



Harbour IT

MONTHLY SECURITY & LICENSING REVIEW

Fabrikam Dental Group

PREPARED BY

Harbour IT

REPORT DATE

9 October 2026

PERIOD COVERED

11 September to 9 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 and key figures	2
What we recommend next	2
What changed since 11 September	3
Fix first	5
Also worth fixing	9
Licences	12
In good shape	13
Not checked	13

Summary

We ran 47 security checks and 34 need attention (1 critical, 10 high, 12 medium and 11 low priority). The most urgent: 1 admin without MFA, and 1 whose registration isn't known.

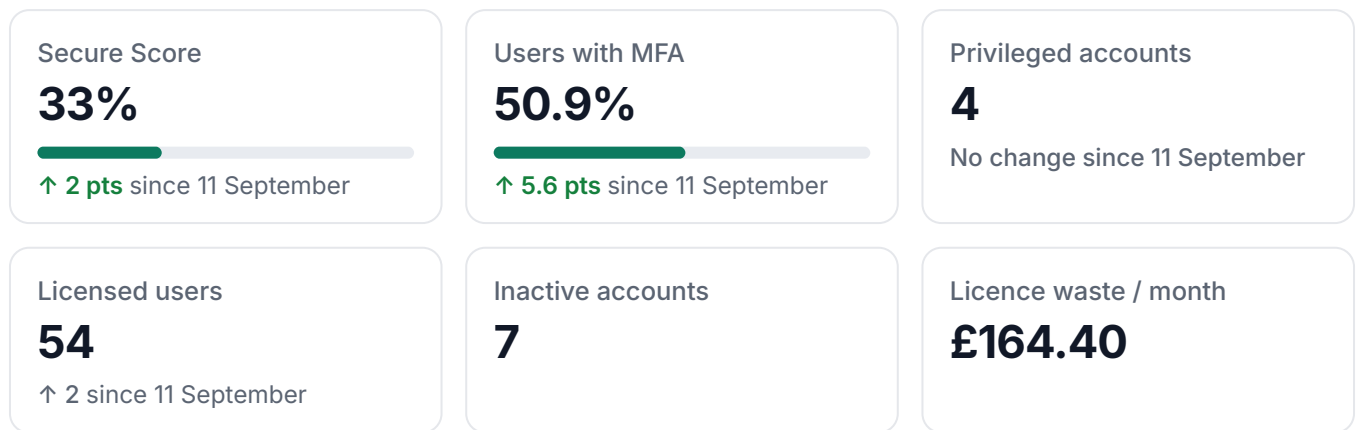
On the positive side, 13 checks passed, including "Between 2 and 4 Global Administrators", "No guests hold admin roles" and "Automatic forwarding to outside addresses is off".

Since 11 September, Microsoft Secure Score rose from 31% to 33%, users with MFA rose from 45.3% to 50.9%, 2 issues were fixed and 14 new items came up.

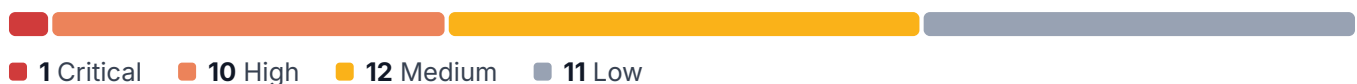
About £164.40 a month (£1,972.80 a year) goes on licences that are unused or assigned to disabled or inactive accounts.

7 checks couldn't run because the data or a licence they need is missing. They're listed at the end.

Key figures



34 of 47 checks need attention



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 5](#)
- 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 5](#)
- 3 Review each app with the client**
 1 app with access to mail, files or the directory. [See page 5](#)

What changed since 11 September

Findings

2 fixed and 14 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	Tenant SharePoint storage: 88% of about 1.45 TB used (1 TB + 10 GB × 46 licences)
NEW	DESK-ROBINSON51 (owen.robinson@fabrikam.example): Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.
NEW	LAPTOP-SMITH50 (oscar.smith@fabrikam.example): Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.
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
NEW	https://fabrikam.sharepoint.com/sites/practice: 182.8 GB, of which 6.0 GB in the recycle bin and 21.1 GB older versions
NEW	owen.robinson@fabrikam.example: Second factor is only Mobile phone (SMS or call)

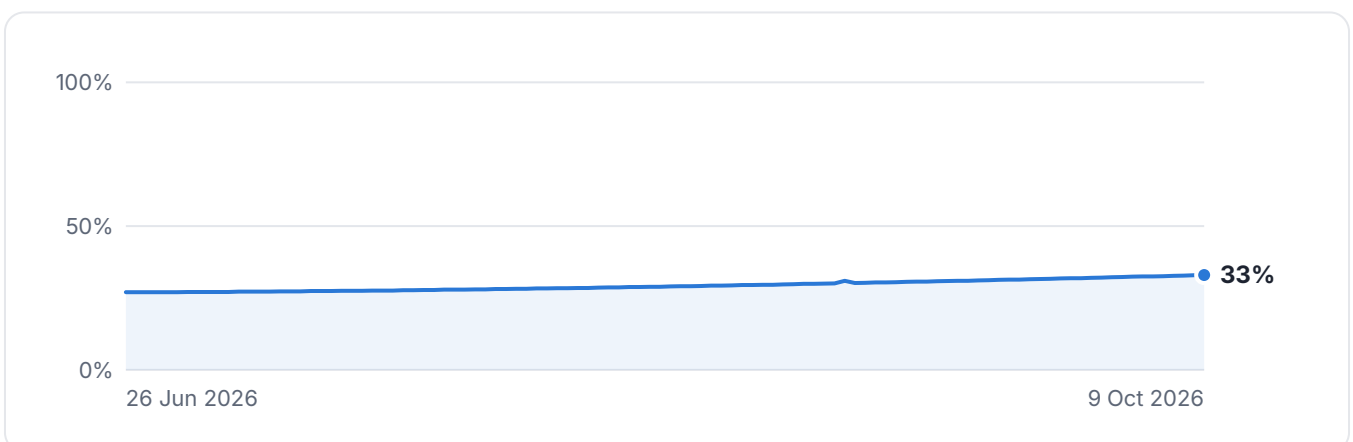
In the tenant

NEW	Accounts: oscar.smith@fabrikam.example: New member account
NEW	Accounts: owen.robinson@fabrikam.example: New member account

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 2026-09-27: Added certificate
CHANGED	Admin activity: Block risky countries: Delete conditional access policy by admin@fabrikam.example on 2026-10-03
CHANGED	Admin activity: Require MFA for all users: Update conditional access policy by admin@fabrikam.example on 2026-10-04: On → Off
CHANGED	Admin activity: anna.kowalski@fabrikam.example: Add eligible member to role in PIM completed (permanent) by admin@fabrikam.example on 2026-10-06: Exchange Administrator
CHANGED	Admin activity: fabrikam.example: Set domain authentication by mallory.quinn@fabrikam.example on 2026-10-07
CHANGED	Admin activity: ben.okafor@fabrikam.example: Add member to role by admin@fabrikam.example on 2026-10-07: Global Administrator
CHANGED	Admin activity: Payroll Sync: Update application – Certificates and secrets management by admin@fabrikam.example on 2026-10-08: Added certificate
CHANGED	Admin activity: Mail Sync Pro: Add service principal credentials by Contoso Automation on 2026-10-09: Credential added

Microsoft Secure Score

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



Fix first 11

● 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 Require MFA for all users	● 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 7 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

Account or item	Detail	Severity
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 end 13 Oct 2026.	● Low
DESK-CLARK06 (ruby.clark@fabrikam.example)	Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.	● Low
DESK-HARRISON21 (leo.harrison@fabrikam.example)	Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.	● Low
...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 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

Account or item	Detail	Severity
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 **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 7 Oct 2026	● High

● **High** 2 files and folders shared with anyone

Sharing

What to do: 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.

Account or item	Detail	Severity
Clients (Finance / Documents)	Anyone can edit, link never expires	● High
holiday.jpg (OneDrive of anna.kowalski@fabrikam.example)	Anyone can view	● Medium

Also worth fixing 23

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** **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** **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.

● **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** **3 teams and groups without an owner** Groups

Affects Project Phoenix, 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 Require MFA for all users, 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** 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 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 13

- ✓ Between 2 and 4 Global Administrators
- ✓ No guests hold admin roles
- ✓ Automatic forwarding to outside addresses is off
- ✓ Shared mailboxes can't be signed in to
- ✓ Mailbox auditing is on
- ✓ Guests have limited directory access
- ✓ Users have a way to get apps approved
- ✓ No old, unaccepted guest invitations
- ✓ 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

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 9 Oct 2026, 23:27 UTC.