



Harbour IT

SECURITY CONTROLS EVIDENCE

Fabrikam Dental Group

PREPARED BY

Harbour IT

DATE

9 October 2026

FOR

Cyber insurance and security questionnaires

MICROSOFT 365 TENANT

fabrikam.onmicrosoft.com

● Gaps to close

Fabrikam Dental Group has 6 controls insurers ask about that are not in place.

IN THIS REPORT

Summary	2
Gaps to close	2
Questionnaire answers	3
Controls, one by one	5
About this evidence	9

Summary

Of the 13 controls cyber insurers usually ask about, 1 is in place, 4 are partly in place and 6 are not in place. 2 controls can't be seen in Microsoft 365 data (such as backups and staff training) and need evidence from elsewhere.

Every answer comes from settings and accounts read directly from Microsoft 365, not from a self-assessment.

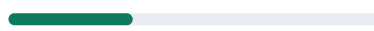
13 controls checked



■ 1 In place ■ 4 Partly in place ■ 6 Not in place ■ 2 Not assessed

Microsoft Secure Score

33%



Microsoft's own measure of recommended security settings

Gaps to close

The controls insurers are most likely to query. Closing these usually improves the answers on the form straight away.

- 1 Is multi-factor authentication required for all users accessing email and cloud apps?**
 MFA is enforced for all users: Enforced by Require MFA for all users, with 1 exclusion to review.
[See page 5](#)
- 2 Is MFA required for all privileged and administrator accounts?**
 Every admin has MFA registered: 1 admin without MFA, and 1 whose registration isn't known.
[See page 5](#)
- 3 Are legacy authentication protocols (which can't do MFA) blocked?**
 Legacy authentication is blocked: Legacy authentication is allowed. [See page 6](#)

Questionnaire answers

The questions cyber insurers usually ask, worded as they ask them, answered from the Microsoft 365 data. "Not known" means the data can't show it. Answers marked with a name were set by your technical lead.

Question	Answer	Why
Is MFA enforced for all remote access and email access?	● Yes	Enforced by Conditional Access ("Require MFA for all users") for everyone except 1 named exclusion: breakglass@fabrikam.example (break-glass). Evidence: MFA coverage: accounts with a gap report
Is MFA enforced for all privileged and administrator accounts?	● Yes	2 of 3 active admin accounts are required to use MFA by "Require MFA for all users"; the exception is 1 break-glass account: breakglass@fabrikam.example (excluded from "Require MFA for all users"). Evidence: Admins and roles: privileged role holders report
Is legacy authentication blocked?	● No	Legacy authentication is allowed. No enabled policy blocks legacy sign-in for all users. Evidence: Legacy sign-ins: what each mailbox allows report
Are admin accounts separate from day-to-day user accounts?	● Partly	1 of 3 admin accounts also has a licence or mailbox, so it looks like an everyday account: anna.kowalski@fabrikam.example. Evidence: Admins and roles: privileged role holders report
Is automatic forwarding of email to external addresses blocked?	● Partly	Outbound policies block automatic external forwarding. But 5 external forwards found. Evidence: Mail forwarding report
Are SPF, DKIM and DMARC in place for your email domains?	● No	1 domain with SPF problems. 1 mail domain without DKIM. 2 domains without DMARC enforcement. Evidence: Email domains report
Are mailbox audit logs enabled?	● Yes	Mailbox auditing is on for the organisation. Evidence: Audit logging control, below
Are company laptops and desktops encrypted?	● No	6 of 54 computers not encrypted. Evidence: Devices: managed devices report
Are company devices centrally managed and required to meet security policies?	● No	1 of 55 joined computers not in Intune. 9 of 55 managed devices not compliant. Evidence: Devices: managed devices report
Are all devices on operating systems that still receive security updates?	● No	7 of 54 Windows computers past end of support. Evidence: Devices: operating systems report
Are leavers' and inactive accounts disabled promptly?	● No	7 accounts inactive for 90+ days or never used. 1 disabled account still licensed. Evidence: Inactive accounts report
Do you review guest and external user access?	● Yes	There are no guest accounts. Evidence: Inactive accounts: inactive guests report

Question	Answer	Why
Is sharing of files with anonymous or external users restricted?	● No	Anyone, including anonymous links. 2 files and folders shared with anyone. Anyone, including guests, can invite guests. Evidence: Guests and sharing: external access settings report
Is access to your data by third-party applications controlled?	● No	Users can consent to any app. 1 app with access to mail, files or the directory. Evidence: Apps and consents report
Do you back up Microsoft 365 data (email, OneDrive, SharePoint) separately?	● Not known	Backups aren't visible in Microsoft 365 data. Answer from the backup product's records.
Do staff receive regular security awareness and phishing training?	● Not known	Training isn't visible in Microsoft 365 data. Answer from the training provider's records.

Controls, one by one

"Partly in place" means the control exists but has the gaps listed. "Not assessed" means Microsoft 365 can't show it, so evidence has to come from elsewhere.

Is multi-factor authentication required for all users accessing email and cloud apps?

● Not in place

WHAT WE FOUND

- 50.9% of checked users have registered an MFA method.
- 54 of 54 enabled accounts are covered by an enforced Conditional Access policy requiring MFA.

GAPS

- MFA is enforced for all users: Enforced by Require MFA for all users, with 1 exclusion to review.
breakglass@fabrikam.example: Excluded from "Require MFA for all users"
- Every active user has MFA registered: 27 users without MFA.
breakglass@fabrikam.example: No MFA method registered
aaron.smith@fabrikam.example: No MFA method registered
aisha.brown@fabrikam.example: No MFA method registered
amelia.khan@fabrikam.example: No MFA method registered
arthur.williams@fabrikam.example: No MFA method registered
...and 22 more

Is MFA required for all privileged and administrator accounts?

● Not in place

WHAT WE FOUND

- Phishing-resistant MFA (passkeys, security keys, Windows Hello): 2 admins without a phishing-resistant method.

GAPS

- Every admin has MFA registered: 1 admin without MFA, and 1 whose registration isn't known.
breakglass@fabrikam.example: Global Administrator with no MFA method registered
g#EXT#@fabrikam.example: Exchange Administrator: MFA registration unknown
- Every admin is covered by an MFA policy: 1 admin not covered by MFA.
breakglass@fabrikam.example: Global Administrator: excluded from Require MFA for all users

Are legacy authentication protocols (which can't do MFA) blocked?

● Not in place

GAPS

- Legacy authentication is blocked: Legacy authentication is allowed.
No enabled policy blocks legacy authentication for all users
- SMTP AUTH is turned off: SMTP AUTH is on for the organisation.
SMTP AUTH is allowed

Is administrative access limited to named, internal accounts?

● Partly in place

WHAT WE FOUND

- 2 Global Administrators.
- No guest holds a privileged role.
- Cloud-only tenant: no accounts are synced from on-premises AD.

GAPS

- Apps with admin roles are reviewed: 1 app with privileged roles.
Some app: App holding Exchange Administrator

Are SPF, DKIM and DMARC configured for your email domains?

● Partly in place

GAPS

- Every domain has a working SPF record: 1 domain with SPF problems.
parked.example: Doesn't receive mail but has no "v=spf1 -all" record to stop spoofing
- DKIM signing is on for every mail domain: 1 mail domain without DKIM.
fabrikam.example: Microsoft 365 DKIM isn't set up (selector2 CNAME missing)
- Every domain enforces DMARC: 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

Is automatic forwarding of email to external addresses blocked or monitored?

● **Partly in place**

WHAT WE FOUND

- Outbound policies block automatic external forwarding.

GAPS

- No mail is forwarded outside the organisation: 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
- No inbox rules hide mail: 1 suspicious inbox rule.
 anna.kowalski@fabrikam.example: ".": Moves to RSS Feeds mail mentioning invoice, payment; Rule name '.' looks deliberately blank

Is audit logging enabled for email and user activity?

● **In place**

WHAT WE FOUND

- Mailbox auditing is on for the organisation.

Are inactive and leavers' accounts disabled promptly?

● **Partly in place**

WHAT WE FOUND

- No stale guest invitations.

GAPS

- No inactive accounts: 7 accounts inactive for 90+ days or never used.
 - aaron.smith@fabrikam.example: Licensed member, last signed in 20 Apr 2026
 - aisha.brown@fabrikam.example: Licensed member, last signed in 4 Mar 2026
 - jack.lee@fabrikam.example: Licensed member, last signed in 1 Jun 2026
 - noah.wood@fabrikam.example: Licensed member, last signed in 4 Feb 2026
 - rhys.walker@fabrikam.example: Licensed member, last signed in 2 Jun 2026
 - ...and 2 more
- No licences on disabled accounts: 1 disabled account still licensed.
 - ben.okafor@fabrikam.example: Disabled, holding 1 licence

Is access by third-party applications controlled?

● **Not in place**

GAPS

- Users can't consent to apps on their own: Users can consent to any app.
 - Any user can grant any app access to their mail and files
- Third-party apps hold only the access they need: 1 app with access to mail, files or the directory.
 - Mail Sync Pro: Mail.Read (application permission; unverified publisher)

Is external file sharing restricted?

● **Not in place**

GAPS

- Files can't be shared with anonymous links: Anyone, including anonymous links.
 - SharePoint and OneDrive: Anyone links are allowed
- No files are shared with anyone links: 2 files and folders shared with anyone.
 - Clients (Finance / Documents): Anyone can edit, link never expires
 - holiday.jpg (OneDrive of anna.kowalski@fabrikam.example): Anyone can view
- Only admins and members can invite guests: Anyone, including guests, can invite guests.
 - Guests can invite other guests

Are company devices managed, encrypted and kept on supported operating systems?

● Not in place

GAPS

- Company computers are encrypted: 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
- Managed devices meet compliance policies: 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
- Windows computers still get security updates: 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

Are backups of Microsoft 365 data taken and kept separately?

● Not assessed

Backups are outside what Microsoft 365 reports. Provide evidence from the backup product.

Do staff receive security awareness and phishing training?

● Not assessed

Training isn't visible in Microsoft 365 data. Provide records from the training provider.

About this evidence

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Collected from Microsoft 365 with read-only access; nothing was changed. The oldest data used was collected 9 Oct 2026, 23:27 UTC. Accepted risks are exceptions the organisation has reviewed and documented.