



MONTHLY SECURITY & LICENSING REVIEW

Fabrikam Dental Group

PREPARED BY
Harbour IT

REPORT DATE
14 October 2026

PERIOD COVERED
16 September to 14 October 2026

MICROSOFT 365 TENANT
fabrikam.onmicrosoft.com

● **Action needed**

Fabrikam Dental Group's Microsoft 365 has a critical security gap that should be fixed now.

IN THIS REPORT

SUMMARY

At a glance	2
This month, and what we recommend next	3

APPENDIX: THE DETAIL

What changed since 16 September	4
Fix first.	6
Also worth fixing	12
Licences	16
In good shape	16
Not checked	17

At a glance

We ran 61 security checks and 46 need attention (1 critical, 14 high, 19 medium and 12 low priority). The most urgent: 1 admin without MFA, and 1 whose registration isn't known.

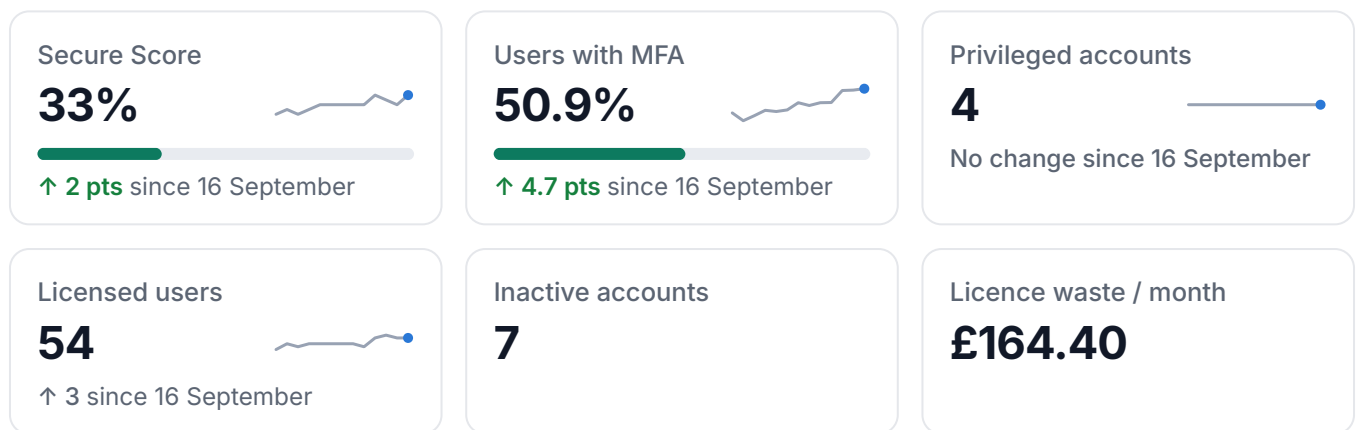
On the positive side, 15 checks passed, including "Between 2 and 4 Global Administrators", "Automatic forwarding to outside addresses is off" and "Shared mailboxes can't be signed in to".

Since 16 September, Microsoft Secure Score rose from 31% to 33%, users with MFA rose from 46.2% to 50.9%, 2 issues were fixed and 17 new items came up.

About £164.40 a month (£1,972.80 a year) goes on licences that are unused or assigned to disabled or inactive accounts.

7 checks couldn't run because the data or a licence they need is missing.

Key figures



46 of 61 checks need attention



This month



What we did

FIXED Every active user has MFA registered · 2 items: george.walker@fabrikam.example, ella.hughes@fabrikam.example

What we recommend next

- 1 Have each listed admin register a strong method**
 1 admin without MFA, and 1 whose registration isn't known. [See page 6](#)
- 2 Make sure each admin is included in an enabled Conditional Access policy that requires MFA for all apps, and isn't excluded from it directly or through a group**
 1 admin not covered by MFA. [See page 6](#)
- 3 Remove admin roles from guest accounts**
 1 guest with admin roles. [See page 7](#)

APPENDIX

The detail

Everything behind the summary: what changed, each finding with the accounts or settings it affects, and licences line by line. The XLSX export has every row.

What changed since 16 September

Findings

2 fixed and 17 new or returning. New ones are also marked **NEW** in the checks below.

FIXED	george.walker@fabrikam.example: No MFA method registered
FIXED	ella.hughes@fabrikam.example: No MFA method registered
NEW	rhys.hall@fabrikam.example: Mailbox forwarding to rhys.hall@homemail.example (doesn't keep a copy)
NEW	rhys.walker@fabrikam.example: Mailbox forwarding to rhys.walker@homemail.example (doesn't keep a copy)
NEW	DESK-ROBINSON51 (owen.robinson@fabrikam.example): Windows disk isn't encrypted
NEW	DESK-ROBINSON51 (owen.robinson@fabrikam.example): Not compliant
NEW	DESK-ROBINSON51 (owen.robinson@fabrikam.example): Windows 11 24H2: updates for Home and Pro ended 13 Oct 2026 (Enterprise and Education: 12 Oct 2027).
NEW	LAPTOP-SMITH50 (oscar.smith@fabrikam.example): Windows 11 24H2: updates for Home and Pro ended 13 Oct 2026 (Enterprise and Education: 12 Oct 2027).
NEW	Tenant SharePoint storage: 88% of about 1.45 TB used (1 TB + 10 GB × 46 licences)
NEW	Budget.xlsx (Finance / Documents): Can be edited by accountant@hargreaves-partners.example
NEW	aisha.brown@fabrikam.example: 47.2 GB of 49.5 GB (95%), no archive
NEW	thomas.robinson@fabrikam.example: 45.6 GB of 49.5 GB (92%), no archive
NEW	DESK-ROBINSON51 (owen.robinson@fabrikam.example): Last check-in 38 days ago
NEW	https://fabrikam.sharepoint.com/sites/finance: 117.5 GB, of which 3.0 GB in the recycle bin and 7.6 GB older versions
NEW	https://fabrikam.sharepoint.com/sites/imaging: 483.2 GB, of which 46.0 GB in the recycle bin and 33.3 GB older versions
NEW	https://fabrikam.sharepoint.com/sites/marketing: 65.3 GB, of which 1.0 GB in the recycle bin and 4.9 GB older versions

NEW <https://fabrikam.sharepoint.com/sites/patient-records>: 352.6 GB, of which 12.0 GB in the recycle bin and 25.2 GB older versions

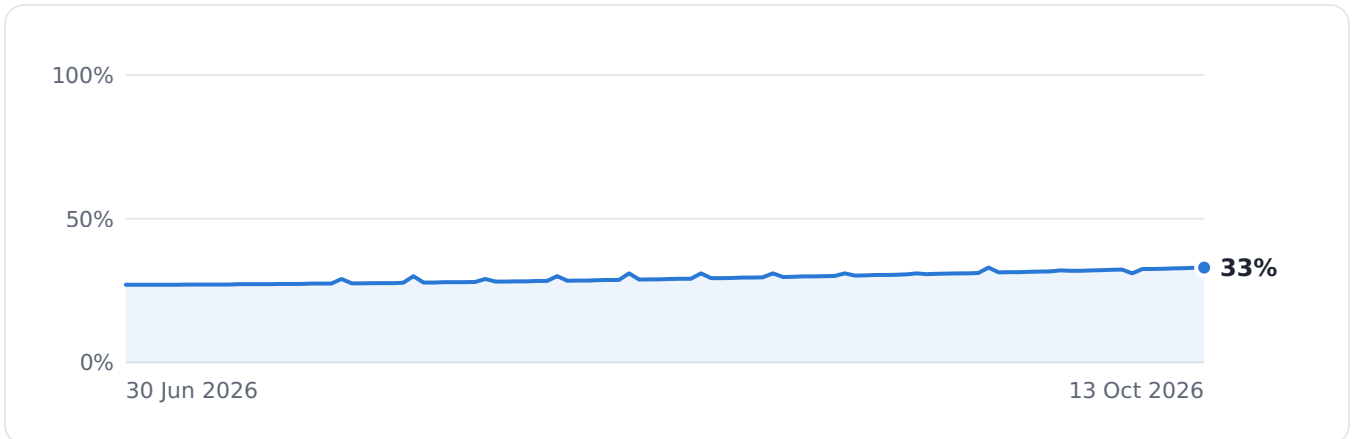
...and 2 more new

In Microsoft 365

NEW	Accounts: oscar.smith@fabrikam.example: New member account
NEW	Accounts: owen.robinson@fabrikam.example: New member account
NEW	Licences: oscar.smith@fabrikam.example: Given Microsoft 365 Business Basic
NEW	Licences: owen.robinson@fabrikam.example: Given Microsoft 365 Business Premium
NEW	Mail: rhys.walker@fabrikam.example: Now forwards to rhys.walker@homemail.example
NEW	Mail: rhys.hall@fabrikam.example: Now forwards to rhys.hall@homemail.example
NEW	Devices: LAPTOP-SMITH50 (oscar.smith@fabrikam.example): Enrolled Windows
NEW	Devices: DESK-ROBINSON51 (owen.robinson@fabrikam.example): Enrolled Windows
CHANGED	Admin activity: Payroll Sync: Update application – Certificates and secrets management by admin@fabrikam.example on 2026-10-01: Added certificate
CHANGED	Admin activity: Block risky countries: Delete conditional access policy by admin@fabrikam.example on 2026-10-06
CHANGED	Admin activity: Require MFA for all users: Update conditional access policy by admin@fabrikam.example on 2026-10-08: On → Off
CHANGED	Admin activity: anna.kowalski@fabrikam.example: Add eligible member to role in PIM completed (permanent) by admin@fabrikam.example on 2026-10-10: Exchange Administrator
CHANGED	Admin activity: fabrikam.example: Set domain authentication by mallory.quinn@fabrikam.example on 2026-10-10
CHANGED	Admin activity: ben.okafor@fabrikam.example: Add member to role by admin@fabrikam.example on 2026-10-11: Global Administrator
CHANGED	Admin activity: Payroll Sync: Update application – Certificates and secrets management by admin@fabrikam.example on 2026-10-11: Added certificate
CHANGED	Admin activity: Mail Sync Pro: Add service principal credentials by Contoso Automation on 2026-10-12: Credential added

Microsoft Secure Score

Microsoft's own measure of how many recommended security settings are turned on. Higher is better.



Fix first 15

● Critical 1 admin without MFA, and 1 whose registration isn't known

Admins

What to do: Have each listed admin register a strong method (Authenticator or a FIDO2 key), or remove the role. Break-glass accounts should use FIDO2 keys kept offline.

Account or item	Detail	Severity
breakglass@fabrikam.example	Global Administrator with no MFA method registered	● Critical
g#EXT#@fabrikam.example	Exchange Administrator: MFA registration unknown	● Low

● High 1 admin not covered by MFA

Admins

What to do: Make sure each admin is included in an enabled Conditional Access policy that requires MFA for all apps, and isn't excluded from it directly or through a group. Use a separate policy for break-glass accounts.

Account or item	Detail	Severity
breakglass@fabrikam.example	Global Administrator: 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	● High

● High 1 guest with admin roles

Admins

What to do: Remove admin roles from guest accounts. If an external partner needs access, use GDAP or a member account in this tenant protected by MFA.

Account or item	Detail	Severity
g#EXT#@fabrikam.example	Guest holding Exchange Administrator	● High

● High 1 app with access to mail, files or the directory

Apps

What to do: Review each app with the client. Remove apps nobody recognises (Enterprise applications > Delete), and for the rest confirm the vendor and that it still needs mailbox or file access.

Account or item	Detail	Severity
Mail Sync Pro	Mail.Read (application permission; unverified publisher)	● High

● High 6 of 54 computers not encrypted

Devices

What to do: 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.

Account or item	Detail	Severity
DESK-MOORE18 (ava.moore@fabrikam.example)	Windows disk isn't encrypted	● High
DESK-ROBINSON51 (owen.robinson@fabrikam.example) NEW	Windows disk isn't encrypted	● High
LAPTOP-OKAFOR (ben.okafor@fabrikam.example)	Windows disk isn't encrypted	● High
LAPTOP-ROBINSON07 (thomas.robinson@fabrikam.example)	Windows disk isn't encrypted	● High
LAPTOP-WARD29 (jack.ward@fabrikam.example)	Windows disk isn't encrypted	● High
LAPTOP-WATSON40 (lily.watson@fabrikam.example)	Windows disk isn't encrypted	● High

● High 36 of 54 Windows computers past end of support

Devices

What to do: 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.

Account or item	Detail	Severity
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.	● High
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.	● High
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.	● High
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.	● High
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.	● High
LAPTOP-WATSON40 (lily.watson@fabrikam.example)	Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.	● High
LAPTOP-WOOD22 (william.wood@fabrikam.example)	Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.	● High
DESK-ALLEN09 (thomas.allen@fabrikam.example)	Windows 11 24H2: updates for Home and Pro ended 13 Oct 2026 (Enterprise and Education: 12 Oct 2027).	● Medium
DESK-CLARK06 (ruby.clark@fabrikam.example)	Windows 11 24H2: updates for Home and Pro ended 13 Oct 2026 (Enterprise and Education: 12 Oct 2027).	● Medium
DESK-HARRISON21 (leo.harrison@fabrikam.example)	Windows 11 24H2: updates for Home and Pro ended 13 Oct 2026 (Enterprise and Education: 12 Oct 2027).	● Medium
...and 26 more in the XLSX export.		

● High 1 suspicious inbox rule

Email

What to do: Check each rule with the mailbox owner. Rules that delete or bury messages about payments or security alerts are a sign of a compromised account: reset the password, revoke sessions and review sign-ins.

Account or item	Detail	Severity
anna.kowalski@fabrikam.example	".": Moves to RSS Feeds mail mentioning invoice, payment; Rule name '.' looks deliberately blank	● High

● High 1 mail flow rule sends mail outside the organisation

Email

What to do: Check each rule that redirects mail or sends copies to an outside address with the client, and remove it unless there's a documented reason (a journaling or archiving service). Attackers with admin access add these rules to read a whole organisation's mail.

Account or item	Detail	Severity
Copy patient letters to archive	Sends mail or copies to records@dentalarchive.example	● High

● High 5 external forwards

Email

What to do: 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.

Account or item	Detail	Severity
anna.kowalski@fabrikam.example	Mailbox forwarding to anna.kowalski@homemail.example (keeps a copy)	● High
anna.kowalski@fabrikam.example	Inbox rule "Copy to home" forwards to anna.kowalski.home@homemail.example	● High
rhys.hall@fabrikam.example NEW	Mailbox forwarding to rhys.hall@homemail.example (doesn't keep a copy)	● High
rhys.walker@fabrikam.example NEW	Mailbox forwarding to rhys.walker@homemail.example (doesn't keep a copy)	● High
thomas.robinson@fabrikam.example	Inbox rule "Invoices to bookkeeper" forwards to bookkeeping@ledgerline.example	● High

● High 2 sender domains skip the spam filter

Email

What to do: Remove the allowed sender domains from the anti-spam policies: anyone can send mail claiming to be from a domain, so it skips spam and spoofing checks. Where a partner's mail is wrongly caught, report it to Microsoft or add an allow entry for their spoofed sender in the Tenant Allow/Block List instead.

Account or item	Detail	Severity
Default	Allows mail claiming to be from gmail.com, labpartners.example past the spam filter (gmail.com is free mail or the organisation's own)	● High

● High 27 users without MFA

Identity

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

Account or item	Detail	Severity
breakglass@fabrikam.example	No MFA method registered	● High
aaron.smith@fabrikam.example	No MFA method registered	● Medium
aisha.brown@fabrikam.example	No MFA method registered	● Medium
amelia.khan@fabrikam.example	No MFA method registered	● Medium
arthur.williams@fabrikam.example	No MFA method registered	● Medium
ava.jackson@fabrikam.example	No MFA method registered	● Medium
ava.moore@fabrikam.example	No MFA method registered	● Medium
ava.thomas@fabrikam.example	No MFA method registered	● Medium
carl.svensson@fabrikam.example	No MFA method registered	● Medium
chloe.jackson@fabrikam.example	No MFA method registered	● Medium
...and 17 more in the XLSX export.		

● High Legacy authentication is allowed

Identity

What to do: 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.

Account or item	Detail	Severity
Whole organisation	No enabled policy blocks legacy authentication for all users	● High

● High 1 domain had sign-in settings changed in the last 30 days

Identity

What to do: Confirm with the client that each change was planned (for example, setting up AD FS or another identity provider). If it wasn't, an attacker with admin rights may have federated the domain to their own identity provider so they can sign in as any user without a password or MFA: switch the domain back to managed sign-in, remove unknown federation settings, reset admin credentials and review the audit log.

Account or item	Detail	Severity
fabrikam.example	Set domain authentication by mallory.quinn@fabrikam.example on 10 Oct 2026	● High

● High 2 sites with no owner, 2 sites with one owner

Sharing

What to do: Give each site a second owner (in the Microsoft 365 group, in the site's owners group, or as a site administrator) so access requests and content questions have someone to go to when one person leaves. The Site access report lists each site's owners.

Account or item	Detail	Severity
Marketing	No enabled owner (Microsoft 365 group)	● High
Old Projects	No enabled owner (site administrators and owners group)	● High
Practice Management	One owner (Microsoft 365 group)	● Low
Staff Intranet	One owner (site administrators and owners group)	● Low

● High 1 guest with full control of 1 site

Sharing

What to do: Take guests out of each site's owners group and away from Full Control; give them Edit or Read through the site's members or visitors group instead. Full Control lets someone outside the organisation change who can open the site and delete anything on it. The Site permissions report lists them.

Account or item	Detail	Severity
accounts@hollis-partners.example on Finance	Full Control, given Full Control directly	● High

Also worth fixing 31

Lower-risk items. Each one lists the accounts or settings affected; the XLSX export has the full detail.

● Medium 7 accounts inactive for 90+ days or never used

Accounts

Affects aaron.smith@fabrikam.example, aisha.brown@fabrikam.example, jack.lee@fabrikam.example, noah.wood@fabrikam.example and 3 more.

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.

● Medium 2 admins without a phishing-resistant method

Admins

Affects anna.kowalski@fabrikam.example, breakglass@fabrikam.example.

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.

● Medium 1 app with privileged roles

Admins

Affects Some app.

Check each app that holds a privileged directory role still needs it. A compromised app secret with an admin role bypasses MFA entirely.

● Medium Users can consent to any app

Apps

Applies to the whole organisation.

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.

● Medium No compliance policy for iOS/iPadOS

Devices

Affects iOS/iPadOS.

In Intune (Devices > Compliance), create and assign a compliance policy for each platform with enrolled devices, requiring at least encryption, a screen lock and a minimum OS version, and set devices with no policy to show as not compliant (Compliance settings). Until then those devices count as compliant, so Conditional Access that requires a compliant device lets them through.

● **Medium** **9 of 55 managed devices not compliant**

Devices

Affects DESK-LEWIS12 (william.lewis@fabrikam.example), DESK-MOORE18 (ava.moore@fabrikam.example), DESK-ROBINSON51 (owen.robinson@fabrikam.example) **NEW**, LAPTOP-DAVIES38 (ruby.davies@fabrikam.example) and 5 more.

Open each non-compliant device in Intune (Devices > Monitor > Noncompliant devices) to see which setting fails, fix it or retire the device, and block non-compliant devices with a Conditional Access policy that requires a compliant device.

● **Medium** **8 of 55 joined Windows computers without a saved recovery key**

Devices

Affects DESK-SMITH03, DESK-WHITE42, LAPTOP-EVANS26, LAPTOP-HUGHES11 and 4 more.

Make Intune's disk encryption policy (Endpoint security > Disk encryption) require the recovery key to be saved in Entra ID before BitLocker turns on, and on computers already encrypted run BackupToAAD-BitLockerKeyProtector (or re-run the policy). Without the key, a computer that asks for it after a firmware or hardware change can't be unlocked, and its data is lost.

● **Medium** **1 mail domain without DKIM**

Email

Affects fabrikam.example.

Turn on DKIM for each domain in the Defender portal (Email authentication settings > DKIM), publishing the two selector CNAME records it shows. This applies to domains behind a mail gateway too when Microsoft 365 still sends for them (their SPF includes spf.protection.outlook.com); a gateway signs only the mail that goes out through it.

● **Medium** **2 domains without DMARC enforcement**

Email

Affects fabrikam.example, parked.example.

Publish a DMARC record with a rua= reporting address, start at p=none to see who sends as the domain, then move to p=quarantine and p=reject. Without enforcement, spoofed mail from the domain is delivered.

● **Medium** **1 anti-malware policy lets risky attachment types through**

Email

Affects Default.

Turn on the common attachments filter in the anti-malware policies (it's on by default), so program files, disk images and scripts (.exe, .iso, .js and the like) are quarantined rather than delivered.

● **Medium** **1 anti-phishing policy weakens spoof protection**

Email

Affects Office365 AntiPhish Default.

Turn spoof intelligence and "Honour DMARC policy" back on in the anti-phishing policies (both are on by default). Without them, mail pretending to be from other organisations' domains is delivered.

● **Medium** **4 teams and groups without an owner**

Groups

Affects Project Phoenix, Marketing, Marketing, Provisioned.

Make an active person, ideally two, an owner of each listed team or group (Teams admin center or Microsoft 365 admin center > Teams & groups). Owners approve members and guests and renew the group; without one, nobody looks after its files and conversations. The ownerless group policy (Microsoft 365 admin center > Settings > Org settings > Microsoft 365 Groups) asks members to take over when the last owner leaves.

● **Medium** **Enforced by CA002 — All users: Require MFA, with 1 exclusion to review**

Identity

Affects breakglass@fabrikam.example.

Create a Conditional Access policy requiring MFA for all users and all cloud apps, or turn on Security Defaults if the tenant has no Entra ID P1. Keep exclusions to break-glass accounts.

● **Medium** **1 disabled account still licensed** Licences

Affects ben.okafor@fabrikam.example.

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

● **Medium** **Anyone, including anonymous links** Sharing

Affects SharePoint and OneDrive.

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.

● **Medium** **2 files and folders shared with anyone** Sharing

Affects holiday.jpg (OneDrive of anna.kowalski@fabrikam.example), Open day flyer.pdf (Marketing / Documents).

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

● **Medium** **2 files and folders outside people can edit** Sharing

Affects Budget.xlsx (Finance / Documents) **NEW**, Lab dockets (Patient Records / Documents).

Change sharing with people outside the organisation to view-only unless they need to edit, and remove sharing that's no longer needed. The File and folder permissions report lists each person outside and what they can edit.

● **Medium** **3 mailboxes at or over 90% of quota** Storage

Affects accounts@fabrikam.example, aisha.brown@fabrikam.example **NEW**, thomas.robinson@fabrikam.example **NEW**.

Turn on the online archive for each listed mailbox (Exchange admin center > Mailboxes > Manage mailbox archive) with a retention policy that moves old mail into it, or clear large old items. A mailbox at its quota can't send, and soon after can't receive.

● **Medium** **88% of about 1.45 TB used (1 TB + 10 GB × 46 licences)** Storage

Affects Tenant SharePoint storage **NEW**, <https://fabrikam.sharepoint.com/sites/finance> **NEW**, <https://fabrikam.sharepoint.com/sites/imaging> **NEW**, <https://fabrikam.sharepoint.com/sites/marketing> **NEW** and 2 more.

Free up space before the tenant runs out, when people can no longer save files. The SharePoint storage report shows where the space goes and what to clear first; otherwise buy Office 365 Extra File Storage.

● **Low** **1 account reports to a blocked manager** Accounts

Affects anna.kowalski@fabrikam.example.

Set a current manager on each listed account (Entra admin center > Users > Properties > Manager, or in on-premises AD for synced accounts). The manager is where approvals, leaver notices and access reviews go; when they've left, those go nowhere, and their blocked account is usually waiting to be deleted too.

● **Low** **1 app registration with expiring or expired credentials** Apps

Affects Old connector.

Renew credentials before they expire to avoid an outage, and delete app registrations whose credentials have all expired if nothing uses them any more.

● Low **1 of 55 joined computers not in Intune**

Devices

Affects DESK-RECEPTION.

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.

● Low **5 devices haven't checked in for 30+ days**

Devices

Affects DESK-LEWIS12 (william.lewis@fabrikam.example), DESK-ROBINSON51 (owen.robinson@fabrikam.example) **NEW**, LAPTOP-DAVIES38 (ruby.davies@fabrikam.example), LAPTOP-LEE25 (arthur.lee@fabrikam.example) and 1 more.

Find out whether each device is lost, replaced or broken. Retire devices that are gone; for devices still in use, restart the Intune Management Extension or re-enrol.

● Low **1 of 57 device records unused for 90+ days**

Devices

Affects OLD-PC.

Disable, then after 30 days delete, device records that haven't signed in for 90 days (Entra admin center > Devices > All devices, filter by activity). Old records can still hold BitLocker keys and count toward device limits.

● Low **1 domain with SPF problems**

Email

Affects parked.example.

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".

● Low **1 of 1 mail domain doesn't fully enforce MTA-STS**

Email

Affects fabrikam.example.

Publish an MTA-STS policy so other mail servers only deliver to the domain over a verified, encrypted connection: a TXT record at _mta-sts.<domain> ("v=STSV1; id=20260101") and a policy file at https://mta-sts.<domain>/.well-known/mta-sts.txt listing the domain's MX hosts (for Microsoft 365, "mx: *.mail.protection.outlook.com"). Start with "mode: testing" and TLS-RPT reports, then switch to "mode: enforce" and change the id.

● Low **SMTP AUTH is on for the organisation**

Email

Applies to the whole organisation.

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

● Low **Anyone, including guests, can invite guests**

Guests

Applies to the whole organisation.

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

● Low **4 people can only use a text or call as a second factor**

Identity

Affects george.baker@fabrikam.example, owen.robinson@fabrikam.example **NEW**, owen.turner@fabrikam.example, thomas.allen@fabrikam.example.

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.

● Low **2 subscriptions with spare licences**

Licences

Affects Microsoft 365 Business Basic, Microsoft 365 Business Premium.
Reduce the subscription quantity at the next renewal, or assign the spare licences.

● Low **Any user can register an app**

Tenant settings

Applies to the whole organisation.
Set "Users can register applications" to No (Entra admin center > Users > User settings) and give the Application Developer role to the people who need it.

Licences

£164.40 a month

could be saved: that's £1,972.80 a year on licences that are unassigned or held by disabled or inactive accounts.

Licence	Purchased	Assigned	Unassigned	Disabled users	Inactive users	Waste / month
Microsoft 365 Business Premium	46	43	3	1	4	£144.80
Microsoft 365 Business Basic	13	11	2	0	2	£19.60
Total	59	54	5	1	6	£164.40

In good shape 15

- ✓ Between 2 and 4 Global Administrators
- ✓ Automatic forwarding to outside addresses is off
- ✓ Shared mailboxes can't be signed in to
- ✓ Mailbox auditing is on
- ✓ No mail flow rule lets mail skip spam filtering
- ✓ Guests have limited directory access
- ✓ Users have a way to get apps approved
- ✓ No old, unaccepted guest invitations
- ✓ No guest owns a team or group
- ✓ Only chosen people can create teams and groups
- ✓ Unused groups and teams expire
- ✓ Admin accounts are cloud-only
- ✓ Every licence assignment works
- ✓ No subscriptions are about to lapse
- ✓ No OneDrive is nearly full

Not checked 7

These checks need data or a Microsoft licence that isn't available, so they're neither a pass nor a fail.

Users can't create new tenants. Microsoft didn't return this setting

People can't join the tenant just by verifying an email address. Microsoft didn't return this setting

Encrypted delivery failures are reported (TLS-RPT). TLS-RPT is checked on mail domains that use MTA-STS, and none do yet

Directory sync is running. Cloud-only tenant: directory sync isn't turned on

Password hash sync is on. Cloud-only tenant: directory sync isn't turned on

No risky sign-ins succeeded. Sign-in risk needs Entra ID P2

No accounts are at risk in Entra ID Protection. Risky users need Entra ID P2

About this report

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Everything here was read from Microsoft 365 with read-only access; nothing was changed. Changes are compared with the closest data from at least 4 weeks earlier. Data collected 13 Oct 2026, 04:00 UTC.