



Harbour IT

CYBER INSURANCE PROPOSAL EVIDENCE

Contoso Legal LLP

PREPARED BY

Harbour IT

DATE

14 October 2026

EVIDENCE DATE

14 Oct 2026

SCHEME

The controls UK cyber insurance proposal and renewal forms ask about, with the answers to paste.

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
Multi-factor authentication and access	5
Email security	9
Devices and patching	11
Backups and recovery	14
Monitoring and data	15
Network and people	17
Answers for the form	18
About this evidence	22

Harbour IT • help@harbourit.example • 0161 496 0000

Confidential. This report describes security settings for Contoso Legal LLP; share it only with people who need it.

Summary

Contoso Legal LLP has 3 controls not in place.

What insurers price the premium on, judged from Microsoft 365 where it can see it. A control missing for the whole organisation is a Fail and a gap on a few accounts is Partly; insurers don't refuse an application for either, they price it or add conditions, so declare both. Match each answer to the question on the form, since wording differs between insurers.

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

24 controls



■ 3 Pass ■ 3 Fail ■ 7 Partly ■ 10 Your evidence ■ 1 Not collected

Gaps to close

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

1 Managed, encrypted and on supported systems

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

2 External sharing restricted

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

3 Third-party apps controlled

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 MFA for every user, on email and cloud apps

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).

5 Legacy authentication blocked

SMTP AUTH is on for the organisation. Fix: Turn off SMTP AUTH for the organisation and enable it only on the mailboxes of devices or apps that still need it.

6 Separate accounts for administration

1 of 2 admin accounts also has a licence or mailbox, so it looks like an everyday account: annabel.fraser@contoso.example. Fix: Give each administrator a separate, unlicensed admin account with no mailbox, used only for administration, and take the admin roles off the account they use every day.

7 Few, named, internal administrators

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

8 Leavers and inactive accounts removed

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 SPF, DKIM and DMARC on every domain

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

10 No automatic forwarding outside

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

Multi-factor authentication and access

● Partly

Every account signs in with MFA, legacy protocols that can't are blocked, administrators are few, separate and named, and accounts go when people do.

MFA for every user, on email and cloud apps

● Partly

Multi-factor authentication is enforced for all users accessing email (including webmail and mobile) and cloud applications.

WHAT WE FOUND

- But: 4 users without MFA.
- 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 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).

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 only. Add VPNs, remote desktop and other systems.

MFA for every administrator

● Pass

Every privileged and administrator account is protected by MFA.

WHAT WE FOUND

- 2 of 3 active admin accounts are required to use MFA by "CA001 — Admins: Require phishing-resistant MFA"; the exception is 1 break-glass account: breakglass@contoso.example (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").
- 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

Text to paste: Multi-factor authentication is enforced for the administrator accounts of Microsoft 365 and Microsoft Entra ID. 2 of 3 active admin accounts are required to use MFA by "CA001 — Admins: Require phishing-resistant MFA"; the exception is 1 break-glass account: breakglass@contoso.example (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").

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

MFA on remote access

● Your evidence

VPN, remote desktop and remote support tools need MFA.

Text to paste: Remote access to the network is only possible through [VPN or remote access product], which requires multi-factor authentication. Remote support tools ([product]) also require multi-factor authentication.

What Microsoft 365 can't show: Not something Microsoft 365 shows; answer from the client's own records.

Legacy authentication blocked

● Partly

Sign-in protocols that can't use MFA (IMAP, POP, SMTP AUTH, older Office clients) are blocked.

WHAT WE FOUND

- Blocked by "CA003 — Block legacy authentication".

GAPS

- SMTP AUTH is on for the organisation.
 - SMTP AUTH is allowed

Fix: Turn off SMTP AUTH for the organisation and enable it only on the mailboxes of devices or apps that still need it, such as scanners. It accepts passwords without MFA.

Text to paste: Legacy authentication is blocked for Microsoft 365 sign-ins, with one exception. Blocked by "CA003 — Block legacy authentication". SMTP AUTH (password-only mail sending) is still allowed: SMTP AUTH is on for the organisation.

What Microsoft 365 can't show: Judged from Conditional Access and Exchange Online settings.

Separate accounts for administration

● Partly

Administrators use a separate account for admin work, not the one they read email with.

GAPS

- 1 of 2 admin accounts also has a licence or mailbox, so it looks like an everyday account: annabel.fraser@contoso.example.

Fix: Give each administrator a separate, unlicensed admin account with no mailbox, used only for administration, and take the admin roles off the account they use every day.

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 admin role holders: an admin account with a licence or a mailbox looks like an everyday account.

Few, named, internal administrators

● Partly

Administrator access is limited to a small number of named internal people: no guests, no unnecessary Global Administrators, no apps with admin roles.

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: 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: Microsoft 365 shows who holds admin roles today; describe how the list is reviewed.

Leavers and inactive accounts removed

● Partly

Accounts are disabled promptly when people leave, inactive accounts are removed, and no disabled account keeps a licence.

WHAT WE FOUND

- No stale guest invitations.

GAPS

- 2 accounts inactive for 90+ days or never used.
 - joseph.morris@contoso.example: Licensed member, last signed in 13 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 Microsoft Entra ID (needs Entra ID P1 for last sign-in dates). Describe the leavers process in the answer.

Email security

● Partly

Mail is filtered, the domains can't be spoofed, nothing forwards outside unnoticed, and payment changes are verified by voice.

Incoming mail filtered

● Pass

Incoming email is filtered for spam, phishing and malicious links and attachments.

WHAT WE FOUND

- Incoming email for contoso.example is delivered to Microsoft 365 and filtered by Exchange Online Protection (anti-spam, anti-phishing and anti-malware).

Text to paste: Incoming email is filtered for spam, phishing and malware. Incoming email for contoso.example is delivered to Microsoft 365 and filtered by Exchange Online Protection (anti-spam, anti-phishing and anti-malware).

What Microsoft 365 can't show: Microsoft 365 shows which mail gateway the domains route through, not its settings.

SPF, DKIM and DMARC on every domain

● Partly

Every email domain publishes SPF, signs with DKIM and has a DMARC policy.

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.

No automatic forwarding outside

● Partly

Automatic forwarding of email to external addresses is blocked, and inbox rules that forward or hide 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.

Payment changes verified by phone

● Your evidence

Requests to change bank details or make payments are verified with a known contact by phone.

Text to paste: Requests to change supplier bank details or make urgent payments are verified by calling the requester on a number already held on file, never one given in the request. Payments over [amount] need approval by [role].

What Microsoft 365 can't show: Not something Microsoft 365 shows; answer from the client's own records.

Devices and patching

● Fail

Computers are managed, encrypted, protected by EDR, on supported operating systems and patched within 14 days.

EDR on every computer and server

● Your evidence

Endpoint detection and response is installed and monitored on all computers and servers.

Text to paste: [EDR product, for example Microsoft Defender for Endpoint] is installed on all [number] computers and servers. Alerts are monitored by [team or security provider] [24/7 or in business hours].

What Microsoft 365 can't show: Office Sentry doesn't read Microsoft Defender; answer from the EDR console.

Managed, encrypted and on supported systems

● Fail

Company devices are managed, encrypted and run operating systems that still get security updates.

WHAT WE FOUND

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

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
- 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
- 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: 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: 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 for devices known to Intune or Entra ID. Servers, macOS and unmanaged devices aren't seen.

Critical updates within 14 days

● Your evidence

Critical security updates are installed within 14 days of release (some forms say 30).

WHAT WE FOUND

- But: 2 devices haven't checked in for 30+ days.

Text to paste: Operating system updates install automatically through [Windows Update for Business, Intune update rings or the RMM tool]. Critical and high-risk updates, including router and firewall firmware, are installed within 14 days of release, and this is checked [weekly] by [IT provider].

What Microsoft 365 can't show: Intune shows when each device last checked in, not when updates were installed.

Backups and recovery

● Your evidence

Data is backed up separately and the restores are tested; there is a plan for an incident and for keeping the business running.

Backups kept separately and tested

● Your evidence

Backups are taken regularly, kept offline or immutable and separate from the main systems, 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: Not something Microsoft 365 shows; answer from the client's own records.

Continuity and recovery plan

● Your evidence

A business continuity and disaster recovery plan exists and is 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: Not something Microsoft 365 shows; answer from the client's own records.

Incident response plan

● Your evidence

A documented incident response plan says who does what.

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: Not something Microsoft 365 shows; answer from the client's own records.

Monitoring and data

● Fail

Activity is logged, suspicious sign-ins are watched, and data only leaves through sharing and apps that are controlled.

Audit logging on

● Pass

Audit logging is enabled for email and user activity.

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.

Suspicious sign-ins monitored

● Not collected

Risky sign-ins and users are detected and 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).

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).

External sharing restricted

● Fail

Sharing files with people outside the organisation is restricted and guests are invited deliberately.

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

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: 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.

Third-party apps controlled

● Fail

Users can't consent to third-party apps on their own, and apps with risky permissions are known.

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: 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 and app permissions.

Network and people

● Your evidence

A firewall between the network and the internet, no remote desktop open to it, and staff trained to spot phishing.

Firewalls at the internet boundary

● Your evidence

Firewalls sit between the network and the internet.

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: Not something Microsoft 365 shows; answer from the client's own records.

No remote desktop open to the internet

● Your evidence

Remote desktop is closed to the internet, or only reachable through a VPN or gateway with MFA.

Text to paste: Remote desktop (RDP) is not reachable from the internet. Remote connections go through [VPN or remote desktop gateway] with multi-factor authentication. This was last confirmed on [date] by [external scan or firewall review].

What Microsoft 365 can't show: Not something Microsoft 365 shows; answer from the client's own records.

Security awareness training

● Your evidence

Staff receive regular security awareness and phishing 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: Not something Microsoft 365 shows; answer from the client's own records.

Answers for the form

The questions UK cyber insurance proposal and renewal forms usually ask. Wording differs between insurers, so match each answer to the question on the form. "Your input" marks what Microsoft 365 can't show, with a text to complete. Answers marked with a name were set by your technical lead.

Multi-factor authentication and access

Question	Answer	Text to paste
Is multi-factor authentication (MFA) enforced for all users accessing email, including webmail and mobile?	● Partly	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). Still to check: This covers Microsoft 365 sign-ins only. Add VPN, remote desktop and any other system people reach from outside the office.
Is MFA required for all remote access to the network, such as VPN, remote desktop and remote support tools?	● Your input	Remote access to the network is only possible through [VPN or remote access product], which requires multi-factor authentication. Remote support tools ([product]) also require multi-factor authentication. Why: Microsoft 365 can't show this. It sees Microsoft 365 sign-ins (see the MFA answer), not VPNs or remote desktop.
Is MFA enforced for all privileged and administrator accounts?	● Yes	Multi-factor authentication is enforced for the administrator accounts of Microsoft 365 and Microsoft Entra ID. 2 of 3 active admin accounts are required to use MFA by "CA001 — Admins: Require phishing-resistant MFA"; the exception is 1 break-glass account: breakglass@contoso.example (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"). Still to check: Covers Microsoft 365 and Entra ID admin roles. Add admin access to servers, firewalls, backup consoles and other cloud services.

Question	Answer	Text to paste
Are legacy authentication protocols that can't use MFA blocked?	● Partly	Legacy authentication is blocked for Microsoft 365 sign-ins, with one exception. Blocked by "CA003 — Block legacy authentication". SMTP AUTH (password-only mail sending) is still allowed: SMTP AUTH is on for the organisation.
Are administrator accounts separate from the accounts people use every day?	● Partly	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. Still to check: Covers Microsoft 365 admin roles. Add local administrator, server and domain admin accounts.
Is administrator access limited to a small number of named people?	● Partly	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. Still to check: Add administrators of servers, firewalls and other systems, and say how the list is kept.
Are leavers' accounts disabled promptly and inactive accounts removed?	● No	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. Still to check: Describe the leavers process: who tells IT, and how quickly accounts are disabled.

Email security

Question	Answer	Text to paste
Is incoming email filtered for spam, phishing and malicious links and attachments?	● Yes	Incoming email is filtered for spam, phishing and malware. Incoming email for contoso.example is delivered to Microsoft 365 and filtered by Exchange Online Protection (anti-spam, anti-phishing and anti-malware). Still to check: Office Sentry sees the mail routing and licences, not the filtering policies. Confirm Safe Links and Safe Attachments (or the gateway's equivalent) apply to every user.
Are SPF, DKIM and DMARC configured for your email domains?	● No	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.
Is automatic forwarding of email to external addresses blocked?	● Partly	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.

Question	Answer	Text to paste
Do you verify requests to change bank details or make payments by calling a known contact?	● Your input	Requests to change supplier bank details or make urgent payments are verified by calling the requester on a number already held on file, never one given in the request. Payments over [amount] need approval by [role]. Why: Microsoft 365 can't show this. It's a finance process.

Devices and patching

Question	Answer	Text to paste
Is endpoint detection and response (EDR) installed and monitored on all computers and servers?	● Your input	[EDR product, for example Microsoft Defender for Endpoint] is installed on all [number] computers and servers. Alerts are monitored by [team or security provider] [24/7 or in business hours]. Why: Microsoft 365 can't show this. Office Sentry doesn't read Microsoft Defender for Endpoint or other EDR consoles.
Are all operating systems supported and still receiving security updates, with no end-of-life systems?	● No	Managed Windows computers run versions of Windows that no longer receive security updates. 11 of 19 Windows computers past end of support. Still to check: Covers Windows computers known to Intune or Entra ID. Add servers, macOS, phones, network devices and other software.
Are critical security updates installed within 14 days of release?	● Your input	Operating system updates install automatically through [Windows Update for Business, Intune update rings or the RMM tool]. Critical and high-risk updates, including router and firewall firmware, are installed within 14 days of release, and this is checked [weekly] by [IT provider]. Why: Microsoft 365 can't show this. Intune shows which Windows version each computer runs (see the supported systems answer), not when updates were installed. Still to check: Some forms ask about 30 days. Answer to the timescale on the form.
Are laptops and desktops encrypted?	● No	Company computers managed in Microsoft Intune are not all encrypted. 2 of 19 computers not encrypted. Still to check: Covers computers managed by Intune. Add any computers that aren't.
Are company devices centrally managed?	● No	Company devices are not all managed centrally. 1 of 20 joined computers not in Intune. 3 of 20 managed devices not compliant. Still to check: Covers devices joined to Entra ID. Add any company devices that aren't.

Backups and recovery

Question	Answer	Text to paste
Are backups taken regularly, kept offline or immutable, separate from your main systems, and tested?	● Your input	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]. Why: Backups aren't visible in Microsoft 365 data. Answer from the backup product's records.
Do you have a business continuity and disaster recovery plan, and is it tested?	● Your input	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]. Why: Microsoft 365 can't show this.
Do you have a documented incident response plan?	● Your input	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]. Why: Microsoft 365 can't show this.

Monitoring and data

Question	Answer	Text to paste
Is audit logging enabled for email and user activity?	● Yes	Mailbox audit logging is enabled in Exchange Online, recording access to and actions on mailboxes. Mailbox auditing is on for the organisation. Still to check: How long audit logs are kept depends on the Microsoft 365 licence; confirm the retention period.
Do you monitor for suspicious sign-ins?	● Your input	Sign-ins are monitored for suspicious activity by [tool or service], and alerts are reviewed by [team or provider] [within one working day]. Why: Sign-in risk needs Entra ID P2.
Is sharing of files with people outside the organisation restricted?	● No	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.
Is access to your data by third-party applications controlled?	● No	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.

Network

Question	Answer	Text to paste
Do you have firewalls between your network and the internet?	● Your input	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. Why: Microsoft 365 can't show this. Firewalls aren't part of Microsoft 365.
Is remote desktop (RDP) closed to the internet?	● Your input	Remote desktop (RDP) is not reachable from the internet. Remote connections go through [VPN or remote desktop gateway] with multi-factor authentication. This was last confirmed on [date] by [external scan or firewall review]. Why: Microsoft 365 can't show this. It's a firewall setting.

People

Question	Answer	Text to paste
Do staff receive regular security awareness and phishing training?	● Your input	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]. Why: Training isn't visible in Microsoft 365 data. Answer from the training provider's records.

About this evidence

Scope: insurers ask about the whole business, not one cloud service. A Pass here covers Microsoft 365; the answer should say what covers the rest.

Most forms are signed as a warranty: a wrong answer can void the policy, so a Partly should be declared, not rounded up.

Requirements: UK cyber insurance proposal forms as commonly worded in 2026. Questions drawn from the proposal and renewal forms of UK cyber insurers and brokers, in their typical wording; no insurer's form is copied.

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