



Essential Eight Maturity Level 3 in practice

Level 3 on all eight strategies, and the order to follow: identity and backups first, application control last, and every control read back from the system that enforces it.



Entity	Black Shard Pty Ltd · ABN 66 696 910 773
Document ID	BS-RPT-03
Classification	Public
Version	1.1
Published	26 October 2026
Figures	Assessed 24 Sep 2026

Executive summary

Essential Eight Maturity Level 3 across all eight strategies. Assessed on 24 September 2026, with each rating read back from the system that enforces it.

Level 3 is the top of the Essential Eight Maturity Model, aimed at adversaries who adapt their methods and will invest in a specific target. Reaching it is a matter of order and discipline more than budget: identity and backups first, administration next, application control last, and every control read back from the system that enforces it.

ASD launched ASD Essentials on 15 October 2026 as the Essential Eight's successor; ASD maps every strategy to an Essentials principle, so this record carries across as the transition baseline.

The controls are watched by the same monitoring that reads our scale figures. Our security monitoring analysed its first 430 million security events from 1 October to 26 October 2026, counted at 00:45 AEST.

- Start with phishing-resistant sign-in and backups an administrator cannot delete: they are the fastest controls to put in and they stop the most damage.
- For a firm working toward Level 3: run application control in audit, then enforce once the audit is quiet.
- Measure each control on the live system, never from the policy document, and give each one a check that runs every day.

Method

The ASD Essential Eight Maturity Model rates each of eight mitigation strategies from Level 0 to Level 3. Overall maturity is the lowest level reached across all eight, so Level 3 means no strategy sits below it.

Assessed on 24 September 2026, with each rating read back from the system that enforces it. A rating is the configuration as the enforcing system reports it, with its mode and its assignment, never the policy document that describes it. Client environments are assessed separately, under their own engagements.

The same method is the one a reader applies at home: for each strategy, name what the control stops, find the system that enforces it, read the setting back from there, and give it a check that runs every day.

The record, strategy by strategy

THE EIGHT STRATEGIES ON OUR OWN ESTATE



Every strategy is held at Maturity Level 3, and each has a running check that keeps it there. Source: Essential Eight Maturity Level 3, assessed 24 September 2026.

Application control

In place. Application control runs on every managed device under an allowlist, enforcing with code integrity, so a program that is not on the list does not run.

Kept. A daily check confirms that the enforcing policy has not slipped back to audit, has not lost code integrity and has not lost its assignment.

Patch applications

In place. Security patches apply unattended on our servers, and office applications update on a managed channel under tenant policy.

Kept. Every internet-facing host is scanned for vulnerabilities every day.

Configure Microsoft Office macro settings

In place. Tenant policy blocks macros from the internet, disables trusted locations and blocks trusted locations on the network for every licensed user. Attack surface reduction rules stop Office macros calling Win32 APIs, stop

Office applications creating child processes or executable content, and stop them injecting code into other processes.

Kept. The policy is read back from the system that enforces it at each assessment, with its assignment.

User application hardening

In place. Attack surface reduction rules run in block mode on every managed device. Browsers run hardening baselines, antivirus runs with real-time and tamper protection, credential protection and the host firewall are on, and script and component logging are on.

Kept. Every block the rules make is logged centrally, and the rule set is read back at each assessment.

Restrict administrative privileges

In place. Administrative identities are separate from daily accounts. Privileged roles are activated just in time, and every activation needs phishing-resistant multi-factor authentication. Local administrator passwords are escrowed and rotated on managed devices. Administrative portal access is governed by the sign-in policy, and privileged access events are forwarded to central logging.

Kept. Credential vault ownership and rotation are tracked.

Patch operating systems

In place. Critical operating system updates reach our hosts within 48 hours. Managed devices run an update ring with an expedited path for out-of-band security releases.

Kept. Every managed device reported encrypted at the assessment.

Multi-factor authentication

In place. Phishing-resistant multi-factor authentication is enforced over every user and every cloud application, with stricter policy over administrators and privileged role activation. Legacy authentication is blocked. Hardware security keys are registered on the administrative accounts. Password-only access is gone.

Kept. The policies run in enforcing mode, and the exceptions list is read at each assessment.

Regular backups

In place. Backups run on a schedule with an off-site copy. The off-site backup copy is held under an immutability lock that no administrator can delete or shorten.

Kept. A daily test restores real data from the off-site copy and checks that the expected snapshots are present. Backup freshness is watched on its own.

What each control stops, and where to read it back

A control counts when the system that enforces it says so. For each strategy, the attack it stops and the record a

reader pulls from their own systems to prove the control is on.

STRATEGY	WHAT IT STOPS	READ IT BACK FROM
Application control	Unapproved programs, scripts and installers running at all	The enforcing policy, its mode and its assignment, with the block log
Patch applications	Exploitation of known flaws in browsers, office suites and services	The update policy and the daily vulnerability scan result
Configure Microsoft Office macro settings	A document that runs code when it is opened	The macro policy and the users it is assigned to
User application hardening	Office, browsers and scripts being used to launch the next stage	The rule set, its mode on each device, and the central block log
Restrict administrative privileges	A stolen daily account carrying administrator rights	The privileged role list, its activation records and the exceptions
Patch operating systems	Exploitation of the operating system and privilege escalation	The update schedule and the last applied patch on each device
Multi-factor authentication	A stolen password being enough to sign in	The sign-in policy in enforcing mode, and every account excluded from it
Regular backups	Ransomware ending the business	The immutability lock on the off-site copy and the last restore test

The read-back column is what an assessor asks for. A policy document on its own rates Level 0.

What each control costs

The controls do not cost the same. Multi-factor authentication, the macro policy and the backup immutability lock go in within days, because each is a policy applied to an estate that already has the accounts and the storage.

Restricting administrative privileges takes longer, because every administrator needs a second identity and every task that used a standing role has to work with just-in-time activation.

Application control takes the longest. An allowlist has to admit every legitimate program before it can block the rest, so it runs in audit while the records are read, the publishers the firm trusts are added, and the software the firm builds is signed. Only then does it enforce.

The running cost at Level 3 is mostly automation: the daily enforcement check, the daily vulnerability scan, the update schedule and the daily restore test. A person reads their results, which is a short task on a quiet day.

What the controls stop

Each block is a program, a script or an action that tried to run and did not: an Office document trying to start a process, a script fetched from the internet, an unsigned tool copied onto a laptop, a stolen password presented without the key. Most are mundane. Their value is that the same rules stop the first step of an intrusion without anyone deciding to, at any time of day the attempt is made.

Every block is written to central logging with the device, the user and the rule, so a pattern shows up and can be investigated. Central security monitoring of every system we run, with immutable log retention. Our security monitoring analysed its first 430 million security events from 1 October to 26 October 2026, counted at 00:45 AEST.

What to do

For a firm working toward Level 3, the order to follow:

1. Enforce phishing-resistant multi-factor authentication on every account and block legacy authentication.
2. Lock the off-site backup copy so no administrator can delete or shorten it, and test a restore every day.
3. Give administrators separate identities and make privileged roles something they activate for a task.
4. Block macros from the internet and turn on the attack surface reduction rules in block mode.
5. Patch on a written schedule, with critical updates on the shortest clock you can hold.
6. Run application control in audit, read the records, sign your own software, and enforce when the audit is quiet.
7. Read every control back from the system that enforces it, and give each a check that runs every day.

We run the same assessment for clients: all eight strategies rated against the ASD maturity model, read from the live systems, with a written report and an uplift plan sequenced by risk and effort. The uplift is delivered in the order above, with each control read back at the end. Scope and price are at blackshard.com.au/essential-eight-assessment.

Our record

Black Shard builds and defends the systems Australian organisations run on. The estate assessed here is the one we run every day, and it carries the same record we ask of our suppliers.

- SMB1001:2026 Gold, issued by CyberCert, valid 16 Jun 2026 to 17 Jun 2027, on the CyberCert register.
- Essential Eight Maturity Level 3, assessed September 2026.
- Pre-qualified supplier to Queensland councils under Local Buy arrangement LB308, ICT Solutions, Products, Services and New Technologies.
- Prequalified supplier under the NSW Government ICT Services Scheme (SCM0020).
- Holder of Victorian Fair Jobs Code pre-assessment certificate FJC-261023-11119, required for Victorian Government threshold and high-value procurement.
- Our CISO holds the Exemplar Global ISO/IEC 27001:2022 Lead Auditor credential.
- Professional indemnity, public liability, cyber and workers' compensation insurance, all current.
- More than 65,000 tests across our repositories, counted on 26 October 2026.
- More than 1,500 deploys and releases shipped since 1 January 2026.

24/7 incident line: 1800 370 270. The evidence behind each line goes out on request to info@blackshard.com.au.

Sources

- Australian Signals Directorate, Essential Eight Maturity Model: <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight>
- Essential Eight Maturity Level 3, assessed 24 September 2026 (evidence on request)
- The running tally of our scale figures, measured 26 October 2026 at 00:45 AEST