



ISO/IEC 27001 ANNEX A EVIDENCE

Contoso Legal LLP

PREPARED BY

Harbour IT

DATE

16 October 2026

EVIDENCE DATE

15 Oct 2026

SCHEME

ISO and IEC

MICROSOFT 365 TENANT

contoso.onmicrosoft.com

● Gaps to close

Contoso Legal LLP has 5 controls not in place.

IN THIS REPORT

Summary	2
Gaps to close	3
Organisational controls (5)	5
People controls (6)	11
Physical controls (7)	13
Technological controls (8)	15
What the assessor checks	23
About this evidence	23

Summary

Contoso Legal LLP has 5 controls not in place.

The Annex A controls Microsoft 365 data speaks to, judged for the Statement of Applicability and the audit, and the others an MSP is asked to evidence, as text to complete.

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

40 controls



■ 2 Pass ■ 5 Fail ■ 11 Partly ■ 21 Your evidence ■ 1 Not collected

Gaps to close

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

1 5.17 Authentication information

4 users without MFA. Fix: Ask these users to register the Microsoft Authenticator app.

2 5.23 Security for use of cloud services

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.

3 7.9 Assets away from the premises

2 of 19 computers not encrypted. Fix: Turn on BitLocker.

4 8.3 Information access restriction

3 files and folders shared with anyone. Fix: Remove anyone links that are no longer needed, and set the rest to view-only with an expiry date.

5 8.8 Management of technical vulnerabilities

11 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.

6 5.14 Information transfer

1 domain with SPF problems. Fix: Publish one SPF record per domain ending in -all.

7 5.15 Access control

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.

8 5.16 Identity management

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.

9 6.5 Responsibilities after leaving

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.

10 6.7 Remote working

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.

11 8.1 User endpoint devices

1 of 20 joined computers not in Intune. Fix: Enrol Entra-joined and hybrid-joined computers in Intune.

12 8.2 Privileged access rights

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

13 8.5 Secure 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.

14 8.9 Configuration management

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

15 8.12 Data leakage prevention

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

16 8.24 Use of cryptography

Data in Microsoft 365 is encrypted at rest by Microsoft (BitLocker and per-file service encryption) and in transit using TLS. Not every company computer is encrypted: 2 of 19 computers not encrypted.

Organisational controls (5)

● Fail

Policies, roles, assets, access rules, suppliers and cloud services, incidents and continuity.

5.1 Information security policies

● Your evidence

A security policy and topic-specific policies are defined, approved by management, published, acknowledged by staff and reviewed.

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.

5.2 Security roles and responsibilities

● Your evidence

Responsibilities for information security are defined and given to named people.

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.

5.9 Inventory of information and assets

● Your evidence

Information and the assets that hold it are listed, with an owner for each.

WHAT WE FOUND

- But: 1 of 22 device records unused for 90+ days.
- But: 1 of 20 joined computers not in Intune.
- Computers managed by Intune: 19
- Of which encrypted: 17
- Windows computers out of support: 11
- Not compliant: 3

Text to paste: An asset register in [tool or spreadsheet] lists [hardware, software, cloud services and the information held], each with a named owner, a category and where it is. Devices are added when they're set up and removed when they're disposed of, and the register was last reviewed on [date].

What Microsoft 365 can't show: Microsoft 365 lists the devices Intune and Entra ID know; the inventory covers everything else.

5.14 Information transfer

● Partly

Rules protect information sent by email and other means: domains can't be spoofed and mail travels encrypted.

WHAT WE FOUND

- But: 1 of 1 mail domain doesn't fully enforce MTA-STS.

GAPS

- 1 domain with SPF problems.
 - parked.example: Doesn't receive mail but has no "v=spf1 -all" record to stop spoofing
- 1 mail domain without DKIM.
 - contoso.example: Microsoft 365 DKIM isn't set up (selector2 CNAME missing)
- 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: Publish one SPF record per domain ending in -all (or ~all while testing), e.g. "v=spf1 include:spf.protection.outlook.com -all". Domains that never send mail should publish "v=spf1 -all".

Text to paste: SPF, DKIM and DMARC are not fully configured for the organisation's email domains. 1 domain with SPF problems. 1 mail domain without DKIM. 2 domains without DMARC enforcement.

What Microsoft 365 can't show: Judged from public DNS and Exchange Online for the tenant's domains.

5.15 Access control

● Partly

Rules for who can reach which information are set by business need, including what guests can see.

WHAT WE FOUND

- Guests have limited access to directory objects (the default).

GAPS

- Anyone, including guests, can invite guests.
 - Guests can invite other guests
- Anyone, including anonymous links.
 - SharePoint and OneDrive: Anyone links are allowed

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

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 guest settings and SharePoint sharing. Describe how staff access is decided.

5.16 Identity management

● Partly

Every identity belongs to one person and is removed when it's no longer needed; shared accounts can't sign in.

WHAT WE FOUND

- All 3 shared mailboxes block sign-in.

GAPS

- 2 accounts inactive for 90+ days or never used.
 - joseph.morris@contoso.example: Licensed member, last signed in 14 Jun 2026
 - g#EXT#@contoso.example: Guest, never signed in, created ?
- 1 disabled account still licensed.
 - bobby.marsh@contoso.example: Disabled, holding 1 licence

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: Some inactive accounts in Microsoft Entra ID have not been disabled. 2 accounts inactive for 90+ days or never used. 1 disabled account still licensed.

What Microsoft 365 can't show: Judged from Entra ID accounts, sign-in activity and shared mailboxes.

5.17 Authentication information

● Fail

Passwords and other sign-in secrets are protected: everyone has a second factor, and weak ones are avoided.

GAPS

- 4 users without MFA.
 - breakglass@contoso.example: No MFA method registered
 - carl.ashworth@contoso.example: No MFA method registered
 - joseph.morris@contoso.example: No MFA method registered
 - lily.harrison@contoso.example: No MFA method registered
- 3 people can only use a text or call as a second factor.
 - rhys.evans@contoso.example: Second factor is only Mobile phone (SMS or call)
 - sophie.taylor@contoso.example: Second factor is only Mobile phone (SMS or call)
 - william.allen@contoso.example: Second factor is only Mobile phone (SMS or call)

Fix: Ask these users to register the Microsoft Authenticator app. Until they do, anyone with their password can register MFA in their place.

Text to paste: Microsoft Entra ID requires passwords of at least 8 characters, blocks commonly used and known compromised passwords (Microsoft's global banned password list) and locks out repeated failed sign-in attempts (smart lockout). These are Microsoft defaults for cloud accounts. Multi-factor authentication is enforced for most users as well (see the MFA answer).

What Microsoft 365 can't show: Judged from Entra ID authentication methods. Add other systems that use passwords.

5.18 Access rights reviewed

● Pass

Access rights are given, reviewed and removed through a defined process, including guests.

WHAT WE FOUND

- No stale guest invitations.
- But: 4 teams and groups without an owner.
- Supporting: Unused teams and groups expire after 365 days.

Text to paste: Administrator access is reviewed [quarterly] by [role] against the list of current administrators, and anyone who no longer needs it has it removed.

What Microsoft 365 can't show: Microsoft 365 shows guests and group owners; describe the review and when it last happened.

5.19 Security in supplier relationships

● Your evidence

Security risks from suppliers are managed, with requirements agreed before they get access.

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: All of this. Answer from the organisation's own records.

5.20 Security in supplier agreements

● Your evidence

Contracts with suppliers set out their security and data protection obligations.

Text to paste: Every supplier that processes personal data for the organisation has a written contract with the terms UK GDPR Article 28 requires: acting only on instructions, confidentiality, security, approval of sub-processors, help with people's rights, and deleting or returning the data at the end. They're recorded in [register].

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

5.23 Security for use of cloud services

● Fail

Cloud services are taken on, used and left under the organisation's control: people can't connect apps to company data on their own, and app access is known.

WHAT WE FOUND

- Supporting: Users can consent to most apps themselves, so admin consent requests are off (see the user consent check).

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)
- 1 app registration with expiring or expired credentials.
 - Old connector: The 1 credential expired, last on 1 Jan 2025

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: Third-party application access to Microsoft 365 data is not controlled. Users can consent to any app. 1 app with access to mail, files or the directory.

What Microsoft 365 can't show: Judged from Entra ID consent settings, app permissions and app credentials.

5.24 Incident management planning

● Your evidence

Roles and procedures for handling security incidents are planned and documented.

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.

5.26 Response to incidents

● Your evidence

Incidents are responded to by the documented procedure, such as containing a compromised account.

Text to paste: If an account may be compromised, [IT provider] resets the password, signs the account out of every session, checks its MFA methods and inbox rules, and reviews its sign-ins. Staff report concerns to [contact].

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

5.29 Security during disruption

● Your evidence

Security is kept up during disruption, with continuity plans that are tested.

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.

5.34 Privacy and protection of personal data

● Your evidence

Legal requirements for personal data (UK GDPR in the UK) are identified and met.

Text to paste: A record of processing activities lists each kind of personal data held, its purpose and lawful basis, who it's shared with, where it's stored and how long it's kept. [Role] maintains it, and it was last reviewed on [date].

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

People controls (6)

● Partly

Screening, awareness and training, leavers, and remote working.

6.1 Screening

● Your evidence

People are checked before they join, in proportion to the information they'll reach.

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.

6.3 Awareness, education and training

● Your evidence

Staff get security awareness training and regular updates relevant to their job.

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.

6.5 Responsibilities after leaving

● Partly

Access ends when people leave or change role, and duties that continue are communicated.

GAPS

- 2 accounts inactive for 90+ days or never used.
 - joseph.morris@contoso.example: Licensed member, last signed in 14 Jun 2026
 - g#EXT#@contoso.example: Guest, never signed in, created ?
- 1 disabled account still licensed.
 - bobby.marsh@contoso.example: Disabled, holding 1 licence

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: Some inactive accounts in Microsoft Entra ID have not been disabled. 2 accounts inactive for 90+ days or never used. 1 disabled account still licensed.

What Microsoft 365 can't show: Judged from sign-in activity in Entra ID. Describe the leavers process.

6.7 Remote working

● Partly

People working away from the office reach company data securely.

WHAT WE FOUND

- Blocked by "CA003 — Block legacy authentication".

GAPS

- Enforced by CA002 — All users: Require MFA, with 1 exclusion to review.
 - breakglass@contoso.example: Excluded from "CA002 — All users: Require MFA"

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: Home and remote workers connect over [home broadband or business-provided routers] to Microsoft 365, with multi-factor authentication. [Office systems are reached through (VPN product).]

What Microsoft 365 can't show: Judged for Microsoft 365 sign-ins. Add VPNs and remote desktop.

6.8 Reporting security events

● Your evidence

Staff know how to report suspected security events quickly.

Text to paste: Every personal data breach is recorded in a breach log with what happened, its effects and what was done. [Role] decides whether it must be reported; reportable breaches go to the ICO within 72 hours of the organisation becoming aware, and to the people affected when the risk to them is high. Lessons learned are reviewed by [role].

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

Physical controls (7)

● Fail

Premises, equipment away from the office, storage media and disposal.

7.1 to 7.4 Secure premises

● Your evidence

Offices and secure areas have perimeters, entry controls and monitoring.

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.

7.9 Assets away from the premises

● Fail

Laptops and other equipment used away from the office are protected, including by encryption.

GAPS

- 2 of 19 computers not encrypted.
 - LAPTOP-HILL07 (oliver.hill@contoso.example): Windows disk isn't encrypted
 - LAPTOP-MARSH (bobby.marsh@contoso.example): Windows disk isn't encrypted

Fix: Turn on BitLocker (Windows) and FileVault (macOS) with an Intune disk encryption policy, with recovery keys escrowed to Entra ID, so a lost or stolen laptop doesn't expose the client's data.

Text to paste: Company computers managed in Microsoft Intune are not all encrypted. 2 of 19 computers not encrypted.

What Microsoft 365 can't show: Judged from Intune for company computers.

7.10 Storage media

● Your evidence

Removable storage is controlled from first use to disposal.

Text to paste: Removable media is [blocked by Intune policy or allowed only on encrypted, company-issued drives], and drives that hold the organisation's data are recorded in the asset register.

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

7.14 Secure disposal or re-use

● Your evidence

Data is securely removed before equipment is reused or 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.

Technological controls (8)

● Fail

Endpoints, privileged access, authentication, malware, vulnerabilities, configuration, leakage, backup, logging, monitoring, networks, web filtering, cryptography and change.

8.1 User endpoint devices

● Partly

Laptops, desktops and phones that reach company data are managed and meet policy.

WHAT WE FOUND

- Computers managed by Intune: 19
- Of which encrypted: 17
- Windows computers out of support: 11
- Not compliant: 3

GAPS

- 1 of 20 joined computers not in Intune.
 - DESK-RECEPTION: Hybrid joined, not managed by Intune
- 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
- 2 devices haven't checked in for 30+ days.
 - DESK-WILSON12 (olivia.wilson@contoso.example): Last check-in 38 days ago
 - LAPTOP-MARSH (bobby.marsh@contoso.example): Last check-in 45 days ago

Fix: Enrol Entra-joined and hybrid-joined computers in Intune (automatic enrolment under Devices > Enrollment > Windows) so compliance, encryption and updates can be enforced on them.

Text to paste: Company devices are not all managed centrally. 1 of 20 joined computers not in Intune. 3 of 20 managed devices not compliant.

What Microsoft 365 can't show: Judged from Intune and Entra ID.

8.2 Privileged access rights

● Partly

Administrator rights are few, given to named internal people, and separate from everyday accounts.

WHAT WE FOUND

- 2 Global Administrators.
- Cloud-only tenant: no accounts are synced from on-premises AD.
- But: 1 admin without MFA, and 1 whose registration isn't known.
- 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: Administrator role assignments in Microsoft 365 are tracked, with gaps. 4 accounts hold privileged admin roles, 2 of them Global Administrator (annabel.fraser@contoso.example, breakglass@contoso.example). 2 Global Administrators. 1 guest with admin roles. 1 app with privileged roles.

What Microsoft 365 can't show: Judged from Microsoft 365 and Entra ID admin roles. Add administrators of other systems.

8.3 Information access restriction

● Fail

Access to files is restricted as the access rules say: nothing open to anyone with the link.

GAPS

- 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
- Anyone, including anonymous links.
 - SharePoint and OneDrive: Anyone links are allowed

Fix: Remove anyone links that are no longer needed, and set the rest to view-only with an expiry date. The Shared files report lists each one.

Text to paste: Sharing with anonymous and external users is not restricted in SharePoint and OneDrive. Anyone, including anonymous links. 3 files and folders shared with anyone. Anyone, including guests, can invite guests.

What Microsoft 365 can't show: Judged from SharePoint and OneDrive sharing settings and links.

8.5 Secure authentication

● Partly

Sign-in is protected by multi-factor authentication, for administrators especially, and protocols that can't use it are blocked.

WHAT WE FOUND

- Blocked by "CA003 — Block legacy authentication".
- But: 2 admins without a phishing-resistant method.
- 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 from Conditional Access, Security Defaults and Exchange Online for Microsoft 365.

8.7 Protection against malware

● Your evidence

Malware protection runs on every device, and mail is filtered for malicious content.

WHAT WE FOUND

- But: 3 of 20 managed devices not compliant.

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: All of this. Answer from the organisation's own records.

8.8 Management of technical vulnerabilities

● Fail

Vulnerabilities are found and fixed in time, and systems that no longer get updates are replaced.

WHAT WE FOUND

- Computers managed by Intune: 19
- Of which encrypted: 17
- Windows computers out of support: 11
- Not compliant: 3

GAPS

- 11 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 ended 13 Oct 2026 (Enterprise and Education: 12 Oct 2027).
 - DESK-WILSON12
(olivia.wilson@contoso.example): Windows 11 24H2: updates for Home and Pro ended 13 Oct 2026 (Enterprise and Education: 12 Oct 2027).
 - 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. 11 of 19 Windows computers past end of support.

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

8.9 Configuration management

● **Partly**

Secure settings are defined and kept: ordinary users can't create tenants, register apps or join by verifying an email address.

WHAT WE FOUND

- Not checked: users can't create new tenants (Microsoft didn't return this setting).
- Not checked: people can't join the tenant just by verifying an email address (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: Judged from Entra ID tenant settings. Describe how settings are recorded and changed.

8.10 Information deletion

● **Your evidence**

Information is deleted when it's no longer needed.

Text to paste: A retention schedule sets how long each kind of data is kept. Data past its retention period is deleted [by Microsoft 365 retention policies or at a review every (period)], and the data held is reviewed [every 12 months] to check it's still needed.

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

8.12 Data leakage prevention

● Partly

Mail can't be forwarded outside unnoticed, and inbox rules that hide or forward mail are caught.

WHAT WE FOUND

- The default outbound policy blocks automatic external forwarding.

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

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 the Exchange Online outbound spam policy, mailbox forwarding and inbox rules.

8.13 Information backup

● Your evidence

Backups are taken and restores tested, as the backup policy says.

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.

8.15 Logging

● Pass

Logs of activity and security events are produced, kept and protected.

WHAT WE FOUND

- Mailbox auditing is on for the organisation.

Text to paste: Mailbox audit logging is enabled in Exchange Online, recording access to and actions on mailboxes. Mailbox auditing is on for the organisation.

What Microsoft 365 can't show: Judged from Exchange Online mailbox auditing and the unified audit log.

8.16 Monitoring activities

● Not collected

Networks, systems and sign-ins are watched for unusual behaviour, and it's acted on.

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).
- But: 1 domain had sign-in settings changed in the last 30 days.

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 (needs Entra ID P2 for the full detections).

8.20 Network security

● Your evidence

Networks are protected by firewalls and managed.

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: All of this. Answer from the organisation's own records.

8.23 Web filtering

● Your evidence

Access to malicious websites is blocked.

Text to paste: Malicious websites are blocked by [Microsoft Defender SmartScreen and network protection, a filtering DNS service such as Quad9, or the firewall's web filter].

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

8.24 Use of cryptography

● Partly

Encryption protects data at rest and in transit, by an agreed approach.

WHAT WE FOUND

- But: 2 of 19 computers not encrypted.
- But: 1 of 1 mail domain doesn't fully enforce MTA-STS.

GAPS

- Data in Microsoft 365 is encrypted at rest by Microsoft (BitLocker and per-file service encryption) and in transit using TLS. Not every company computer is encrypted: 2 of 19 computers not encrypted.

Text to paste: Data in Microsoft 365 is encrypted at rest by Microsoft (BitLocker and per-file service encryption) and in transit using TLS. Not every company computer is encrypted: 2 of 19 computers not encrypted.

What Microsoft 365 can't show: Microsoft encrypts Microsoft 365 data itself; laptops are judged from Intune.

8.32 Change management

● Your evidence

Changes to systems are planned, tested and approved.

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: All of this. Answer from the organisation's own records.

What the assessor checks

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

Stage 2 certification and surveillance audits

The auditor samples Annex A controls from the Statement of Applicability and asks for evidence that each works in practice: records, settings and interviews.

Microsoft 365 shows: Microsoft 365 can show the technical evidence the day it's asked for: authentication, privileged access, endpoints, logging and leakage controls on this page, with the rows behind them, and what changed since the last audit.

Today: 8.5 ● Partly 8.2 ● Partly 8.1 ● Partly 8.15 ● Pass 8.12 ● Partly

About this evidence

Use the controls marked Pass as evidence in the Statement of Applicability, with this pack's date. A Partly is a likely minor nonconformity; a Fail is a likely major one.

Scope: the ISMS scope may be wider than Microsoft 365. A Pass here covers Microsoft 365; say what covers the rest.

Requirements: ISO/IEC 27001:2022 with Amendment 1:2024, Annex A. Control numbers are ISO's; titles and requirements are paraphrased. This pack is part of the Statement of Applicability, not all of it: the other Annex A controls and the management system clauses 4 to 10 are the organisation's own.

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 15 Oct 2026, 04:00 UTC. Accepted risks are exceptions the organisation has reviewed and documented. Complete the [parts in brackets] before using a text.