



ESSENTIAL EIGHT (AUSTRALIA) EVIDENCE

Contoso Legal LLP

PREPARED BY

Harbour IT

DATE

12 October 2026

EVIDENCE DATE

12 Oct 2026

SCHEME

Australian Signals Directorate

MICROSOFT 365 TENANT

contoso.onmicrosoft.com

● Not ready

Contoso Legal LLP has 3 controls to fix before reaching Maturity Level One.

IN THIS REPORT

Summary	2
Fix these first	2
Prevent malware running	3
Limit the extent of incidents	4
Recover data and availability	7
About this evidence	7

Summary

Contoso Legal LLP has 3 controls to fix before reaching Maturity Level One.

The eight strategies at Maturity Level One: admin privileges, operating system patching and MFA judged from Microsoft 365, the rest as text to complete from Intune or Group Policy.

5 controls need evidence Microsoft 365 can't show (firewalls, patch timing, anti-malware settings and processes): each has a text to complete.

8 controls



0 Pass 3 Fail 5 Your evidence

Fix these first

An assessor won't accept a gap in these. Each one names the accounts or settings behind it and the fix.

1 5 Restrict administrative privileges

1 guest with admin roles. Fix: Remove admin roles from guest accounts.

2 6 Patch operating systems

3 of 19 Windows computers past end of support. Fix: Upgrade computers on Windows 10 or an old Windows 11 release to the current Windows 11 release.

3 7 Multi-factor authentication

Enforced by CA002 — All users: Require MFA, with 1 exclusion to review. Fix: Create a Conditional Access policy requiring MFA for all users and all cloud apps, or turn on Security Defaults if the tenant has no Entra ID P1.

Prevent malware running

● Your evidence

Only approved programs run, applications are patched, Office macros are controlled and applications hardened.

1 Application control

● Your evidence

Only approved programs, scripts and installers can run on workstations, including from user folders.

Text to paste: Application control ([App Control for Business, AppLocker or product]) lets only approved programs, scripts and installers run on [workstations and servers], including from user profile and temporary folders. Blocked attempts are logged and reviewed by [team].

What Microsoft 365 can't show: All of this. Answer from Intune, Group Policy or the tool that sets it.

2 Patch applications

● Your evidence

Internet-facing services, browsers, Office, PDF software and email clients are patched promptly, and unsupported applications are removed.

Text to paste: Applications update automatically where they can (Microsoft 365 Apps, web browsers and [other software]). Updates that can't install automatically are applied within 14 days of release by [process or tool].

What Microsoft 365 can't show: All of this. Answer from Intune, Group Policy or the tool that sets it.

3 Configure Microsoft Office macro settings

● Your evidence

Macros are blocked for users who don't need them, macros from the internet are blocked, and users can't change the settings.

Text to paste: Microsoft Office macros are [blocked for all users, or allowed only for (group) from trusted locations or signed by a trusted publisher], macros in files from the internet are blocked, and users can't change these settings. This is set by [Intune or Group Policy].

What Microsoft 365 can't show: All of this. Answer from Intune, Group Policy or the tool that sets it.

4 User application hardening

● Your evidence

Browsers don't process Java or ads from the internet, and users can't change browser security settings.

Text to paste: Web browsers block Java and web advertisements from the internet and don't process them, Microsoft Office blocks OLE packages, PowerShell 2.0 is removed, and users can't change these settings. This is set by [Intune or Group Policy].

What Microsoft 365 can't show: All of this. Answer from Intune, Group Policy or the tool that sets it.

Limit the extent of incidents

● Fail

Admin privileges are few and separate, operating systems are patched, and everyone uses MFA.

5 Restrict administrative privileges

● Fail

Privileged access is validated when first asked for, limited to what's needed, held by separate accounts that don't read email or browse the web, and removed when it's no longer needed.

WHAT WE FOUND

- 2 Global Administrators.
- Cloud-only tenant: no accounts are synced from on-premises AD.
- Accounts holding privileged roles: 4
- Admins with no MFA policy: 1
- Admins with no MFA method registered: 2

GAPS

- 1 guest with admin roles.
 - g#EXT#@contoso.example: Guest holding Exchange Administrator
- 1 app with privileged roles.
 - Some app: App holding Exchange Administrator

Fix: Remove admin roles from guest accounts. If an external partner needs access, use GDAP or a member account in this tenant protected by MFA.

Text to paste: Most administrator accounts are separate from day-to-day accounts. There are exceptions. 1 of 2 admin accounts also has a licence or mailbox, so it looks like an everyday account: annabel.fraser@contoso.example.

What Microsoft 365 can't show: Judged from Microsoft 365 and Entra ID admin roles. Add local and server admins.

6 Patch operating systems

● Fail

Operating systems are patched promptly and versions no longer supported by the vendor are replaced.

WHAT WE FOUND

- But: 2 devices haven't checked in for 30+ days.
- Computers managed by Intune: 19
- Of which encrypted: 17
- Windows computers out of support: 3
- Reaching end of support within 90 days: 8
- Not compliant: 3

GAPS

- 3 of 19 Windows computers past end of support.
 - LAPTOP-CLARK13
(william.clark@contoso.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-JOHNSON04
(jacob.johnson@contoso.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-MARSH
(bobby.marsh@contoso.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - DESK-SMITH03
(megan.smith@contoso.example): Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.
 - DESK-WILSON12
(olivia.wilson@contoso.example): Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.
 - and 6 more

Fix: Upgrade computers on Windows 10 or an old Windows 11 release to the current Windows 11 release (Intune: Windows feature updates policy). Replace hardware that can't run Windows 11, or buy Extended Security Updates as a stopgap.

Text to paste: Managed Windows computers run versions of Windows that no longer receive security updates. 3 of 19 Windows computers past end of support.

What Microsoft 365 can't show: Judged from the Windows versions Intune reports. Add servers and devices it doesn't manage.

7 Multi-factor authentication

● Fail

Users authenticate with MFA to online services holding sensitive data, and admins use phishing-resistant MFA at higher maturity levels.

WHAT WE FOUND

- Blocked by "CA003 — Block legacy authentication".
- But: 2 admins without a phishing-resistant method.
- But: 3 people can only use a text or call as a second factor.
- Users with an MFA method registered: 80% of 20
- Accounts covered by an enforced MFA policy: 19 of 20
- Not covered: breakglass@contoso.example

GAPS

- Enforced by CA002 — All users: Require MFA, with 1 exclusion to review.
 - breakglass@contoso.example: Excluded from "CA002 — All users: Require MFA"
- 1 admin not covered by MFA.
 - breakglass@contoso.example: Global Administrator: excluded from CA001 — Admins: Require phishing-resistant MFA, CA002 — All users: Require MFA, CA003 — Block legacy authentication, CA004 — All users: Require compliant or hybrid-joined device, CA005 — Block sign-ins from disallowed countries, CA006 — Require MFA for Azure management, CA007 — Admins: No persistent browser, 8h sign-in frequency, CA008 — All users: 8h sign-in frequency, CA009 — Require MFA for device registration, CA010 — Insider risk: Step-up MFA, CA011 — High sign-in risk: Block

Fix: Create a Conditional Access policy requiring MFA for all users and all cloud apps, or turn on Security Defaults if the tenant has no Entra ID P1. Keep exclusions to break-glass accounts.

Text to paste: Multi-factor authentication (MFA) is enforced through Microsoft Entra ID for Microsoft 365 email and cloud applications, with exceptions. Enforced by Conditional Access ("CA002 — All users: Require MFA"), but with 12 exclusions to review: breakglass@contoso.example (break-glass), Application Administrator (role), Cloud Application Administrator (role), Conditional Access Administrator (role), Exchange Administrator (role), Global Administrator (role), Password Administrator (role), Privileged Authentication Administrator (role), Privileged Role Administrator (role), Security Administrator (role), SharePoint Administrator (role), User Administrator (role).

What Microsoft 365 can't show: Judged for Microsoft 365 sign-ins. Add other online services.

Recover data and availability

● Your evidence

Backups are taken, kept and tested, and can't be changed or deleted by ordinary accounts.

8 Regular backups

● Your evidence

Backups of data, applications and settings are made, kept, protected from change and deletion, and restores are tested.

Text to paste: Microsoft 365 data (Exchange Online mail, OneDrive, SharePoint and Teams) is backed up [daily] by [backup product or provider] to storage separate from Microsoft 365. Backups are kept for [retention period], are [immutable or offline], and use credentials separate from the Microsoft 365 administrator accounts. Restores were last tested on [date].

What Microsoft 365 can't show: Microsoft 365 doesn't back itself up for this purpose; describe the backup of Microsoft 365 too.

About this evidence

Maturity Level One is met only when all eight strategies meet it. Higher levels add requirements (such as phishing-resistant MFA and 48-hour patching) this pack doesn't judge.

Requirements: ASD Essential Eight Maturity Model, Maturity Level One. Strategies are ASD's, numbered in their usual order; requirements are paraphrased. Check the current maturity model on cyber.gov.au before an assessment.

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Pass and Fail are judged from Microsoft 365 settings and accounts read with read-only access; nothing was changed. The oldest data used was collected 12 Oct 2026, 06:36 UTC. Accepted risks are exceptions the organisation has reviewed and documented. Complete the [parts in brackets] before using a text.