use MFA” may conceal gaps in older applications, remote access or privileged accounts.

“Are your systems patched, and how quickly?”

Clients want to know that patching is routine, monitored and not left until a convenient day that never arrives. Explain how you identify missing updates, set priorities and handle systems that need testing before changes are applied. Engineering software can have compatibility constraints, but that is a reason to manage and document exceptions—not to ignore patching indefinitely.

“Can you restore your backups?”

“We have backups” is only the start of the answer. Can you restore it? Be prepared to say what is backed up, how recovery is tested, who can access or delete the backup copies, and how often tests occur. A successful backup job does not prove that a usable project file, server or business system can be recovered in the time your work requires.

How to prepare credible answers

1. **Confirm the scope.** Identify the systems, users, locations and client information covered by the question. Do not assume a control applies everywhere if it only covers some devices.
2. **Check the evidence.** Useful evidence may include configuration reports, patch records, MFA coverage, access reviews, backup logs and documented restore-test results. Keep sensitive technical details out of a general questionnaire unless they are requested through an appropriate channel.

3. **Be honest about exceptions.** Record why a system is excluded, who accepted the risk, what compensating measures exist and when the exception will be reviewed.
4. **Separate current state from planned work.** Write “in progress” or give a target date where appropriate. Do not describe a future control as if it is already operating.
5. **Align answers with contracts and insurance.** Check wording, renewal declarations and client commitments. Inaccurate answers can cause problems even if they were intended as shorthand.

Choosing a sensible starting point

For an SMB engineering firm, a practical first step is to establish what devices and systems exist, who has administrative access, whether MFA is consistently enabled, and whether operating systems and applications are being patched. Then review how project data is shared and backed up, including whether recovery has been tested.

Consider specialist engineering software and any operational technology separately. A control that is straightforward on a standard office laptop may need testing or a managed exception on a workstation tied to a licensed tool, test rig or production process. Keep exceptions limited, assigned to an owner and revisited as systems change.

Essential Eight work is not a one-off questionnaire exercise. Staff join and leave, software changes, new projects introduce new data flows, and vulnerabilities continue to appear. Assign responsibility for reviewing controls and keep evidence current enough that you can answer a client’s question without guessing.. Pretty simple.

Conclusion

Clients usually ask about the Essential Eight because they want confidence that a supplier can protect shared information and keep work moving after a security incident. Insurance forms and supplier questionnaires may use the framework as a reference, but their specific requirements still need to be read on their own terms.



Answer with evidence, describe the scope, and distinguish what is implemented from what is planned. Whether you are working towards **essential eight maturity level 1** or simply responding to a client’s

controls checklist, clear answers about patching, access, MFA, application controls and tested backups are more useful than a vague claim of compliance. That is the foundation of credible **client data protection**—and a much stronger response to the next supplier questionnaire.