Short answer: not necessarily. Application control is often one of the harder Essential Eight strategies for a small or medium business to implement well, so it can make sense to tackle it after you understand your devices, users and software. But “leave it until last” is not a security plan. The right order depends on your risks, systems, business needs and the maturity level you are working towards.

Application control can stop unapproved software from running. It can also interrupt legitimate work if the rules are too broad, too strict or poorly tested. That is why **planning and testing** matter, and why a careful **allowlist setup** is usually safer than switching on a restrictive rule across every computer in one hit.

This guide explains what the ASD Essential Eight is, why businesses keep being asked about it, what the eight strategies mean in plain language, and how to decide when application control belongs on your roadmap.

What is the ASD Essential Eight?

The Essential Eight is a set of eight mitigation strategies published by the Australian Signals Directorate (ASD). The Australian Cyber Security Centre (ACSC), which is part of ASD, provides cyber security guidance and resources for Australian organisations. The strategies are intended to help reduce the likelihood and impact of common cyber threats, including malware, stolen credentials and attackers exploiting vulnerable systems.

The Essential Eight is not a complete cyber security program. It does not replace good identity management, staff training, incident response, secure cloud configuration or reliable backups. Nor is it a guarantee that an organisation cannot be breached. Think of it as a practical baseline of technical controls, supported by a maturity model that helps organisations describe how consistently those controls are implemented.



For a Windows and Microsoft 365 business, Essential Eight work often involves settings such as application control, Office macro restrictions, Windows security configuration, patching, multi-factor authentication and backup arrangements. The exact implementation depends on your environment. A one-office accounting

firm with a handful of standard laptops has different constraints from an engineering company using specialist design software or a hospitality group with shared point-of-sale devices.

Why do small businesses keep hearing about it?

Essential Eight has become a common reference point because it gives buyers, insurers and business leaders a recognisable way to discuss baseline cyber security. You may see it in **cyber insurance forms**, supplier questionnaires, tender requirements or a large customer's security assessment.

That does not mean every Australian business is legally required to reach a particular Essential Eight maturity level. Adoption is often voluntary in the general sense, but it can become an expectation in a specific commercial relationship. A government contract, a customer's supplier terms or an insurer's underwriting questions may require particular controls or evidence. Requirements vary, so read the actual wording rather than assuming "Essential Eight compliant" means the same thing everywhere.

Be especially careful with broad claims such as "we are basically Level Two". Maturity levels have defined requirements, https://www.techguide.com.au/news/computers-news/the-essential-eight-explained-for-small-and-medium-australian-businesses/ and an organisation should be able to explain what is implemented, where it applies, what is excluded and what evidence supports the claim. A questionnaire answer should describe the control honestly—for example, whether MFA is enforced for all remote access and cloud services—not simply name a framework.

The eight strategies in plain language

Strategy Plain-language purpose Application control Allow approved software to run and block unapproved or unauthorised programs. Patch applications Keep software such as browsers, PDF tools and business applications updated to fix known weaknesses. Configure Microsoft Office macro settings Restrict risky macros, particularly those delivered in files from untrusted sources. User application hardening Reduce risky features in browsers and other user-facing software that attackers commonly exploit. Restrict administrative privileges Give users only the access they need, and keep everyday accounts separate from administrator accounts. Patch operating systems Install supported Windows and other operating system security updates promptly and consistently. Multi-factor authentication Require an additional proof of identity, not just a password, for important accounts and access. Regular backups Keep protected, recoverable copies of important data and systems, and test that recovery works.

The strategies work as a set. Application control is less effective if attackers can use an administrator account to change its rules. Patching is less useful if devices are routinely left offline or unsupported. And backups are only useful if you can recover the data and systems you need in a time that suits the business. When someone says, "we have backups", the practical question is: **can you restore it?**

Why application control feels like a final step

Application control can be operationally demanding because it changes what software is permitted to run. Before you can safely restrict execution, you need a reasonable picture of what the business actually uses. That includes approved applications, installers, scripts, plug-ins, line-of-business tools and software that may run only occasionally.

This is where an allowlist setup can get tricky. A rule based on a publisher, a trusted location, a file path or a specific file hash has different security and maintenance trade-offs. A rule that is too broad may allow

unwanted software. A rule that is too narrow may block a legitimate update or a specialist application. The business impact is not theoretical: staff may be unable to process invoices, open project files or use a point-of-sale system.

Application control also relies on sound administration. If too many users have local administrator rights, they may be able to bypass restrictions or install software outside the intended process. If nobody owns application approvals, exceptions can accumulate until the control becomes difficult to understand and maintain.

That is why application control is often scheduled after foundational work such as asset discovery, patching, removal of unnecessary administrator rights and a review of how software is installed. This is a practical sequencing choice—not a rule that application control must always be the eighth or final task.

So, is application control the last thing I should do?

For many SMBs, it is sensible to **plan application control early and enforce it in stages**. Waiting until the end to think about it can create avoidable surprises: you may discover that a critical application is unsupported, no one knows who maintains it, or the only person who can approve software is on leave.

On the other hand, rushing straight to restrictive enforcement can cause outages. The goal is not to turn on a setting simply to tick a box. The goal is to establish a control that reduces risk without creating an informal workaround, such as staff sharing administrator passwords or using personal devices to get work done.

Consider your risk and obligations. If a customer contract, tender or insurer specifically asks about application control, confirm what they mean and what evidence they expect. Some questions may ask whether the control exists; others may ask about coverage, exceptions or a particular maturity level. Answer the question actually asked. If the control is planned but not yet enforced, say so and provide a realistic date or interim measure where appropriate.

A practical path to application control

1. **Define the scope.**

   List the devices that matter: staff laptops, desktops, servers and any special-purpose endpoints. Identify devices that may need a different approach, such as engineering workstations or point-of-sale terminals. Record exclusions and the reason for each one.

2. **Understand your software.**

   Use device inventories and software records to identify what is installed and who relies on it. Ask department leads about less frequent tasks and specialist tools. Confirm that critical applications are supported and that someone is responsible for updates.

3. **Review how software gets installed.**

   Agree who can request and approve software, how updates are handled, and how urgent exceptions are authorised. Avoid a process that depends on one person remembering to approve every routine update.

4. **Choose the control design.**

   Match the policy method to your systems and management capability. Decide how you will handle trusted publishers, approved directories, scripts, updates and exceptions. Document why the rules are appropriate; do not assume a single rule fits every device.

5. **Test before broad enforcement.**

   Start with a representative pilot group and observe what would be blocked. Include different job roles and any specialist applications. Check logs, resolve false positives and confirm that normal work still functions before expanding the rollout.

6. **Roll out in stages.**

   Move from a small pilot to larger groups, with a clear support contact and a way to handle legitimate business-critical issues. Keep emergency changes controlled and reviewable. Do not let “temporary” exceptions become permanent without an owner and review date.

7. **Maintain and review.**

   Review policy changes, exceptions, new software and device coverage regularly. Keep evidence of testing and approvals. Revisit the design when the business changes, not just when an insurance renewal form arrives.

How application control fits into the wider plan

There is no universal order that suits every organisation, but a sensible roadmap usually starts with visibility and basic hygiene. Know which devices and accounts you have. Remove unnecessary administrator access. Turn on MFA for important accounts and remote access. Establish a reliable patching process for operating systems and applications. Review Office macro settings and harden browsers. Confirm that backups are protected and recovery has been tested.



Then build application control on a clear understanding of approved software and support processes. Some work can run in parallel: for example, you can inventory applications while improving patching. If your threat profile or a customer requirement makes application control urgent, bring it forward—but keep the pilot and testing stages. “Urgent” does not mean “skip change management”.

Also be realistic about the level of effort. Essential Eight maturity is not achieved by installing one product or switching on one policy. It requires the right controls to be implemented across the relevant systems,

operated consistently and supported by processes. If you outsource IT, ask the provider which settings they manage, which devices are in scope, how exceptions work and what evidence they can supply.

What to say on a supplier questionnaire or insurance form

Be specific and evidence-based. A useful response may explain that application control is being piloted on a named device group, describe the planned expansion and identify any documented exclusions. If it is not implemented, do not imply that it is. Where the question is ambiguous, ask the insurer, broker, customer or tender contact what scope and level they expect.

Keep evidence that matches the claim: policy configuration, device coverage, exception records, test results and approval history. The same principle applies to patching, MFA and backups. A policy document alone does not prove that the control is working across every relevant device.

Conclusion: plan it early, enforce it carefully

Application control is not automatically the last Essential Eight strategy to implement. It is, however, a control that benefits from careful preparation because poor rules can disrupt work and weak exception handling can undermine the result. Start planning early, understand your applications and dependencies, and use a measured allowlist setup with **planning and testing** before broad enforcement.

Work through the Essential Eight as a practical risk-reduction program, not a badge. Be clear about what is implemented, what remains, and where the gaps are. That will give you a more useful answer to a customer questionnaire or cyber insurance form—and a better chance of keeping both your systems and your business running.