Retiring an unsupported Windows computer is rarely as simple as replacing it on a Friday afternoon. It may run the software that handles payroll, bookings, production equipment or a client's specialist workflow. The aim is to move users and services to supported systems with as little disruption as practical—not to promise zero downtime when a business-critical application or device may need testing.

regular backups restore test

A safe change starts with an inventory, a tested migration path and a rollback plan. It also helps to understand why customers, insurers and suppliers are asking about the ASD Essential Eight—and what those questions do, and do not, require of your business.

Why do small businesses keep hearing about the Essential Eight?

The Essential Eight is a set of eight mitigation strategies published by the Australian Signals Directorate (ASD), through its Australian Cyber Security Centre (ACSC). It is intended to help organisations reduce common cyber risks, particularly those associated with malicious software and compromised accounts. The strategies are useful as a practical security baseline, not a complete security programme.





SMBs often meet the Essential Eight through market pressure rather than a law that applies to every business. You may see it in a cyber insurance form, a supplier questionnaire, a tender, or a large customer's security requirements. A customer may ask whether you patch operating systems, use multi-factor authentication or work towards a particular maturity level.

Answer those questions accurately. The Essential Eight has maturity levels, and a broad statement such as "we are basically Level Two" is not a useful assessment. If a form asks for a level, you need evidence against the relevant requirements and scope. A small business can use the strategies without claiming a formal maturity level.

Voluntary, expected and required are not the same thing

For many Australian SMBs, adopting the Essential Eight is voluntary. However, a contract, tender condition, customer policy or insurance term can make particular controls an expectation—or a contractual requirement—for that relationship. Separate legal or regulatory obligations may also apply depending on your industry and the information you handle.

Read the question and the terms carefully. An insurer's question is not automatically proof that a specific maturity level is legally mandatory, and a customer's requirement may apply only to the systems handling its data. Ask for clarification if the wording is unclear. Do not claim a control is in place just because you intend to implement it.

What are the eight Essential Eight strategies?

In plain language, the strategies aim to reduce the chance that an attacker can get in, run harmful code, take over an account or recover easily after an incident. They work best together; none is a substitute for the others.

Strategy What it means in practice Connection to retiring old Windows Application control Control which software is allowed to run, especially on higher-risk systems. Check that required applications are approved and can run under the replacement configuration. Patch applications Keep browsers, PDF readers and other applications updated, not just Windows. Confirm the replacement computer can run supported versions of the software your team needs. Configure Microsoft Office macros Limit risky macros and allow only

approved business use. Test macro-enabled spreadsheets and documents before moving users. User application hardening Reduce risky features and behaviours in commonly used applications. Apply the same protections to the new device instead of carrying forward insecure defaults. Restrict administrative privileges Give users only the access they need; keep routine work separate from admin tasks. Do not solve migration problems by leaving users permanently signed in as administrators. Patch operating systems Install security updates for supported operating systems promptly and consistently. Retire unsupported Windows versions and keep the replacement OS maintained. Multi-factor authentication (MFA) Require more than a password for access to important accounts and services. Make sure users can complete MFA on the new device and that recovery methods are documented. Regular backups Keep backups protected and test recovery, rather than assuming a backup job is enough. Back up the data and configurations needed for migration. Can you restore it?

Start with an inventory, not a mass upgrade

Before you plan to retire unsupported versions, find out what is actually running. Include desktops, laptops, servers, virtual machines and any specialist Windows devices that may be easy to overlook. Record the Windows edition and version, device owner, business purpose, location and whether it is still connected to the network.

Then identify dependencies. Ask which applications, printers, scanners, line-of-business systems, licences, peripherals and scheduled tasks rely on each device. For servers, include the services hosted there, who uses them, what connects to them and whether another system depends on them. An old computer under a counter may be supporting a critical process.

- Record the vendor and support status for each business application.
- Check whether the device meets the requirements for a supported Windows version.
- Confirm how data, settings, certificates and licences will be moved.
- Identify devices that cannot be upgraded, such as specialist equipment with vendor restrictions.
- Prioritise internet-facing systems, devices holding sensitive data and systems that cannot receive security updates.

Microsoft ended support for Windows 10 on 14 October 2025. A device still running it does not stop working, but it no longer receives standard security updates from Microsoft. Check the support lifecycle for the exact Windows edition and any extended support arrangement rather than relying on the device’s age or a familiar product name.

Build upgrade planning around business impact

Good upgrade planning separates devices into groups. A standard office laptop may be straightforward to replace. A server running an old accounting package or a Windows PC attached to a manufacturing machine may need vendor advice, a test environment or a longer-term replacement project.

1. **Set the target.** Choose a supported Windows version and hardware that can be maintained for the expected service life. Confirm that required applications and security settings are supported.
2. **Speak to vendors early.** Get written confirmation for specialist applications, peripherals and equipment. If a vendor says a system must remain on an unsupported OS, ask what supported alternative, isolation method or replacement schedule they offer.

3. **Test a representative device.** Trial the migration with a user and workload that reflect normal business use. Test printing, scanning, VPN access, file shares, macros, finance or booking software, backups and MFA.
4. **Move in small waves.** Start with a low-risk group, fix issues, then expand. Schedule changes outside peak periods where possible and tell staff what will change and where to get help.
5. **Keep a rollback route.** Define who can pause the rollout, how the previous service can be restored, and what data must be preserved. For a server migration, avoid switching off the old system until the new service has passed agreed checks.
6. **Remove the old system properly.** Once the replacement is confirmed, revoke old accounts and connections, remove the device from management and securely erase or dispose of it according to your process.

How to minimise downtime in practice

For a user's computer, a preconfigured replacement can reduce the time they are without a working device. Prepare the operating system, security settings, applications and access before the handover. Move data using a controlled method, then have the user verify their essential work. Keep the old device available for a defined, short transition period if that is safe and practical—but do not leave it connected indefinitely as a convenient fallback.

For servers and shared systems, plan the cutover around the service, not just the Windows installation. Depending on the application, options may include migrating to a supported server, moving a workload to a supported cloud service, replacing the application or running a temporary parallel service. Each option needs testing for performance, access, data consistency and recovery.

Backups are part of the plan, but a green backup status is not proof that a migration can be recovered. Identify what must be restored and test that process before making a major change. Can you restore the files, application data and configuration you actually need within an acceptable time? Record who performs the restore and how you would return to service if the new system fails.

What if the old system cannot be retired yet?

Sometimes a vendor dependency makes immediate replacement impractical. That is a risk to manage, not a reason to pretend the system is secure. Document the business owner, the reason it remains, the data it can access, and the planned retirement date. Get approval for the exception and review it regularly.

- Limit network access to only the systems and services the device needs.
- Remove unnecessary accounts and restrict administrative privileges.
- Block general internet access where it is not required for the business function.
- Use other available controls to monitor access and reduce exposure.
- Keep a funded replacement plan, with a named owner and milestones.

These measures reduce exposure; they do not make an unsupported Windows version equivalent to a supported, patched system. Check whether compensating controls meet the relevant customer, insurance or contractual requirement, and get specialist advice for high-risk systems.

Keep evidence for insurance forms and supplier questionnaires

When a cyber insurance form or supplier questionnaire asks about patching or unsupported systems, respond based on current evidence. Useful records include a device inventory, patching reports, the approved migration plan, test results, backup restore records and documented exceptions with review dates.

Be precise about scope. For example, state which device groups are covered, how quickly updates are applied, and whether any unsupported systems remain. If a control is only partly implemented, say so and describe the remediation plan. A clear, bounded answer is more credible than a blanket claim that every device is fully protected.

Retire unsupported Windows versions as a managed change

To retire unsupported versions without unnecessary downtime, know what each device does, confirm application compatibility, migrate in tested stages and define a rollback path. Keep the replacement operating system patched, restrict admin access, use MFA where appropriate, and test your backups rather than assuming they will work.

The Essential Eight gives Australian businesses a practical language for these improvements. It is not automatically compulsory for every SMB, but insurers, tender panels and larger customers may expect evidence of sound controls. A realistic upgrade plan—with owners, dates, tests and honest reporting—helps protect operations as well as your position in those conversations.