



MONTHLY SECURITY & LICENSING REVIEW

Northwind Traders

PREPARED BY
Harbour IT

REPORT DATE
13 October 2026

PERIOD COVERED
15 September to 13 October 2026

MICROSOFT 365 TENANT
northwindtraders.onmicrosoft.com

● **Action needed**

Northwind Traders' 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 15 September	4
Fix first.	6
Also worth fixing	11
Licences	15
In good shape	16
Not checked	16

At a glance

We ran 61 security checks and 43 need attention (1 critical, 14 high, 16 medium and 12 low priority). The most urgent: 1 admin without MFA, and 1 whose registration isn't known.

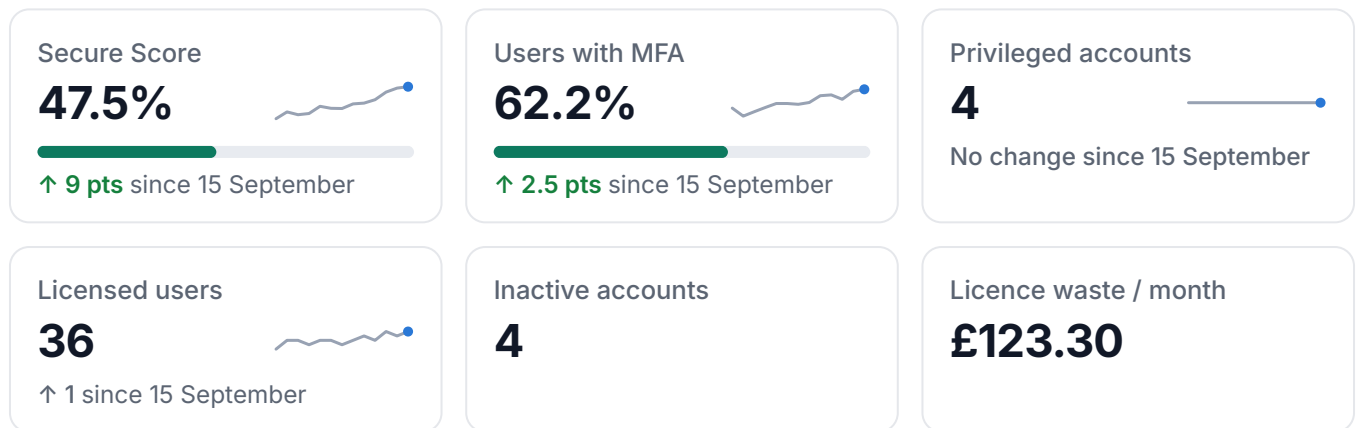
On the positive side, 18 checks passed, including "Between 2 and 4 Global Administrators", "Automatic forwarding to outside addresses is off" and "Shared mailboxes can't be signed in to".

Since 15 September, Microsoft Secure Score rose from 38.5% to 47.5%, users with MFA rose from 59.7% to 62.2%, 1 issue was fixed and 7 new items came up.

About £123.30 a month (£1,479.60 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



43 of 61 checks need attention



This month



What we did

FIXED Every active user has MFA registered · 1 item: megan.lee@northwindtraders.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 6](#)

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 15 September

Findings

1 fixed and 7 new or returning. New ones are also marked **NEW** in the checks below.

FIXED	megan.lee@northwindtraders.example: No MFA method registered
NEW	grace.taylor@northwindtraders.example: Mailbox forwarding to grace.taylor@homemail.example (doesn't keep a copy)
NEW	Campaign video.mp4 (Marketing / Documents): Anyone can edit
NEW	Year end/Draft accounts FY26.xlsx (Clients / Documents): Can be edited by partner@mason-legal.example
NEW	hannah.robinson@northwindtraders.example: 47.2 GB of 49.5 GB (95%), no archive
NEW	olivia.smith@northwindtraders.example: 45.6 GB of 49.5 GB (92%), no archive
NEW	DESK-EDWARDS33 (imogen.edwards@northwindtraders.example): Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.
NEW	LAPTOP-WATSON32 (aaron.watson@northwindtraders.example): Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.

In Microsoft 365

NEW	Accounts: aaron.watson@northwindtraders.example: New member account
NEW	Accounts: imogen.edwards@northwindtraders.example: New member account
NEW	Licences: aaron.watson@northwindtraders.example: Given Microsoft 365 Business Premium
NEW	Licences: imogen.edwards@northwindtraders.example: Given Microsoft 365 Business Premium
NEW	Mail: grace.taylor@northwindtraders.example: Now forwards to grace.taylor@homemail.example
NEW	Devices: LAPTOP-WATSON32 (aaron.watson@northwindtraders.example): Enrolled Windows
NEW	Devices: DESK-EDWARDS33 (imogen.edwards@northwindtraders.example): Enrolled Windows
CHANGED	Admin activity: Payroll Sync: Update application – Certificates and secrets management by admin@northwindtraders.example on 2026-10-01: Added certificate

CHANGED **Admin activity:** Block risky countries: Delete conditional access policy by admin@northwindtraders.example on 2026-10-06

CHANGED **Admin activity:** Require MFA for all users: Update conditional access policy by admin@northwindtraders.example on 2026-10-08: On → Off

CHANGED **Admin activity:** ann.patel@northwindtraders.example: Add eligible member to role in PIM completed (permanent) by admin@northwindtraders.example on 2026-10-10: Exchange Administrator

CHANGED **Admin activity:** northwindtraders.example: Set domain authentication by mallory.price@northwindtraders.example on 2026-10-10

CHANGED **Admin activity:** robert.hughes@northwindtraders.example: Add member to role by admin@northwindtraders.example on 2026-10-11: Global Administrator

CHANGED **Admin activity:** Payroll Sync: Update application – Certificates and secrets management by admin@northwindtraders.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@northwindtraders.example	Global Administrator with no MFA method registered	● Critical
g#EXT#@northwindtraders.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@northwindtraders.example	Global Administrator: excluded from Require MFA for all users	● 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#@northwindtraders.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 4 of 36 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-WRIGHT18 (leo.wright@northwindtraders.example)	Windows disk isn't encrypted	● High
LAPTOP-HUGHES (robert.hughes@northwindtraders.example)	Windows disk isn't encrypted	● High
LAPTOP-SCOTT29 (olivia.scott@northwindtraders.example)	Windows disk isn't encrypted	● High
LAPTOP-SMITH07 (olivia.smith@northwindtraders.example)	Windows disk isn't encrypted	● High

● High 5 of 36 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-HUGHES (robert.hughes@northwindtraders.example)	Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.	● High
LAPTOP-MARTIN22 (maya.martin@northwindtraders.example)	Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.	● High
LAPTOP-PATEL13 (hannah.patel@northwindtraders.example)	Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.	● High
LAPTOP-ROBERTS31 (george.roberts@northwindtraders.example)	Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.	● High
LAPTOP-TAYLOR04 (grace.taylor@northwindtraders.example)	Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.	● High
DESK-BAKER27 (ella.baker@northwindtraders.example)	Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.	● Low

Account or item	Detail	Severity
DESK-CLARKE00 (thomas.clarke@northwindtraders.example)	Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.	● Low
DESK-EDWARDS33 (imogen.edwards@northwindtraders.example) NEW	Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.	● Low
DESK-HILL15 (ruby.hill@northwindtraders.example)	Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.	● Low
DESK-LEE03 (megan.lee@northwindtraders.example)	Windows 11 24H2: updates for Home and Pro end 13 Oct 2026.	● Low
...and 15 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
ann.patel@northwindtraders.example	".": Moves to RSS Feeds mail mentioning invoice, payment; Rule name '.' looks deliberately blank	● High

● High **1 mail flow rule skips spam filtering**

Email

What to do: Remove mail flow rules that skip spam filtering (set the spam confidence level to -1) for senders picked by their address, domain or a header, which anyone can fake. For mail arriving through another filtering service use enhanced filtering on its inbound connector instead, and for a partner limit the rule to the addresses of their sending servers.

Account or item	Detail	Severity
Supplier invoices never junk	Skips spam filtering for mail picked out by: From domains supplierhub.example	● High

● High 4 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
ann.patel@northwindtraders.example	Mailbox forwarding to ann.patel@homemail.example (keeps a copy)	● High
ann.patel@northwindtraders.example	Inbox rule "Copy to home" forwards to ann.patel.home@homemail.example	● High
grace.taylor@northwindtraders.example NEW	Mailbox forwarding to grace.taylor@homemail.example (doesn't keep a copy)	● High
olivia.smith@northwindtraders.example	Inbox rule "Invoices to bookkeeper" forwards to bookkeeping@ledgerline.example	● High

● High 14 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@northwindtraders.example	No MFA method registered	● High
alfie.roberts@northwindtraders.example	No MFA method registered	● Medium
alfie.scott@northwindtraders.example	No MFA method registered	● Medium
carl.jensen@northwindtraders.example	No MFA method registered	● Medium
grace.wilson@northwindtraders.example	No MFA method registered	● Medium
hannah.robinson@northwindtraders.example	No MFA method registered	● Medium
leo.morris@northwindtraders.example	No MFA method registered	● Medium
leo.wright@northwindtraders.example	No MFA method registered	● Medium

Account or item	Detail	Severity
maya.martin@northwindtraders.example	No MFA method registered	● Medium
olivia.scott@northwindtraders.example	No MFA method registered	● Medium
...and 4 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
northwindtraders.example	Set domain authentication by mallory.price@northwindtraders.example on 10 Oct 2026	● High

● High 1 site 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
Operations	One owner (Microsoft 365 group)	● Low

Account or item	Detail	Severity
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

● High 3 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
Campaign video.mp4 (Marketing / Documents) NEW	Anyone can edit	● High
Brand assets (Marketing / Documents)	Anyone can view, link never expires	● Medium
holiday.jpg (OneDrive of ann.patel@northwindtraders.example)	Anyone can view	● Medium

Also worth fixing 28

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

● Medium 4 accounts inactive for 90+ days or never used

Accounts

Affects hannah.robinson@northwindtraders.example, sophie.smith@northwindtraders.example, thomas.clarke@northwindtraders.example, g#EXT#@northwindtraders.example.

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 ann.patel@northwindtraders.example, breakglass@northwindtraders.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** **6 of 37 managed devices not compliant** Devices

Affects DESK-ROBINSON12 (george.robinson@northwindtraders.example), DESK-WRIGHT18 (leo.wright@northwindtraders.example), LAPTOP-HUGHES (robert.hughes@northwindtraders.example), LAPTOP-SCOTT25 (alfie.scott@northwindtraders.example) and 2 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** **5 of 37 joined Windows computers without a saved recovery key** Devices

Affects DESK-LEE03, LAPTOP-CLARK26, LAPTOP-MORRIS19, LAPTOP-WATSON11 and 1 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 northwindtraders.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 northwindtraders.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 sender domain skips the spam filter

Email

Affects Default.

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.

● **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 Require MFA for all users, with 1 exclusion to review

Identity

Affects breakglass@northwindtraders.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 robert.hughes@northwindtraders.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** 1 file or folder outside people can edit

Sharing

Affects Year end/Draft accounts FY26.xlsx (Clients / Documents) **NEW**.

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@northwindtraders.example, hannah.robinson@northwindtraders.example **NEW**, olivia.smith@northwindtraders.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.

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

Accounts

Affects ann.patel@northwindtraders.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 37 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 3 devices haven't checked in for 30+ days

Devices

Affects DESK-ROBINSON12 (george.robinson@northwindtraders.example), LAPTOP-HUGHES (robert.hughes@northwindtraders.example), LAPTOP-SCOTT25 (alfie.scott@northwindtraders.example).

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 39 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 northwindtraders.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 **3 people can only use a text or call as a second factor** Identity

Affects arthur.evans@northwindtraders.example, mia.hughes@northwindtraders.example, zara.jackson@northwindtraders.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

£123.30 a month

could be saved: that's £1,479.60 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	32	29	3	1	2	£108.60
Microsoft 365 Business Basic	9	7	2	0	1	£14.70
Total	41	36	5	1	3	£123.30

In good shape 18

- ✓ 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 sends mail outside the organisation
- ✓ Spoof protection is on
- ✓ Risky attachment types are blocked
- ✓ 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
- ✓ SharePoint storage isn't nearly full
- ✓ 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.