



Harbour IT

SUPPLIER SECURITY QUESTIONNAIRE EVIDENCE

Fabrikam Dental Group

PREPARED BY

Harbour IT

DATE

12 October 2026

EVIDENCE DATE

12 Oct 2026

SCHEME

What clients ask in supplier and vendor due-diligence questionnaires, answered for this client.

MICROSOFT 365 TENANT

fabrikam.onmicrosoft.com

● Gaps to close

Fabrikam Dental Group has 4 controls not in place.

IN THIS REPORT

Summary	2
Gaps to close	3
Governance	5
Access control	6
Data protection	11
Email security	13
Devices	15
Logging and monitoring	18
Incidents, backups and continuity	19
Third parties, people and premises	20
Harbour IT - help@harbourit.example 0161 496 0000	20
Confidential: This report describes security settings for Fabrikam Dental Group; share it only with people who need it.	22
Answers for the form	22
About this evidence	28

Summary

Fabrikam Dental Group has 4 controls not in place.

Due-diligence questionnaires are read by a customer's security team, so the answers should be specific and true. A control missing for the whole organisation is a Fail and a gap on a few accounts is Partly: say what's in place and what's planned. Use the text for the matching question on the client's form.

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

36 controls



 **12** Pass  **4** Fail  **10** Partly  **9** Your evidence  **1** Not collected

Gaps to close

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

1 External sharing controlled

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

2 Portable devices encrypted

6 of 54 computers not encrypted. Fix: Turn on BitLocker.

3 Supported operating systems

7 of 54 Windows computers past end of support. Fix: Upgrade computers on Windows 10 or an old Windows 11 release to the current Windows 11 release.

4 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.

5 MFA for every user

Enforced by Conditional Access ("CA002 — All users: Require MFA"), but with 12 exclusions to review: breakglass@fabrikam.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).

6 Phishing-resistant MFA for administrators

2 admins without a phishing-resistant method. Fix: Have each listed admin register a passkey.

7 No weak MFA methods

4 people can only use a text or call as a second factor. Fix: Ask these people to set up the Microsoft Authenticator app.

8 Separate admin accounts

1 of 2 admin accounts also has a licence or mailbox, so it looks like an everyday account: anna.kowalski@fabrikam.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.

9 Privileged access restricted and tracked

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

10 Access removed when people leave

7 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.

11 Encrypted at rest and in transit

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: 6 of 54 computers not encrypted.

12 SPF, DKIM and DMARC

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

13 No automatic forwarding outside

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

14 Devices managed to a baseline

1 of 55 joined computers not in Intune. Fix: Enrol Entra-joined and hybrid-joined computers in Intune.

Governance

● Your evidence

Written policies and recognised certifications.

Information security policies

● Your evidence

Documented information security policies exist and are 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: Not something Microsoft 365 shows; answer from the client's own records.

Security certifications held

● Your evidence

Cyber Essentials, CE Plus, ISO 27001 or similar, with dates.

Text to paste: The organisation holds [Cyber Essentials or Cyber Essentials Plus or ISO 27001] certification, number [certificate number], valid until [date].

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

Access control

● Partly

Unique accounts with MFA, phishing-resistant for administrators, separate admin accounts, a password policy, and access removed when people leave.

MFA for every user

● Partly

Multi-factor authentication is required for all users.

WHAT WE FOUND

- But: 27 users without MFA.
- Users with an MFA method registered: 50.9% of 55
- Accounts covered by an enforced MFA policy: 54 of 55
- Not covered: breakglass@fabrikam.example

GAPS

- Enforced by Conditional Access ("CA002 — All users: Require MFA"), but with 12 exclusions to review: breakglass@fabrikam.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@fabrikam.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 privileged accounts

● Pass

Every privileged account uses 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@fabrikam.example (excluded from "CA001 — Admins: Require phishing-resistant MFA", "CA002 — All users: Require MFA", "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@fabrikam.example (excluded from "CA001 — Admins: Require phishing-resistant MFA", "CA002 — All users: Require MFA", "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.

Phishing-resistant MFA for administrators

● Partly

Administrators sign in with FIDO2 keys, passkeys or Windows Hello for Business, not codes.

GAPS

- 2 admins without a phishing-resistant method.
 - anna.kowalski@fabrikam.example: Global Administrator; signs in with Authenticator app
 - breakglass@fabrikam.example: Global Administrator; signs in with no MFA method at all

Fix: Have each listed admin register a passkey (in Microsoft Authenticator or on a security key) or Windows Hello for Business, then require the Phishing-resistant MFA authentication strength for admin roles in Conditional Access. Codes and push approvals can be relayed by a fake sign-in page; these can't.

Text to paste: Administrator accounts don't all use phishing-resistant sign-in methods yet. 2 admins without a phishing-resistant method.

What Microsoft 365 can't show: Judged from the sign-in methods admin accounts have registered.

No weak MFA methods

● Partly

Text-message and voice-call MFA are turned off or being retired.

GAPS

- 4 people can only use a text or call as a second factor.
 - george.baker@fabrikam.example: Second factor is only Mobile phone (SMS or call)
 - owen.robinson@fabrikam.example: Second factor is only Mobile phone (SMS or call)
 - owen.turner@fabrikam.example: Second factor is only Mobile phone (SMS or call)
 - thomas.allen@fabrikam.example: Second factor is only Mobile phone (SMS or call)

Fix: Ask these people to set up the Microsoft Authenticator app (the registration campaign in the authentication methods policy prompts them at sign-in), then turn off text message and voice call sign-in, or keep them only as a backup. Texts and calls can be intercepted or moved to an attacker's SIM.

Text to paste: Some users rely on a text message or phone call as their only second factor. 4 people can only use a text or call as a second factor.

What Microsoft 365 can't show: Judged from the authentication methods policy and what people have registered.

Separate admin accounts

● Partly

Administrative accounts are separate from standard user accounts.

GAPS

- 1 of 2 admin accounts also has a licence or mailbox, so it looks like an everyday account:
 - anna.kowalski@fabrikam.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: anna.kowalski@fabrikam.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.

Privileged access restricted and tracked

● Partly

Few named administrators, no guests or apps with admin roles, and the list is reviewed.

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#@fabrikam.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 (anna.kowalski@fabrikam.example, breakglass@fabrikam.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.

Unique accounts, no shared logins

● Pass

Every user has their own account; shared mailboxes can't be signed in to.

WHAT WE FOUND

- All 3 shared mailboxes block sign-in.

Text to paste: Each person signs in to Microsoft 365 with their own named account. Shared mailboxes can't be signed in to directly; people reach them through their own accounts. All 3 shared mailboxes block sign-in.

What Microsoft 365 can't show: Judged from whether shared mailboxes can be signed in to. Check devices and other systems.

Password policy

● Pass

Passwords have a minimum length, common ones are banned and repeated failures lock the account.

WHAT WE FOUND

- 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: Microsoft Entra ID's defaults (8 characters, a banned password list and smart lockout) aren't read from the tenant. Add other systems that take passwords.

Access removed when people leave

● Partly

Leavers' accounts are disabled promptly and inactive accounts removed.

GAPS

- 7 accounts inactive for 90+ days or never used.
 - aaron.smith@fabrikam.example: Licensed member, last signed in 23 Apr 2026
 - aisha.brown@fabrikam.example: Licensed member, last signed in 7 Mar 2026
 - jack.lee@fabrikam.example: Licensed member, last signed in 4 Jun 2026
 - noah.wood@fabrikam.example: Licensed member, last signed in 7 Feb 2026
 - rhys.walker@fabrikam.example: Licensed member, last signed in 5 Jun 2026
 - and 2 more
- 1 disabled account still licensed.
 - ben.okafor@fabrikam.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. 7 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. Describe the leavers process in the answer.

Guest access reviewed

● Pass

Guests and external users are reviewed and pending invitations cleared.

WHAT WE FOUND

- No stale guest invitations.
- Guests have limited access to directory objects (the default).

Text to paste: Guest and external user accounts are not reviewed regularly. 1 guest account: 1 guest inactive for 90+ days or never signed in (g#EXT#@fabrikam.example).

What Microsoft 365 can't show: Judged from guest accounts and the external collaboration settings.

Data protection

● Fail

Where data lives, encryption at rest and in transit, and sharing under control.

Where data is stored

● Pass

The region the tenant's data is held in.

WHAT WE FOUND

- Email, files and Teams data are held in Microsoft 365, in Microsoft's datacentres.

What Microsoft 365 can't show: Microsoft 365 reports the tenant's data location; add any other systems.

Encrypted at rest and in transit

● Partly

Data is encrypted at rest and in transit.

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: 6 of 54 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: 6 of 54 computers not encrypted.

What Microsoft 365 can't show: Microsoft 365 encrypts stored data and connections; add other systems.

External sharing controlled

● Fail

Data can't be shared with unauthorised people: sharing settings, anyone links and guest invitations.

GAPS

- Anyone, including anonymous links.
 - SharePoint and OneDrive: Anyone links are allowed
- 2 files and folders shared with anyone.
 - holiday.jpg (OneDrive of anna.kowalski@fabrikam.example): Anyone can view
 - Open day flyer.pdf (Marketing / Documents): Anyone can view, link never expires
- 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. 2 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.

Portable devices encrypted

● Fail

Laptops and other portable devices are encrypted.

GAPS

- 6 of 54 computers not encrypted.
 - DESK-MOORE18 (ava.moore@fabrikam.example): Windows disk isn't encrypted
 - DESK-ROBINSON51 (owen.robinson@fabrikam.example): Windows disk isn't encrypted
 - LAPTOP-OKAFOR (ben.okafor@fabrikam.example): Windows disk isn't encrypted
 - LAPTOP-ROBINSON07 (thomas.robinson@fabrikam.example): Windows disk isn't encrypted
 - LAPTOP-WARD29 (jack.ward@fabrikam.example): Windows disk isn't encrypted
 - and 1 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: Company computers managed in Microsoft Intune are not all encrypted. 6 of 54 computers not encrypted.

What Microsoft 365 can't show: Judged for devices managed by Intune.

Email security

● Partly

Mail filtered, domains protected against spoofing, no forwarding outside.

Mail filtered for phishing and malware

● Pass

Incoming email is filtered for phishing and malware.

WHAT WE FOUND

- Incoming email for fabrikam.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 fabrikam.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

● 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.
 - fabrikam.example: Microsoft 365 DKIM isn't set up (selector2 CNAME missing)
- 2 domains without DMARC enforcement.
 - fabrikam.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 outside the organisation is blocked.

WHAT WE FOUND

- The default outbound policy blocks automatic external forwarding.

GAPS

- 5 external forwards.
 - anna.kowalski@fabrikam.example: Mailbox forwarding to anna.kowalski@homemail.example (keeps a copy)
 - anna.kowalski@fabrikam.example: Inbox rule "Copy to home" forwards to anna.kowalski.home@homemail.example
 - rhys.hall@fabrikam.example: Mailbox forwarding to rhys.hall@homemail.example (doesn't keep a copy)
 - rhys.walker@fabrikam.example: Mailbox forwarding to rhys.walker@homemail.example (doesn't keep a copy)
 - thomas.robinson@fabrikam.example: Inbox rule "Invoices to bookkeeper" forwards to bookkeeping@ledgerline.example
- 1 suspicious inbox rule.
 - anna.kowalski@fabrikam.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 5 external forwards found.

What Microsoft 365 can't show: Judged from the Exchange Online outbound spam policy, mailbox forwarding and inbox rules.

Devices ● Fail

Managed to a baseline, supported, patched quickly and protected by anti-malware.

Devices managed to a baseline ● Partly

Devices are centrally managed and must meet a security baseline.

WHAT WE FOUND

- Computers managed by Intune: 54
- Of which encrypted: 48
- Windows computers out of support: 7
- Reaching end of support within 90 days: 29
- Not compliant: 9

GAPS

- 1 of 55 joined computers not in Intune.
 - DESK-RECEPTION: Hybrid joined, not managed by Intune
- 9 of 55 managed devices not compliant.
 - DESK-LEWIS12 (william.lewis@fabrikam.example): Not compliant
 - DESK-MOORE18 (ava.moore@fabrikam.example): Not compliant
 - DESK-ROBINSON51 (owen.robinson@fabrikam.example): Not compliant
 - LAPTOP-DAVIES38 (ruby.davies@fabrikam.example): Not compliant
 - LAPTOP-LEE25 (arthur.lee@fabrikam.example): Not compliant
 - and 4 more

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 55 joined computers not in Intune. 9 of 55 managed devices not compliant.

What Microsoft 365 can't show: Judged from Intune enrolment and compliance for devices joined to Entra ID.

Supported operating systems

● Fail

Every operating system is still supported by its vendor.

GAPS

- 7 of 54 Windows computers past end of support.
 - LAPTOP-HARRIS31 (noah.harris@fabrikam.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-JACKSON49 (chloe.jackson@fabrikam.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-OKAFOR (ben.okafor@fabrikam.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-SMITH13 (owen.smith@fabrikam.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-WALKER04 (rhys.walker@fabrikam.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - and 31 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. 7 of 54 Windows computers past end of support.

What Microsoft 365 can't show: Judged for Windows computers known to Intune or Entra ID.

Security updates applied quickly

● Pass

Security updates are applied within an agreed time, 14 days for critical ones.

WHAT WE FOUND

- But: 5 devices haven't checked in for 30+ days.

Text to paste: Windows updates install through Intune update rings with a 3-day deferral, and Harbour IT checks every Monday that no device is more than 14 days behind. Router and firewall firmware is updated within 14 days of a security release by Harbour IT. Set by demo on 12 Oct 2026.

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

Anti-malware on every device

● Pass

Anti-malware software is installed and kept up to date on all devices.

WHAT WE FOUND

- But: 9 of 55 managed devices not compliant.

Text to paste: All laptops and desktops run Microsoft Defender Antivirus with Defender for Endpoint, which updates automatically, scans files on access and blocks malicious websites through SmartScreen. Phones and tablets only install apps from the Apple App Store and Google Play, enforced by Intune. Set by demo on 12 Oct 2026.

What Microsoft 365 can't show: Office Sentry doesn't read Microsoft Defender or anti-malware settings.

Logging and monitoring

● Not collected

Security events logged, suspicious activity watched, vulnerabilities looked for.

Security events logged

● Pass

Security events are logged and kept.

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 activity monitored

● Not collected

Suspicious sign-ins and users are detected and responded to.

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).

Vulnerability scanning or penetration testing

● Your evidence

Vulnerability scans or penetration tests are carried out and findings fixed.

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

Incidents, backups and continuity

● Your evidence

A plan for incidents (and telling the client), tested backups, and continuity plans.

Incident response and notification

● Your evidence

An incident response plan exists and clients are told about incidents affecting their data.

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.

Backups and tested restores

● Pass

Data is backed up and restores are tested.

Text to paste: Microsoft 365 mail, OneDrive, SharePoint and Teams data is backed up daily by Datto SaaS Protection to storage separate from Microsoft 365, kept for 12 months, with credentials separate from the Microsoft 365 administrator accounts. The last restore test was on 2 September 2026. Set by demo on 12 Oct 2026.

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

Continuity and recovery plans

● Your evidence

Business continuity and disaster recovery plans exist.

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.

Third parties, people and premises

● Fail

Apps and sub-processors under control, staff trained and vetted, premises secured, and a firewall with MFA on remote access.

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.

Cloud services and sub-processors

● Pass

The cloud services and sub-processors that hold the client's data.

WHAT WE FOUND

- Microsoft 365 (Microsoft 365 Business Basic, Microsoft 365 Business Premium). Cloud services connected to Microsoft 365 sign-in: Mail Sync Pro, Survey Tool, Zoom.

What Microsoft 365 can't show: Microsoft 365 lists the apps connected to its sign-in; add the rest.

Security awareness training

● Your evidence

Staff receive security awareness 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.

Staff vetted before access

● Your evidence

Staff are vetted before they're given access.

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

Premises and equipment secured

● Your evidence

Premises and equipment are physically secured.

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

Network protected by firewalls

● Pass

The network is protected by firewalls.

Text to paste: A WatchGuard Firebox T45 firewall protects the internet connection at the Manchester practice, and the Leeds practice uses the same model. Home and remote workers are protected by the Microsoft Defender Firewall on their company laptops, enforced by Intune. Set by demo on 12 Oct 2026.

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

MFA on remote access

● Your evidence

Remote access is protected by 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.

Answers for the form

What clients ask in supplier and vendor due-diligence questionnaires. Use the text for the matching question on the client's 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.

Governance

Question	Answer	Text to paste
Do you have documented information security policies?	● Your input	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. Why: Microsoft 365 can't show this.
Do you hold any security certifications, such as Cyber Essentials or ISO 27001?	● Your input	The organisation holds [Cyber Essentials or Cyber Essentials Plus or ISO 27001] certification, number [certificate number], valid until [date]. Why: Microsoft 365 can't show this.

Access control

Question	Answer	Text to paste
Is multi-factor authentication required for all users?	● 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@fabrikam.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.

Question	Answer	Text to paste
Is multi-factor authentication required for privileged 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@fabrikam.example (excluded from "CA001 — Admins: Require phishing-resistant MFA", "CA002 — All users: Require MFA", "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.
Do administrators use phishing-resistant MFA?	● No	Administrator accounts don't all use phishing-resistant sign-in methods yet. 2 admins without a phishing-resistant method.
Do you avoid weaker MFA methods such as text messages?	● No	Some users rely on a text message or phone call as their only second factor. 4 people can only use a text or call as a second factor.
Are administrative accounts separate from standard user accounts?	● 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: anna.kowalski@fabrikam.example. Still to check: Covers Microsoft 365 admin roles. Add local administrator, server and domain admin accounts.
Is privileged access restricted and tracked?	● Partly	Administrator role assignments in Microsoft 365 are tracked, with gaps. 4 accounts hold privileged admin roles, 2 of them Global Administrator (anna.kowalski@fabrikam.example, breakglass@fabrikam.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.
Does every user have a unique account, with no shared logins?	● Yes	Each person signs in to Microsoft 365 with their own named account. Shared mailboxes can't be signed in to directly; people reach them through their own accounts. All 3 shared mailboxes block sign-in. Still to check: Check devices, line-of-business apps and other systems for shared logins.

Question	Answer	Text to paste
Describe your password policy.	● Answered	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). Still to check: The password rules are Microsoft's defaults, not read from the tenant. Add other systems that use passwords (devices, servers, other cloud services).
How quickly is access removed when someone leaves?	● No	Some inactive accounts in Microsoft Entra ID have not been disabled. 7 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.
Is access by guests and external users reviewed?	● No	Guest and external user accounts are not reviewed regularly. 1 guest account: 1 guest inactive for 90+ days or never signed in (g#EXT#@fabrikam.example). Still to check: Say how often guest access is reviewed, and by whom.

Data protection

Question	Answer	Text to paste
Where is our data stored?	● Answered	Email, files and Teams data are held in Microsoft 365, in Microsoft's datacentres. Still to check: Confirm the data location in the Microsoft 365 admin centre (Settings > Org settings > Organization profile > Data location), and add data held anywhere else.
Is data encrypted at rest and in transit?	● Partly	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: 6 of 54 computers not encrypted. Still to check: The Microsoft 365 encryption is Microsoft's own, not read from the tenant. Add servers, backups and other systems.
How do you stop data being shared with unauthorised people?	● No	Sharing with anonymous and external users is not restricted in SharePoint and OneDrive. Anyone, including anonymous links. 2 files and folders shared with anyone. Anyone, including guests, can invite guests.
Are laptops and other portable devices encrypted?	● No	Company computers managed in Microsoft Intune are not all encrypted. 6 of 54 computers not encrypted. Still to check: Covers computers managed by Intune. Add any computers that aren't.

Email security

Question	Answer	Text to paste
How is email protected against phishing and malware?	● Yes	Incoming email is filtered for spam, phishing and malware. Incoming email for fabrikam.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.
Do you use SPF, DKIM and DMARC to stop your domains being spoofed?	● 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 outside the organisation blocked?	● Partly	Automatic forwarding to external addresses is restricted in Exchange Online, with exceptions. The default outbound policy blocks automatic external forwarding. But 5 external forwards found.

Devices

Question	Answer	Text to paste
Are devices centrally managed and required to meet a security baseline?	● No	Company devices are not all managed centrally. 1 of 55 joined computers not in Intune. 9 of 55 managed devices not compliant. Still to check: Covers devices joined to Entra ID. Add any company devices that aren't.
Are all operating systems supported by their vendor?	● No	Managed Windows computers run versions of Windows that no longer receive security updates. 7 of 54 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.
How quickly are security updates applied?	● Yes	Windows updates install through Intune update rings with a 3-day deferral, and Harbour IT checks every Monday that no device is more than 14 days behind. Router and firewall firmware is updated within 14 days of a security release by Harbour IT. Set by demo on 12 Oct 2026.
Is anti-malware software installed and kept up to date on all devices?	● Yes	All laptops and desktops run Microsoft Defender Antivirus with Defender for Endpoint, which updates automatically, scans files on access and blocks malicious websites through SmartScreen. Phones and tablets only install apps from the Apple App Store and Google Play, enforced by Intune. Set by demo on 12 Oct 2026.

Logging and monitoring

Question	Answer	Text to paste
Are security events logged?	☒ 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 and respond to suspicious activity?	☐ 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.
Do you carry out vulnerability scanning or penetration testing?	☐ Your input	External vulnerability scans run [monthly] using [tool or provider]. [A penetration test was last carried out on (date) by (provider).] Why: Microsoft 365 can't show this.

Incidents, backups and continuity

Question	Answer	Text to paste
Do you have an incident response plan, and would you tell us about an incident affecting our data?	☐ 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.
Is data backed up, and are restores tested?	☒ Yes	Microsoft 365 mail, OneDrive, SharePoint and Teams data is backed up daily by Datto SaaS Protection to storage separate from Microsoft 365, kept for 12 months, with credentials separate from the Microsoft 365 administrator accounts. The last restore test was on 2 September 2026. Set by demo on 12 Oct 2026. Still to check: Add servers and any data held outside Microsoft 365.
Do you have business continuity and disaster recovery plans?	☐ 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.

Third parties

Question	Answer	Text to paste
How do you control third-party applications' access to data?	☐ 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.

Question	Answer	Text to paste
Which cloud services and sub-processors do you use?	● Answered	Microsoft 365 (Microsoft 365 Business Basic, Microsoft 365 Business Premium). Cloud services connected to Microsoft 365 sign-in: Mail Sync Pro, Survey Tool, Zoom. Still to check: Add cloud services people sign in to with separate accounts (accounting, payroll, CRM, file transfer, social media); Microsoft 365 can't see them.

People and premises

Question	Answer	Text to paste
Do staff receive security awareness 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.
Are staff vetted before they're given access?	● Your input	New staff go through [right-to-work, reference and DBS] checks before they get access, and sign [confidentiality agreements]. Why: Microsoft 365 can't show this.
How are your premises and equipment secured?	● Your input	Offices are protected by [locked doors, access control and alarms]. [Servers and network equipment are kept in a locked room or cabinet.] Why: Microsoft 365 can't show this.

Network

Question	Answer	Text to paste
Is your network protected by firewalls?	● Yes	A WatchGuard Firebox T45 firewall protects the internet connection at the Manchester practice, and the Leeds practice uses the same model. Home and remote workers are protected by the Microsoft Defender Firewall on their company laptops, enforced by Intune. Set by demo on 12 Oct 2026.
Is remote access protected by multi-factor authentication?	● 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.

About this evidence

Scope: the client's customer asks about the client's whole business. A Pass here covers Microsoft 365; the answer should say what covers the rest.

Requirements: Supplier and vendor due-diligence questionnaires as commonly worded in 2026. Questions drawn from the supplier security questionnaires UK organisations send their suppliers, in their typical wording; no organisation'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 12 Oct 2026, 17:16 UTC. Accepted risks are exceptions the organisation has reviewed and documented. Complete the [parts in brackets] before using a text.