



Harbour IT

CYBER ESSENTIALS PLUS EVIDENCE

Fabrikam Dental Group

PREPARED BY

Harbour IT

DATE

14 October 2026

EVIDENCE DATE

14 Oct 2026

SCHEME

NCSC and IASME

MICROSOFT 365 TENANT

fabrikam.onmicrosoft.com

● Not ready

Fabrikam Dental Group has 5 controls to fix before applying for CE Plus.

IN THIS REPORT

Summary	2
Fix before you apply	3
Firewalls	4
Secure configuration	6
Security update management	8
User access control	10
Malware protection	15
What the assessor checks	16
Answers for the form	18
About this evidence	24

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

Confidential. This report describes security settings for Fabrikam Dental Group; share it only with people who need it.

Summary

Fabrikam Dental Group has 5 controls to fix before applying for CE Plus.

The same five controls as Cyber Essentials, audited: a certification body tests a sample of devices and every cloud service against the locked self-assessment. Use the verdicts to clear every gap before the assessor's visit; the self-assessment can't be changed once testing starts.

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

29 controls



 **7** Pass  **5** Fail  **2** Partly  **15** Your evidence

Fix before you apply

An assessor won't accept a gap in these. Each one names the accounts or settings behind it and the fix.

1 A7.17 MFA for every user of cloud services (auto-fail)

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). Fix: Require MFA for all users and all apps with a Conditional Access policy (or turn on Security Defaults), with only a named break-glass account excluded, then chase everyone not yet registered.

2 A5.1 (cloud services) Unneeded sign-in protocols turned off in Microsoft 365

Legacy authentication is allowed. Fix: Block legacy authentication.

3 A6.1 Every operating system still supported by its vendor

36 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 A7.3 Leavers' accounts disabled or deleted

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.

5 A7.6 Separate accounts for administration

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.

6 A5.2 Only the accounts that are needed

1 disabled account still licensed. Fix: Remove licences from disabled accounts, or convert leavers' mailboxes to shared mailboxes.

7 A7.8 Administrator accounts tracked and reviewed

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

Firewalls

● Your evidence

Every device and network in scope sits behind a firewall that blocks unauthenticated inbound connections by default, with changed passwords, reviewed rules and no administration from the internet.

A4.1 A firewall at every boundary with the internet

● Pass

A boundary firewall (or the router's firewall) protects each internet connection, and home workers are protected by the firewall on their device.

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 14 Oct 2026.

What Microsoft 365 can't show: Firewalls aren't part of Microsoft 365. Intune can enforce the Windows firewall, but reading its configuration profiles needs a permission the app doesn't hold, so answer from the firewall itself.

A4.1.1 Software firewalls on every computer and server

● Pass

The built-in firewall is turned on for every laptop, desktop and server.

Text to paste: Microsoft Defender Firewall is turned on for every Windows laptop and desktop and enforced by an Intune endpoint security policy; the two Macs use the built-in macOS firewall. Set by demo on 14 Oct 2026.

What Microsoft 365 can't show: Firewalls aren't part of Microsoft 365. Intune can enforce the Windows firewall, but reading its configuration profiles needs a permission the app doesn't hold, so answer from the firewall itself.

A4.2 Default firewall passwords changed

● Your evidence

The default administrator password of every router and firewall was changed to a strong one.

Text to paste: The default administrator passwords on all firewalls and routers were changed when they were installed, to [unique passwords of at least 12 characters, kept in a password manager].

What Microsoft 365 can't show: Firewalls aren't part of Microsoft 365. Intune can enforce the Windows firewall, but reading its configuration profiles needs a permission the app doesn't hold, so answer from the firewall itself.

A4.6 Firewall rules reviewed in the last 12 months

● Your evidence

Inbound rules are reviewed and removed when no longer needed, at least yearly.

Text to paste: Firewall rules are reviewed [every 12 months] by [IT provider], and rules that are no longer needed are removed. The last review was on [date].

What Microsoft 365 can't show: Firewalls aren't part of Microsoft 365. Intune can enforce the Windows firewall, but reading its configuration profiles needs a permission the app doesn't hold, so answer from the firewall itself.

A4.7 Unauthenticated inbound connections blocked by default

● Your evidence

The firewall blocks inbound connections unless an approved, documented rule allows one (A4.8).

Text to paste: Firewalls block all inbound connections by default. [No inbound connections are allowed.] or [Each allowed inbound connection is documented, with its business need approved by (role).]

What Microsoft 365 can't show: Firewalls aren't part of Microsoft 365. Intune can enforce the Windows firewall, but reading its configuration profiles needs a permission the app doesn't hold, so answer from the firewall itself.

A4.9 No firewall administration from the internet

● Your evidence

The firewall's administration interface can't be reached from the internet, or only with MFA or from an allow list of trusted addresses with a documented need (A4.10, A4.11).

Text to paste: The firewall's administration interface can't be reached from the internet. [Or: remote administration is limited to (trusted IP addresses) and protected by multi-factor authentication.]

What Microsoft 365 can't show: Firewalls aren't part of Microsoft 365. Intune can enforce the Windows firewall, but reading its configuration profiles needs a permission the app doesn't hold, so answer from the firewall itself.

Secure configuration

● Fail

Devices and cloud services run only the software, services and accounts they need, with default passwords changed, automatic running of files off and devices that lock.

A5.1 Unused software and services removed from devices

● Your evidence

Software and services nobody uses are removed or turned off on every device.

Text to paste: New devices are set up from [a standard build or Windows Autopilot] without unnecessary software, and unused software and services are removed [during regular reviews by the IT provider].

What Microsoft 365 can't show: Microsoft 365 doesn't report what's installed on devices.

A5.1 (cloud services) Unneeded sign-in protocols turned off in Microsoft 365

● Fail

Services that aren't needed are turned off in cloud services too: for Microsoft 365, the legacy sign-in protocols that can't use MFA, and SMTP AUTH on mailboxes that don't send mail that way.

GAPS

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

Fix: Block legacy authentication (Exchange ActiveSync and other clients) with a Conditional Access policy for all users. Legacy protocols can't do MFA and are the most common password-spray target.

Text to paste: Legacy authentication is allowed. SMTP AUTH is on for the organisation.

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

A5.2 Only the accounts that are needed

● **Partly**

Devices and cloud services hold only the user accounts in use: no leftover licensed-but-disabled accounts and no forgotten guest invitations.

WHAT WE FOUND

- No stale guest invitations.

GAPS

- 1 disabled account still licensed.
 - ben.okafor@fabrikam.example: Disabled, holding 1 licence

Fix: Remove licences from disabled accounts, or convert leavers' mailboxes to shared mailboxes (free up to 50 GB) before removing the licence.

Text to paste: No stale guest invitations. 1 disabled account still licensed.

What Microsoft 365 can't show: Judged from Microsoft Entra ID accounts and guest invitations. Add local accounts on devices and servers.

A5.3 Default passwords changed on every device and account

● **Your evidence**

Default and built-in account passwords are changed at set-up.

Text to paste: Default and built-in accounts on devices are turned off or given new passwords at set-up. [Local administrator passwords are managed by Windows LAPS.]

What Microsoft 365 can't show: Microsoft 365 accounts have no default password; this is about devices and built-in accounts.

A5.8 Automatic running of downloaded files turned off

● **Your evidence**

AutoRun and AutoPlay are off, and downloaded files don't run without the user's say-so.

Text to paste: AutoPlay and AutoRun are turned off on Windows computers [by Intune policy], and downloaded files can't run without the user's permission.

What Microsoft 365 can't show: Office Sentry doesn't read device configuration profiles from Intune, so answer from the Intune policy.

A5.9 Devices lock and need a PIN, password or biometric

● **Your evidence**

Every device locks after inactivity and unlocks with a password, PIN of at least six digits or biometric (A5.10), with brute-force protection.

Text to paste: Computers lock after [5 to 15] minutes of inactivity and need a password, PIN or Windows Hello to unlock. Phones and tablets need a PIN of at least 6 digits or biometrics [enforced by Intune].

What Microsoft 365 can't show: Office Sentry doesn't read device configuration profiles from Intune, so answer from the Intune policy.

Security update management

● Fail

Every operating system and application is supported by its vendor, licensed, set to update automatically where possible, and has high-risk and critical updates installed within 14 days.

A6.1 Every operating system still supported by its vendor

● Fail

All operating systems in scope receive regular security updates from their vendor; Windows 10 needs Extended Security Updates after October 2025.

WHAT WE FOUND

- Computers managed by Intune: 54
- Of which encrypted: 48
- Windows computers out of support: 36
- Not compliant: 9

GAPS

- 36 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. 36 of 54 Windows computers past end of support.

What Microsoft 365 can't show: Judged for Windows computers known to Intune or Entra ID. macOS, Linux, phones, servers not joined to Entra ID and router or firewall firmware aren't seen.

A6.2 Every application supported and licensed

● Your evidence

Browsers, anti-malware, email and office applications are supported versions (A6.2.1 to A6.2.4), nothing is unlicensed or unsupported (A6.3, A6.6), and any unsupported software is on a separate sub-set (A6.7).

Text to paste: All software in use is supported by its vendor and licensed: [browser and version], [anti-malware product and version], [email application and version] and [office applications and version]. Software that is no longer supported has been removed[, or runs on a separate sub-set outside the scope].

What Microsoft 365 can't show: Microsoft 365 doesn't report installed application versions. Intune's discovered apps would need a permission the app doesn't hold.

A6.4 Operating system updates within 14 days (auto-fail)

● Pass

High-risk and critical security updates for operating systems, routers and firewalls are installed within 14 days of release, by automatic updates where possible (A6.4.1, A6.4.2).

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 14 Oct 2026.

What Microsoft 365 can't show: Intune shows which Windows release each computer runs and when it last checked in, not when updates were installed.

A6.5 Application updates within 14 days (auto-fail)

● Your evidence

High-risk and critical application updates are installed within 14 days of release, by automatic updates where possible (A6.5.1, A6.5.2).

Text to paste: Applications update automatically where they can (Microsoft 365 Apps, web browsers and [other software]). Updates that can't install automatically are applied within 14 days of release by [process or tool].

What Microsoft 365 can't show: Microsoft 365 doesn't see application versions on devices.

User access control

● Fail

Accounts are created through a process, are unique to a person, hold only the access the job needs, are removed when people leave, use separate accounts for administration, strong passwords and MFA on every cloud service.

A7.1 Accounts created only through an approval process

● Your evidence

A user account is created only after a request has been approved and recorded.

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

What Microsoft 365 can't show: A process Microsoft 365 doesn't show. The directory audit log records who created each account.

A7.2 Every account used by one person, with unique credentials

● Pass

User and administrator accounts are each tied to a person: no shared sign-ins.

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 for shared logins.

A7.3 Leavers' accounts disabled or deleted

● Fail

Accounts of people who have left are disabled or deleted promptly, and no account sits unused.

GAPS

- 7 accounts inactive for 90+ days or never used.
 - aaron.smith@fabrikam.example: Licensed member, last signed in 24 Apr 2026
 - aisha.brown@fabrikam.example: Licensed member, last signed in 9 Mar 2026
 - jack.lee@fabrikam.example: Licensed member, last signed in 5 Jun 2026
 - noah.wood@fabrikam.example: Licensed member, last signed in 9 Feb 2026
 - rhys.walker@fabrikam.example: Licensed member, last signed in 7 Jun 2026
 - and 2 more

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 (needs Entra ID P1 for last sign-in dates). Describe the leavers process in the answer.

A7.4 Only the access the job needs

● Your evidence

Staff have the access their current role needs and no more, through role-based groups.

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

What Microsoft 365 can't show: A process Microsoft 365 doesn't show; the group membership and admin role reports help review it.

A7.5 A formal process for giving administrator access

● Your evidence

Administrator access is granted only after approval, to a named person, and recorded.

Text to paste: Administrator access is given only after approval by [role], to a separate named admin account, and is recorded in [ticket system or register].

What Microsoft 365 can't show: A process Microsoft 365 doesn't show.

A7.6 Separate accounts for administration

● Fail

Administration is done from separate admin accounts that aren't used for email, browsing or everyday work (A7.6, A7.7).

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. Add local and domain administrators on devices and servers.

A7.8 Administrator accounts tracked and reviewed

● Partly

The organisation knows which accounts hold administrator access (A7.8) and reviews the list regularly (A7.9).

WHAT WE FOUND

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

GAPS

- 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 often the list is reviewed and by whom.

A7.10 Passwords protected from guessing, with quality controls

● Pass

Passwords are protected from brute-force guessing (A7.10: MFA, throttling or lockout) and their quality is managed technically (A7.11: MFA, 12 characters, or 8 characters with a deny list).

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 devices, servers and other systems that take passwords.

A7.13 A process for a compromised password or account

● Your evidence

When a password or account may be compromised, it's reset and the account checked promptly.

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

What Microsoft 365 can't show: A process Microsoft 365 doesn't show; Entra ID Protection's risk detections support it.

A7.14 MFA available on every cloud service

● Your evidence

Every cloud service in use offers MFA, or is linked to one that does; any that don't are listed (A7.15).

Text to paste: All cloud services in use offer multi-factor authentication: Microsoft 365 (through Microsoft Entra ID) and [other cloud services]. [Or list any that don't offer it.]

What Microsoft 365 can't show: Microsoft 365 offers MFA through Entra ID. List the other cloud services and check each.

A7.16 MFA for every administrator of cloud services (auto-fail)

● Pass

Every administrator account on every cloud service uses MFA with a password of at least 8 characters. The assessment fails on a No.

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, from Conditional Access enforcement with named break-glass accounts allowed. Add administrators of other cloud services.

A7.17 MFA for every user of cloud services (auto-fail)

● Fail

Every user of every cloud service uses MFA with a password of at least 8 characters. The assessment fails on a No.

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).

Fix: Require MFA for all users and all apps with a Conditional Access policy (or turn on Security Defaults), with only a named break-glass account excluded, then chase everyone not yet registered.

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 from Conditional Access enforcement (or Security Defaults), with named break-glass accounts allowed. Add other cloud services.

Malware protection

● Pass

Every computer, tablet and phone is protected by anti-malware software that updates and scans, or only runs approved applications from a managed store.

A8.1 Anti-malware on every computer, tablet and phone

● Pass

Each device has anti-malware software that updates itself, scans files on access and blocks malicious websites (A8.2, A8.3), or installs apps only from an approved store or allow list (A8.4, A8.5).

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 14 Oct 2026.

What Microsoft 365 can't show: Office Sentry doesn't read Microsoft Defender or anti-malware settings. Intune compliance supports the answer only if the compliance policy requires anti-malware; check the policy.

What the assessor checks

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

Test 1: Remote vulnerability assessment

The assessor scans every internet-facing IP address the organisation uses and fails any service with a high or critical vulnerability, or that lets someone in without authentication.

Microsoft 365 shows: Microsoft 365 has no part in this test; it's about the firewall, routers and anything published to the internet. Have the firewall review and inbound rules ready.

Today: A4.7 ● Your evidence A4.9 ● Your evidence A4.6 ● Your evidence

Test 2: Patching, by authenticated vulnerability scan of sampled devices

A sample of computers, servers and cloud servers is scanned while signed in. Any high-risk or critical update older than 14 days, or an unsupported operating system or application, fails the test.

Microsoft 365 shows: The Windows release of each managed computer and whether it's still supported, so unsupported machines can be replaced before the sample is picked. Patch dates aren't visible.

Today: A6.1 ● Fail A6.4 ● Pass A6.5 ● Your evidence

Test 3: Malware protection on sampled devices

On each sampled device the assessor checks that anti-malware is installed, updating and scanning (or that only approved apps can install), then sends test files by email and downloads them in the browser: they must be blocked.

Microsoft 365 shows: Whether managed devices meet their Intune compliance policy, if that policy requires anti-malware. The email test lands in Exchange Online: Exchange Online Protection or the mail gateway must block it.

Today: A8.1 ● Pass

Test 4: Multi-factor authentication on cloud services

Users and administrators of sampled devices sign in to each cloud service from an untrusted browser session. A Pass needs an MFA prompt before access, for every authentication service in use.

Microsoft 365 shows: Exactly this for Microsoft 365: the Conditional Access policies (or Security Defaults) that require MFA, every account not covered, and the admins without an MFA method. Fix every gap first.

Today: A7.17 ● Fail A7.16 ● Pass

Test 5: Account separation

On each sampled device a standard user tries to run an administrative task. A Pass needs a prompt for separate administrator credentials.

Microsoft 365 shows: Whether Microsoft 365 admin roles sit on separate accounts rather than the ones people use every day. Local administrator rights on the devices themselves aren't visible.

Today: A7.6  **Fail**

Answers for the form

The Cyber Essentials self-assessment questions Microsoft 365 helps with, by their number in the IASME portal, plus the ones about firewalls, updates and processes it can't see. Questions marked auto-fail fail the whole assessment on a No. "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.

A2 Scope of assessment

Question	Answer	Text to paste
A2.4.2 How are home and remote workers connecting to company data and services?	● Your input	Home and remote workers connect over [home broadband or business-provided routers] to Microsoft 365, with multi-factor authentication. [Office systems are reached through (VPN product).] Why: Microsoft 365 can't show this. It sees where people sign in from, not how their network connects.
A2.6 List the quantities and operating systems of your laptops, desktops and virtual desktops.	● Answered	54 computers managed in Microsoft Intune: 13 Dell computers running Windows 11 24H2; 7 HP computers running Windows 11 24H2; 6 Dell computers running Windows 11 25H2; 5 Lenovo computers running Windows 11 24H2; 5 Lenovo computers running Windows 11 25H2; 5 Microsoft computers running Windows 11 25H2; 4 Microsoft computers running Windows 11 24H2; 3 Dell computers running Windows 10; 2 HP computers running Windows 10; 2 HP computers running Windows 11 25H2; 1 Lenovo computer running Windows 10; 1 Microsoft computer running Windows 10. Still to check: Microsoft 365 doesn't report the Windows edition (Pro, Enterprise): add it. Add any computers not managed by Intune or joined to Entra ID, and servers. Give the make and the operating system edition and version (for example Windows 11 Pro 24H2).
A2.8 List the quantities and operating systems of your tablets and mobile devices.	● Answered	1 device managed in Microsoft Intune: 1 Apple device running iOS 18.6. Still to check: Add personal phones and tablets (BYOD) that reach work email or files but aren't enrolled.
A2.9 List all the cloud services in use, provided by a third party.	● 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. Cloud services can't be left out of scope, and social media accounts count.

A4 Firewalls

Question	Answer	Text to paste
A4.1 Do you have firewalls at the boundaries between your networks, devices and the internet?	● 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 14 Oct 2026.
A4.1.1 Do you have software firewalls turned on for all computers, laptops and servers?	● Yes	Microsoft Defender Firewall is turned on for every Windows laptop and desktop and enforced by an Intune endpoint security policy; the two Macs use the built-in macOS firewall. Set by demo on 14 Oct 2026.
A4.2 Have you changed the default passwords on your boundary firewalls?	● Your input	The default administrator passwords on all firewalls and routers were changed when they were installed, to [unique passwords of at least 12 characters, kept in a password manager]. Why: Microsoft 365 can't show this. Firewalls aren't part of Microsoft 365.
A4.6 Have you reviewed your firewall rules in the last 12 months?	● Your input	Firewall rules are reviewed [every 12 months] by [IT provider], and rules that are no longer needed are removed. The last review was on [date]. Why: Microsoft 365 can't show this. Firewalls aren't part of Microsoft 365.
A4.7 Is your firewall set to allow unauthenticated inbound connections?	● Your input	Firewalls block all inbound connections by default. [No inbound connections are allowed.] or [Each allowed inbound connection is documented, with its business need approved by (role).] Why: Microsoft 365 can't show this. Firewalls aren't part of Microsoft 365. Still to check: The form asks this the other way round, so the answer shown is already swapped (the hoped-for answer is No).
A4.9 Can your boundary firewalls' settings be reached over the internet?	● Your input	The firewall's administration interface can't be reached from the internet. [Or: remote administration is limited to (trusted IP addresses) and protected by multi-factor authentication.] Why: Microsoft 365 can't show this. Firewalls aren't part of Microsoft 365. Still to check: The form asks this the other way round, so the answer shown is already swapped (the hoped-for answer is No). If they can, A4.10 and A4.11 ask for the business need and MFA.

A5 Secure configuration

Question	Answer	Text to paste
A5.1 Have you removed or turned off software and services you don't use?	● Your input	New devices are set up from [a standard build or Windows Autopilot] without unnecessary software, and unused software and services are removed [during regular reviews by the IT provider]. Why: Microsoft 365 can't show this.
A5.2 Do your devices and cloud services only have the user accounts you need and use?	● 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.
A5.3 Have you changed the default passwords on all user and administrator accounts on your devices?	● Your input	Default and built-in accounts on devices are turned off or given new passwords at set-up. [Local administrator passwords are managed by Windows LAPS.] Why: Microsoft 365 can't show this.
A5.8 Have you turned off features that run downloaded or imported files automatically?	● Your input	AutoPlay and AutoRun are turned off on Windows computers [by Intune policy], and downloaded files can't run without the user's permission. Why: Microsoft 365 can't show this. Office Sentry doesn't read device configuration profiles.
A5.9 Do devices lock and need a PIN, password or biometric to unlock?	● Your input	Computers lock after [5 to 15] minutes of inactivity and need a password, PIN or Windows Hello to unlock. Phones and tablets need a PIN of at least 6 digits or biometrics [enforced by Intune]. Why: Microsoft 365 can't show this. Office Sentry doesn't read device configuration profiles.

A6 Security update management

Question	Answer	Text to paste
A6.1 Are all operating systems on your devices supported by a vendor that produces regular security updates?	● No	Managed Windows computers run versions of Windows that no longer receive security updates. 36 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. Windows 10 needs Extended Security Updates after 14 October 2025. Router and firewall firmware counts as an operating system.
A6.2 Is all the software on your devices supported by a supplier that produces regular security updates, and licensed?	● Your input	All software in use is supported by its vendor and licensed: [browser and version], [anti-malware product and version], [email application and version] and [office applications and version]. Software that is no longer supported has been removed[, or runs on a separate sub-set outside the scope]. Why: Microsoft 365 can't show this. Office Sentry doesn't see which application versions are installed. Still to check: A6.2.1 to A6.2.4 ask for the browser, anti-malware, email and office applications with their versions.

Question	Answer	Text to paste
A6.4 Are high-risk and critical updates for operating systems, routers and firewalls installed within 14 days of release? (auto-fail)	● 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 14 Oct 2026.
A6.5 Are high-risk and critical updates for applications installed within 14 days of release? (auto-fail)	● Your input	Applications update automatically where they can (Microsoft 365 Apps, web browsers and [other software]). Updates that can't install automatically are applied within 14 days of release by [process or tool]. Why: Microsoft 365 can't show this. Office Sentry doesn't see which application versions are installed.

A7 User access control

Question	Answer	Text to paste
A7.1 Are user accounts only created after an approval process?	● Your input	New accounts are created only after a request from [manager or HR] is approved by [role], recorded in [ticket system]. Why: Microsoft 365 can't show this.
A7.2 Are all user and administrator accounts accessed with unique credentials?	● 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.
A7.3 How do you make sure leavers' accounts are deleted or disabled?	● 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.
A7.4 Do staff only have the access they need for their current job?	● Your input	Access to files and systems is given through role-based groups, approved by [role], and changed when people move roles. [Access is reviewed every 12 months.] Why: Microsoft 365 can't show this.
A7.5 Do you have a formal process for giving someone administrator access?	● Your input	Administrator access is given only after approval by [role], to a separate named admin account, and is recorded in [ticket system or register]. Why: Microsoft 365 can't show this.
A7.6 How do you make sure separate accounts are used for administrative tasks?	● 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.

Question	Answer	Text to paste
A7.7 How do you stop administrator accounts being used for everyday tasks like email and browsing?	● 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.
A7.8 Do you formally track which users have administrator accounts?	● 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.
A7.9 Do you review who should have administrative access regularly?	● Your input	Administrator access is reviewed [quarterly] by [role] against the list of current administrators, and anyone who no longer needs it has it removed. Why: Microsoft 365 can't show this. It shows who holds admin roles today (see the administrator access answer), not that a review happens.
A7.10 How are passwords protected from brute-force attacks?	● 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).
A7.13 Do you have a process for when passwords or accounts may be compromised?	● Your input	If an account may be compromised, [IT provider] resets the password, signs the account out of every session, checks its MFA methods and inbox rules, and reviews its sign-ins. Staff report concerns to [contact]. Why: Microsoft 365 can't show this.
A7.14 Do all of your cloud services offer multi-factor authentication?	● Your input	All cloud services in use offer multi-factor authentication: Microsoft 365 (through Microsoft Entra ID) and [other cloud services]. [Or list any that don't offer it.] Why: Microsoft 365 can't show this. It knows about Microsoft 365, which offers MFA; other cloud services need checking.

Question	Answer	Text to paste
A7.16 Has MFA been applied to all administrators of your cloud services? (auto-fail)	● 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. Covers every cloud service that offers MFA, not only Microsoft 365.
A7.17 Has MFA been applied to all users of your cloud services? (auto-fail)	● 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. Covers every cloud service that offers MFA, not only Microsoft 365.

A8 Malware protection

Question	Answer	Text to paste
A8.1 Are all desktops, laptops, tablets and phones protected from malware?	● 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 14 Oct 2026.

About this evidence

Scope: Cyber Essentials covers every device that reaches organisational data or services, every cloud service holding the organisation's data, and home workers' devices. Microsoft 365 is one cloud service in that scope, so a Pass here is evidence for the form, not the whole answer.

The answers must be approved by a board member or the business owner before submission.

Cyber Essentials Plus is taken within three months of the Cyber Essentials self-assessment, on the same scope. From v3.3 the self-assessment is locked before the first device is tested, and a difference between it and what the assessor finds is recorded as a finding.

The assessor samples devices from the inventory in A2.6 to A2.8: make sure it matches what Intune and Entra ID hold, since a device missing from the inventory can still be sampled.

Requirements: Cyber Essentials: Requirements for IT Infrastructure v3.3 (NCSC and IASME, April 2026) and IASME question set Danzell, version 16 (April 2026), for assessments bought from 27 April 2026; test cases from the Cyber Essentials Plus Test Specification (v3.2, April 2025; v3.3 applies to assessment accounts created from 27 April 2026). Requirements paraphrased from the NCSC and IASME Cyber Essentials documents; question numbers from IASME's self-assessment preparation booklet, checked 10 October 2026. IASME publishes a new question set most Aprils: check the portal's numbers before submitting. Test cases paraphrased from the NCSC's published Cyber Essentials Plus Test Specification; the certification body's own specification is the one that counts.

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.