



SOC 2 TRUST SERVICES CRITERIA EVIDENCE

Contoso Legal LLP

PREPARED BY

Harbour IT

DATE

12 October 2026

EVIDENCE DATE

12 Oct 2026

SCHEME

AICPA

MICROSOFT 365 TENANT

contoso.onmicrosoft.com

● Gaps to close

Contoso Legal LLP has 3 controls not in place.

IN THIS REPORT

Summary	2
Gaps to close	3
Control environment, risk and communication (CC1 to CC5)	4
Logical and physical access (CC6)	6
System operations and change (CC7 and CC8)	11
Risk mitigation and availability (CC9 and A1)	14
What the assessor checks	15
About this evidence	15

Summary

Contoso Legal LLP has 3 controls not in place.

The Trust Services Criteria Microsoft 365 gives evidence for, judged from the data, and text for the rest. Use it to prepare for a SOC 2 audit or answer a customer who holds one.

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

21 controls



 **0** Pass  **3** Fail  **7** Partly  **11** Your evidence

Gaps to close

The controls most likely to be queried, with the fix for each.

1 CC6.6 Protection from outside threats

Anyone, including anonymous links. Fix: Change SharePoint external sharing to "New and existing guests".

2 CC7.1 Vulnerabilities and configuration changes detected

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 CC9.2 Vendor and partner risk

Users can consent to any app. Fix: Set user consent to "Allow user consent for apps from verified publishers, for selected permissions" or turn it off and use the admin consent workflow.

4 CC6.1 Logical access security

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.

5 CC6.2 Access registered and authorised

Anyone, including guests, can invite guests. Fix: Restrict guest invitations to admins and the Guest Inviter role, or at least to members, under External collaboration settings.

6 CC6.3 Access based on role, removed when not needed

2 accounts inactive for 90+ days or never used. Fix: Disable accounts that haven't signed in for 90 days, or were created over 30 days ago and never used.

7 CC6.7 Transmission and movement of data restricted

3 external forwards. Fix: Remove forwarding to outside addresses unless the client has a documented business reason.

8 CC6.8 Malicious software prevented or detected

3 of 20 managed devices not compliant. Fix: Open each non-compliant device in Intune.

9 CC7.2 System components monitored for anomalies

1 suspicious inbox rule. Fix: Check each rule with the mailbox owner.

10 CC8.1 Change management

Any user can register an app. Fix: Set "Users can register applications" to No.

Control environment, risk and communication (CC1 to CC5)

● Your evidence

Oversight and accountability, competent and vetted people, policies, and risk assessment.

CC1.3 Structures, reporting lines and responsibilities

● Your evidence

Management sets structures, reporting lines and responsibilities for security.

Text to paste: [Name], [role], has overall responsibility for information security and data protection and reports to [the board or partners], where security is a standing agenda item. Day-to-day IT security is managed by [IT provider].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

CC1.4 Competent, vetted people

● Your evidence

People are checked before they join and trained for their responsibilities.

Text to paste: New staff go through [right-to-work, reference and DBS] checks before they get access, and sign [confidentiality agreements].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

CC2.2 Security responsibilities communicated

● Your evidence

Security responsibilities are communicated to staff, including through training.

Text to paste: All staff complete security awareness training [when they join and every year], through [training provider or platform]. Simulated phishing exercises run [monthly or quarterly] and the results are reviewed by [role].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

CC3.2 Risks identified and analysed

● Your evidence

Risks to the service's objectives are identified and analysed.

Text to paste: An information security risk assessment covering [scope] names an owner for each risk, the agreed treatment and an action plan. It was last reviewed on [date] by [name and role] and approved by [director or partner].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

CC5.3 Policies and procedures

● Your evidence

Control activities are set out in policies and put into practice through procedures.

Text to paste: Information security policies covering [acceptable use, access control, passwords, data protection and incident response] are approved by [role], reviewed every [12 months] and acknowledged by staff.

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

Logical and physical access (CC6)

● Fail

Access is authenticated and authorised, given and removed by process, data movement is restricted and devices are protected.

CC6.1 Logical access security

● Partly

Access to systems and data is protected by authentication: multi-factor for everyone, legacy protocols blocked, and data encrypted.

WHAT WE FOUND

- Blocked by "CA003 — Block legacy authentication".
- But: 2 admins without a phishing-resistant method.
- But: 2 of 19 computers not encrypted.
- 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
- SMTP AUTH is on for the organisation.
 - SMTP AUTH is allowed

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 the service's own systems.

CC6.2 Access registered and authorised

● Partly

New users and guests are registered and authorised before they're given access; old invitations go.

WHAT WE FOUND

- No stale guest invitations.

GAPS

- Anyone, including guests, can invite guests.
 - Guests can invite other guests

Fix: Restrict guest invitations to admins and the Guest Inviter role, or at least to members, under External collaboration settings.

Text to paste: New accounts are created only after a request from [manager or HR] is approved by [role], recorded in [ticket system].

What Microsoft 365 can't show: Microsoft 365 shows who can invite guests; describe how staff accounts are approved.

CC6.3 Access based on role, removed when not needed

● Partly

Access follows least privilege and is removed when people leave or change role; admin rights are few.

WHAT WE FOUND

- 2 Global Administrators.
- Accounts holding privileged roles: 4
- Admins with no MFA policy: 1
- Admins with no MFA method registered: 2

GAPS

- 2 accounts inactive for 90+ days or never used.
 - joseph.morris@contoso.example: Licensed member, last signed in 11 Jun 2026
 - g#EXT#@contoso.example: Guest, never signed in, created ?
- 1 disabled account still licensed.
 - bobby.marsh@contoso.example: Disabled, holding 1 licence
- 1 guest with admin roles.
 - g#EXT#@contoso.example: Guest holding Exchange Administrator

Fix: Disable accounts that haven't signed in for 90 days, or were created over 30 days ago and never used (after checking with the client), then remove their licences. Inactive accounts are a common foothold for attackers.

Text to paste: Access to files and systems is given through role-based groups, approved by [role], and changed when people move roles. [Access is reviewed every 12 months.]

What Microsoft 365 can't show: Judged from Entra ID sign-in activity and admin roles.

CC6.4 Physical access restricted

● Your evidence

Physical access to facilities and equipment is restricted to authorised people.

Text to paste: Offices are protected by [locked doors, access control and alarms]. [Servers and network equipment are kept in a locked room or cabinet.]

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

CC6.5 Data removed from disposed assets

● Your evidence

Data is removed from equipment before it's disposed of.

Text to paste: Before devices and storage are reused or disposed of, data is securely wiped [with an Intune wipe or a certified erasure tool] or the storage is destroyed by [certified disposal company], and the certificate is kept.

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

CC6.6 Protection from outside threats

● Fail

Access from outside is restricted: firewalls at the boundary and no open sharing.

GAPS

- Anyone, including anonymous links.
 - SharePoint and OneDrive: Anyone links are allowed
- 3 files and folders shared with anyone.
 - Campaign video.mp4 (Marketing / Documents): Anyone can edit
 - Brand assets (Marketing / Documents): Anyone can view, link never expires
 - holiday.jpg (OneDrive of annabel.fraser@contoso.example): Anyone can view

Fix: Change SharePoint external sharing to "New and existing guests" so every external person signs in. If the client relies on Anyone links, set them to expire and to view-only.

Text to paste: A [make and model] firewall protects the internet connection at [site]. Home and remote workers are protected by the software firewall on their company devices.

What Microsoft 365 can't show: Microsoft 365 shows its sharing; describe the network boundary.

CC6.7 Transmission and movement of data restricted

● Partly

Data moving outside is restricted and protected: no unnoticed forwarding, domains can't be spoofed.

WHAT WE FOUND

- The default outbound policy blocks automatic external forwarding.
- But: 1 of 1 mail domain doesn't fully enforce MTA-STS.
- But: 1 domain with SPF problems.
- But: 1 mail domain without DKIM.

GAPS

- 3 external forwards.
 - annabel.fraser@contoso.example: Mailbox forwarding to annabel.fraser@homemail.example (keeps a copy)
 - annabel.fraser@contoso.example: Inbox rule "Copy to home" forwards to annabel.fraser.home@homemail.example
 - oliver.hill@contoso.example: Inbox rule "Invoices to bookkeeper" forwards to bookkeeping@ledgerline.example
- 2 domains without DMARC enforcement.
 - contoso.example: DMARC is monitor-only (p=none); spoofed mail is still delivered
 - parked.example: Doesn't receive mail but has no DMARC p=reject record

Fix: Remove forwarding to outside addresses unless the client has a documented business reason. Forwarding is the most common way attackers keep reading a mailbox after a password reset.

Text to paste: Automatic forwarding to external addresses is restricted in Exchange Online, with exceptions. The default outbound policy blocks automatic external forwarding. But 3 external forwards found.

What Microsoft 365 can't show: Judged from Exchange Online forwarding and public DNS.

CC6.8 Malicious software prevented or detected

● Partly

Unauthorised or malicious software is prevented or detected on managed devices.

WHAT WE FOUND

- 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 20 managed devices not compliant.
 - DESK-WILSON12 (olivia.wilson@contoso.example): Not compliant
 - LAPTOP-HILL07 (oliver.hill@contoso.example): Not compliant
 - LAPTOP-MARSH (bobby.marsh@contoso.example): Not compliant
- 1 of 20 joined computers not in Intune.
 - DESK-RECEPTION: Hybrid joined, not managed by Intune

Fix: Open each non-compliant device in Intune (Devices > Monitor > Noncompliant devices) to see which setting fails, fix it or retire the device, and block non-compliant devices with a Conditional Access policy that requires a compliant device.

Text to paste: All desktops and laptops run [anti-malware product, for example Microsoft Defender Antivirus], which updates automatically, scans files when they're opened and blocks malicious websites. Tablets and phones only install apps from the official app stores.

What Microsoft 365 can't show: Intune shows devices are managed and compliant; describe the anti-malware product.

System operations and change (CC7 and CC8)

● Fail

Vulnerabilities and anomalies are detected, events are evaluated, incidents responded to and recovered from, and changes are controlled.

CC7.1 Vulnerabilities and configuration changes detected

● Fail

Vulnerabilities and unexpected configuration changes are found, including systems out of support.

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
- 1 domain had sign-in settings changed in the last 30 days.
 - contoso.example: Set domain authentication by mallory.hart@contoso.example on 9 Oct 2026

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: External vulnerability scans run [monthly] using [tool or provider]. [A penetration test was last carried out on (date) by (provider).]

What Microsoft 365 can't show: Judged from Intune and Entra ID domain settings. Describe vulnerability scanning.

CC7.2 System components monitored for anomalies

● Partly

Sign-ins, accounts and mailboxes are monitored for anomalies, and activity is logged.

WHAT WE FOUND

- Not checked: no accounts are at risk in Entra ID Protection (Risky users need Entra ID P2).
- Not checked: no risky sign-ins succeeded (Sign-in risk needs Entra ID P2).
- Mailbox auditing is on for the organisation.

GAPS

- 1 suspicious inbox rule.
 - annabel.fraser@contoso.example: ":" Moves to RSS Feeds mail mentioning invoice, payment; Rule name ':' looks deliberately blank

Fix: Check each rule with the mailbox owner. Rules that delete or bury messages about payments or security alerts are a sign of a compromised account: reset the password, revoke sessions and review sign-ins.

Text to paste: Sign-ins are monitored for suspicious activity by [tool or service], and alerts are reviewed by [team or provider] [within one working day].

What Microsoft 365 can't show: Judged from Entra ID Protection, inbox rules and Exchange auditing.

CC7.3 Security events evaluated

● Your evidence

Security events are evaluated to decide whether they're incidents.

Text to paste: Security alerts and sign-in logs are reviewed [daily or weekly] by [team or provider]. Logs are kept for [period] where users can't change them.

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

CC7.4 Incidents responded to

● Your evidence

Security incidents are contained, fixed and communicated by a defined programme.

Text to paste: A documented incident response plan sets out roles, contacts and the steps to contain and recover from a cyber incident, including notifying [the insurer and IT provider]. It was last reviewed on [date] and tested on [date].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

CC7.5 Recovery from incidents

● Your evidence

Activities to recover from incidents are identified and carried out.

Text to paste: A business continuity and disaster recovery plan covers [key systems and services]. Recovery targets are [time to restore] to restore service and no more than [data loss window] of data loss. It was last tested on [date].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

CC8.1 Change management

● Partly

Changes to infrastructure, data and software are authorised, tested and approved; tenant settings that let users make their own changes are locked down.

WHAT WE FOUND

- Not checked: users can't create new tenants (Microsoft didn't return this setting).
- Only admins and members of Group creators can create teams and groups.

GAPS

- Any user can register an app.
 - Users can register apps that nobody reviews

Fix: Set "Users can register applications" to No (Entra admin center > Users > User settings) and give the Application Developer role to the people who need it.

Text to paste: Changes to systems, applications and networks are logged in [ticket system], checked for their security effect, tested where possible and approved by [role] before they're made. Emergency changes are reviewed afterwards.

What Microsoft 365 can't show: Microsoft 365 shows the tenant settings; describe the change process.

Risk mitigation and availability (CC9 and A1)

● Fail

Vendors and partners are managed, and data is backed up and recoverable.

CC9.2 Vendor and partner risk

● Fail

Risks from vendors and business partners are assessed and managed, including apps connected to the tenant.

GAPS

- Users can consent to any app.
 - Any user can grant any app access to their mail and files
- 1 app with access to mail, files or the directory.
 - Mail Sync Pro: Mail.Read (application permission; unverified publisher)

Fix: Set user consent to "Allow user consent for apps from verified publishers, for selected permissions" or turn it off and use the admin consent workflow. Consent phishing relies on this setting.

Text to paste: Suppliers and contractors that handle the organisation's data are checked before they're used, must meet [Cyber Essentials or equivalent security requirements], and are reviewed [every 12 months]. They're listed in [supplier register].

What Microsoft 365 can't show: Microsoft 365 shows which apps reach its data; describe the vendor reviews.

A1.2 Backups and recovery infrastructure

● Your evidence

Data is backed up and the recovery infrastructure is in place and monitored.

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.

What the assessor checks

What the assessor or auditor checks, what each needs, and what Microsoft 365 already shows for it.

Type 2 testing over the period

The auditor tests that each control worked throughout the period (often 6 or 12 months), sampling access changes, leavers, alerts and changes.

Microsoft 365 shows: Microsoft 365 shows the access and monitoring controls on this page, and the What changed view shows how each one stood at the start of the period.

Today: CC6.1 ● **Partly** CC6.3 ● **Partly** CC7.2 ● **Partly** CC8.1 ● **Partly**

About this evidence

A Pass is evidence for the Microsoft 365 part of a criterion; the auditor still tests the service's own systems and processes.

Requirements: AICPA 2017 Trust Services Criteria (revised points of focus, 2022): Security and Availability. Criteria identifiers are the AICPA's; criteria are paraphrased. This pack covers the criteria Microsoft 365 speaks to, not every point of focus.

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.