VITALS
A product by Innova Group

VITALS ASSESSMENT

Microsoft 365 Assessment

A read-only review of your Microsoft 365 tenant — how content is shared and protected, how sign-in and devices are governed, what you are paying for and using, and whether you are ready for Copilot. Scored, with every finding in priority order and the reasoning behind it.

PREPARED FOR
Kirkwell Industries Ltd

DATE
28 July 2026

PREPARED BY
Innova Group

389 files **8** sites **200** user accounts **27** checks

Read-only assessment · nothing in the tenant was changed

hello@innovagroup.tech · innovagroup.tech

THE HEADLINE

Overall health

EMERGING

Significant gaps. Content is reachable by people who should not reach it, and the environment needs work before more is built on it.

OPTIMISED	HEALTHY	DEVELOPING	EMERGING	AT RISK
90+	75–89	60–74	40–59	UNDER 40

By area

WEAKEST FIRST WITHIN EACH

12%
Email & Domain
Whether your domains can be impersonated, and what mailbox rules are doing
2 CHECKS

25%
Identity & Access
Sign-in protection, administrative control and third-party access
8 CHECKS

29%
Copilot Readiness
Whether Copilot can safely be switched on
1 CHECK

46%
Licensing & Devices
What you pay for, what is used, and what is managed
2 CHECKS

69%
Content & Protection
How content is shared, labelled, owned and maintained
10 CHECKS

76%
Workplace Experience
Whether the intranet is current and worth visiting
4 CHECKS

THE SHORT VERSION

Executive summary

Kirkwell Industries Ltd scored **47.5 / 100** — **Emerging**. On the evidence below the environment needs **substantial work**. Access is wider than intended in several places and there is little to distinguish sensitive content from ordinary content.

The assessment reviewed 389 files across 8 sites and 200 users.

10	20	47
Critical	**High**	**Everything else**
ADDRESS THIS WEEK	ADDRESS THIS MONTH	ADDRESS THIS QUARTER

Resolve these first

HIGHEST SEVERITY, MOST AFFECTED

1. Nothing is protecting sign-in
2. 37 likely-sensitive files with no sensitivity label
3. 20 files shared via anonymous "anyone with the link" links

HOW TO READ THIS REPORT

The sections that follow say what to do first: the priorities above, then the scores, then the evidence behind them. The findings section near the back is the reference — grouped by area and ordered by severity within each, so it can be worked through an area at a time or handed to whoever owns that area.

ALL 27 DIMENSIONS

Scores in detail

Ordered weakest area first. The count beside each dimension is how many items were flagged out of how many were examined.

Email & Domain

12%

Email Domain Protection

2 of 2 flagged

0%

Each domain the tenant sends mail from; a domain counts as flagged when its published SPF, DKIM or DMARC records leave it open to impersonation.

Mailbox Rules

Weighted by severity: one rule forwarding mail outside the organisation caps the score, however few there are.

25%

Inbox rules across sampled mailboxes; a rule counts as flagged when it forwards mail outside the organisation or deletes it on arrival. Rule names and conditions only — never message content.

Identity & Access

25%

Identity & Administration

5 of 5 flagged

0%

A fixed set of tenant identity settings — administrator counts, legacy authentication, self-service consent and similar; each one either passes or is flagged.

Third-Party Applications

3 of 3 flagged

0%

Third-party applications holding standing consent in the tenant, and the permissions each one was granted.

Collaboration Exposure

Scored on the combination of external exposure and the controls behind it, not on any single setting. External collaboration alone is not a fault.

14%

External collaboration, sign-in conditions, device compliance and detection coverage, scored as one path rather than four settings.

Credential Registration

Weighed from the controls on registering a method and from what the audit log shows was registered in the last 30 days — not a flagged ratio. The absence of a policy protecting registration costs the most.

20%

The rules that decide who may add or recover a sign-in method and under what conditions, and every method added or removed across the tenant in the last 30 days.

Sign-in Protection

2 of 3 flagged

20%

Every Conditional Access policy in the tenant; a policy counts as flagged when it is not actually enforcing — report-only, disabled, or scoped to nobody.

Authentication Maturity

Maturity level 2 of 5 — Multi-factor present. Most people can complete a second-factor prompt, but the methods are phishable and unevenly governed.

40%

Every account with a registration record; scored as a maturity level from the strength of the methods registered and whether account recovery would still work.

Microsoft Security Baseline

Scored on Microsoft's own Secure Score for this tenant, not on the count beside it.

42%

The Microsoft Secure Score controls that apply to this tenant; a control counts as flagged when it is not implemented.

Multi-Factor Coverage

Weighted: an administrator who cannot complete a prompt counts for more than a standard account.

59%

Every licensed account; an account counts as flagged when it cannot complete a multi-factor prompt.

Copilot Readiness

29%

Licensing & Devices

46%

Device Management

20%

55 of 69 flagged

Staff entitled to a managed device; a person counts as flagged when they have no compliant Intune-managed device enrolled.

Licence Utilisation

83%

15 of 86 flagged

Paid licences bought against licences actually assigned; a licence counts as flagged when it is paid for and sitting unassigned.

Content & Protection

69%

Sharing Defaults

0%

3 of 3 flagged

Tenant-wide sharing settings — default link type, anonymous link expiry, external sharing scope; each one either passes or is flagged.

Labelling & Protection

37%

Weighted: an unlabelled file that looks sensitive counts twice.

Every sampled file; a file counts as flagged when it carries no sensitivity label, so no protection travels with it.

Site Ownership

57%

Scored across every workspace, not only the sites counted beside it.

Every sampled site; a site counts as flagged when it has no active owner to approve access or answer for its content.

Bulk Access Exposure

75%

Each person who stands far outside the organisation's own range costs points; the count beside the bar is how many did. The usage report is a month in one number, not a timeline.

Every person's SharePoint and OneDrive volume over the last 30 days — files synced to a device and files shared outside — against what is typical for this organisation.

Workspace Hygiene

79%

3 of 14 flagged

Every Team, group and site; a workspace counts as flagged when it is empty, abandoned or duplicated.

Content Freshness

80%

79 of 389 flagged

Every sampled file; a file counts as flagged when it has not been modified in more than two years.

Access & Oversharing

86%

56 of 389 flagged

Every sampled file; a file counts as flagged when it is shared more widely than it needs to be — anonymous links, organisation-wide sharing, or external guests.

Duplication

86%

53 of 389 flagged

Files with a content hash, compared to each other; a file counts as flagged when it is a byte-for-byte copy of another one already counted.

Findability

87%

49 of 389 flagged

Every sampled file name; a file counts as flagged when its name cannot identify it — "final v3", "doc1", "scan0001" and the like.

Guest Access

93%

Scored on dormant guests as a share of all accounts, not on the guest count beside it.

External guest accounts with access to tenant content, and how long each has been dormant.

Workplace Experience

76%

Legacy SharePoint

62%

Weighted by disposal: 1 to rebuild, 1 to modernise, 1 to retire, 5 to keep.

Every scanned site; a site counts as flagged when it carries classic publishing, form libraries or classic pages that Microsoft's retirement dates will affect.

Page Freshness

67%

10 of 30 flagged

Published site pages; a page counts as flagged when it has not been edited in more than two years.

Landing Pages

88%

1 of 8 flagged

The landing page of each sampled site, and whether it has been set up rather than left as the default.

Publishing Hygiene

94%

2 of 32 flagged

Site pages; a page counts as flagged when it is still an unpublished draft that readers cannot see.

WHAT WAS FOUND

Evidence

Email protection by domain

PUBLIC DNS

Three public records decide whether somebody can send email in your name. SPF lists who may send, DKIM signs what they send, and DMARC is the only one that tells a receiving server to act on a forgery. A domain with the first two and not the third looks protected and is not.

DOMAIN	SPF	DKIM	DMARC	POLICY IN FORCE
kirkwell-joinery.co.uk	✓	✗	✗	Anyone can send as this domain
kirkwell.co.uk	✓	✓	•	Reported only — nothing is blocked

Applications with access to your data

THIRD PARTY ONLY

Consent does not expire and is not tied to anybody's session, so none of this is affected by a password reset. Microsoft's own services are excluded. The question for each row is whether somebody can name it and say why it is still here.

APPLICATION	SUPPLIER	MAIL	FILES	CAN CHANGE	SINCE
Invoice Sync Helper	not recorded	✓	✓	—	Feb 2026
Mail Signature Manager	Exclaimer Ltd VERIFIED	✓	—	✓	Sept 2023
DocuSign	DocuSign Inc. VERIFIED	—	✓	—	May 2024

A tick under Mail or Files means organisation-wide access, not access to one person's account.

Who can complete a multi-factor prompt

46 OF 69

41 app or security key **5** text message or call only **23** nothing registered

Of 5 administrators, **2 cannot**. Those accounts can change anything in the tenant and are protected by a password alone. Registration is what a sign-in policy depends on: a requirement applied to people who cannot meet it produces exclusions, not protection.

THE QUESTION EVERYONE ASKS

Microsoft 365 Copilot

Not yet

Copilot answers using whatever the person asking is already allowed to see. It does not widen access — it makes existing access easy to find by asking. So what decides readiness is not the technology, it is whether anything is sitting somewhere it should not be.

Resolve before rollout

IN ORDER

1. **9 likely-sensitive files are readable across the organisation before Copilot is switched on**
   Resolve the sharing on these before any Copilot rollout. This is the single most common reason an AI pilot has to be paused after launch rather than before.
2. **2 third-party applications can already read the content Copilot would draw on**
   Review each one against a named business owner and a reason. Remove consent where neither exists — an application nobody can account for is not one to leave reading everything. This review belongs in the same conversation as the Copilot rollout, not a separate one.
3. **Sign-in protection is not enforced, and Copilot raises what an account is worth**
   Enforce multi-factor authentication before rollout rather than after.

ALREADY PAID FOR

What you already own

Every subscription in this tenant, and how many are assigned to somebody. Capability that is already paid for is the cheapest improvement available — it needs switching on rather than buying.

SUBSCRIPTION	ASSIGNED	BOUGHT	SPARE
Microsoft 365 Business Premium	61	68	7
Microsoft 365 E3	8	12	4
Visio Plan 2	2	6	4

Included with Microsoft 365 Business Premium, whether or not it is switched on:

- Device management (Intune)
- Conditional Access and multi-factor authentication
- Information protection and sensitivity labels
- Defender for Business
- Multi-factor authentication
- Exchange Online

What was scanned

COVERAGE

3 personal or app sites excluded by design. OneDrive, Designer, Loop and similar are not part of a SharePoint readiness assessment.

My workspace, Designer, Loop

1 SITE COULD NOT BE READ

Real business sites blocked by an access policy. Worth an administrator confirming the restriction is intended: Board Confidential.

IN PRIORITY ORDER

Action plan

The same findings as the reference section, arranged as work rather than as evidence. Nothing here is new — it is the order to do it in.

This week

10 CRITICAL FINDINGS

- Nothing is protecting sign-in
- 37 likely-sensitive files with no sensitivity label
- 20 files shared via anonymous "anyone with the link" links
- External contact is possible and no policy requires a managed device
- 9 likely-sensitive files over-shared
- 9 likely-sensitive files are readable across the organisation before Copilot is switched on
- 2 mailbox rules send company mail to an outside address

and 3 more — all listed in full in the findings section.

This month

20 HIGH-SEVERITY FINDINGS

- 69 people are licensed for device management, and 14 devices are enrolled
- 36 files shared org-wide ("Everyone")
- The tenant permits anonymous "anyone with the link" sharing
- 18 accounts have contact details that no longer allow a password reset
- 15 licences paid for and assigned to nobody
- 14 guest accounts over a year old
- 10 intranet pages not updated in over 2 years

and 13 more — all listed in full in the findings section.

This quarter

47 REMAINING FINDINGS

- Microsoft rates this tenant at 41.8% of its own security baseline
- 173 further files with no label
- Registering a new sign-in method is protected only by a prompt the caller can talk someone through
- 79 files not modified in over 2 years
- 53 duplicate copies across 21 sets of identical files
- 49 poorly named files
- 21 accounts have no multi-factor method registered

and 40 more — all listed in full in the findings section.

THE REFERENCE

Every finding, in full

The evidence behind the score, grouped by area and ordered by severity within each — what was found, why it matters, and the standard remedy. Meant to be worked through an area at a time.

Identity & Access

35 FINDINGS · 10 NEEDING ATTENTION

CRITICAL Nothing is protecting sign-in

Security defaults are switched off and no Conditional Access policy is enforced. Microsoft offers two ways to require multi-factor authentication and neither is in use, so a password on its own is currently enough to sign in as anybody here, from anywhere.

Security defaults	**Off** Graph /policies/identitySecurityDefaultsEnforcementPolicy
Enforced Conditional Access policies covering sign-in	**0** Graph /identity/conditionalAccess/policies
Accounts affected	**200**

Recommended fix: If Conditional Access is licensed, use it — it is the more flexible of the two. If not, switch security defaults on. It is free, takes a minute, and is far better than nothing.

CRITICAL External contact is possible and no policy requires a managed device

Any external organisation can start a Teams conversation with an employee here, and no enforced Conditional Access policy requires a managed device — 86% of devices report compliant. Microsoft has documented attackers using exactly this opening: a message that appears to come from IT support, a remote-support session the employee agrees to, and tooling run on the machine from there. Each part of that is legitimate behaviour, which is why no single setting in this report flags it. Nothing enforces multi-factor either, so the same conversation also yields credentials that work from anywhere.

Inbound collaboration	**Open to any organisation** Graph /policies/crossTenantAccessPolicy
Guest accounts	**18**
Enforced policies requiring a compliant device	**0** Graph /identity/conditionalAccess/policies
Multi-factor enforced	**No**

Recommended fix: Require a compliant or hybrid-joined device for access to Microsoft 365 through Conditional Access. That single control is what makes the difference between a persuaded employee and a compromised organisation, because it constrains where a working session can be used rather than trying to prevent the conversation. Restricting who may start an external Teams chat to named partner organisations is worth doing as well, but on its own it only narrows the opening.

CRITICAL 2 third-party applications can read mail across this organisation

These applications hold access to mailboxes for the whole organisation, granted once and not tied to anybody's session. A password reset does not affect them, revoking sign-ins does not affect them, and multi-factor authentication was never involved. Some will be tools somebody chose deliberately — a signature manager, a CRM, a backup product. The rest are how a consent-phishing attack keeps reading mail months afterwards.

Third-party applications with consent	3	Graph /servicePrincipals appRoleAssignments
Tenant-wide read of all mailboxes	2	Mail.Read / Mail.ReadWrite application permission

> **Recommended fix:** Review each one in Entra under Enterprise applications. Anything nobody can name and account for should have its permissions revoked today; the access does not lapse on its own.

CRITICAL 2 administrators have no multi-factor method registered

These accounts can change anything in the tenant and are protected by a password alone. An administrator without multi-factor is the single most valuable target in the organisation and the least defended, and the credentials for it are worth buying rather than guessing.

Administrator accounts in the registration report	5	Graph /reports/authenticationMethods/userRegistrationDetails
Of which not MFA-capable	2	isMfaCapable = false

> **Recommended fix:** Register a method on these accounts today. Where one is a break-glass account kept deliberately outside the policy, it still needs a method registered, a long stored password and somebody watching it for use.

HIGH INFERRED 18 accounts have contact details that no longer allow a password reset

A mobile number or alternate address is recorded against these accounts, but was never registered as an authentication method. Since 7 September 2026 Microsoft no longer accepts directory contact details for self-service password reset. The people affected cannot tell: they can see their own number on their profile, and it will do nothing when they are locked out — which is exactly when they will find out, and when it becomes a call to somebody rather than a self-service reset.

Accounts in the registration report	69
Recovery relies on contact details that cannot reset a password	18

> **Recommended fix:** Run a registration campaign before these accounts need recovery rather than after. Microsoft can prompt people to register at next sign-in. Where the number really is the recovery route, it has to be registered as a method, not left as a profile field.

HIGH 5 accounts rely on text message or phone call alone

Codes by text and voice call are better than a password on its own and are the weakest thing Microsoft still counts as multi-factor. A mobile number can be moved to an attacker's SIM by persuading the network to do it, which is a routine attack against anybody worth the effort, and it defeats both. At least one of these is an administrator.

Accounts whose only methods are SMS or voice	5	methodsRegistered on the registration report
Of which administrators	2	

> **Recommended fix:** Move these to the Microsoft Authenticator app, which is free and works on any phone. Administrators should move first.

HIGH No enforced policy requires multi-factor authentication

Conditional Access is in use, but nothing currently in force requires a second factor. A password on its own remains enough to sign in, which is the single most common way an account is taken over.

Enforced policies	1	
Of which require multi-factor	0	grantControls.builtInControls contains mfa

Recommended fix: Add a policy requiring multi-factor authentication, starting with administrators and then all users.

HIGH INFERRED Legacy authentication does not appear to be blocked

Older sign-in protocols cannot present a second factor, so they are the route around multi-factor authentication rather than through it. Where they remain available, an attacker will use them in preference to anything else.

Enforced policies	1	
Of which block legacy client apps	0	conditions.clientAppTypes with a block grant

Recommended fix: Add a policy blocking legacy authentication. Check for older devices or line-of-business applications that still rely on it before enforcing.

HIGH 1 disabled account still holds administrative rights

A disabled account that retains Global Administrator is a re-enabled account away from full control of the tenant. Disabling is what happens when somebody leaves; removing the role is what should happen with it.

Global Administrators	6	
Of which sign-in disabled	1	user.accountEnabled on role members

Recommended fix: Remove the administrative role from these accounts, then decide separately whether the account itself should still exist.

HIGH 1 administrator account acquired a new sign-in method in the last 30 days

Registered since 25 July: 1 passkey. Each of these should be something the administrator remembers doing. A method registered against a privileged account by anybody else, at any hour, from anywhere, is the whole intrusion in one line of a log — and the log is where it stays unless somebody looks.

Security-info changes in the audit log, last 30 days	9	Graph /auditLogs/directoryAudits
On administrator accounts	1	
Administrators affected	1	

Recommended fix: Confirm each with the administrator concerned. Anything they cannot account for: remove the method, revoke the account's sessions, reset the password, and treat everything that account touched since the registration as suspect.

Hand-over document: The first hour: a sign-in method nobody can account for →

MEDIUM CALCULATED **Microsoft rates this tenant at 41.8% of its own security baseline**

Secure Score is Microsoft's assessment of the tenant against its own recommendations — currently 214 points of 512 available. It is a useful independent measure precisely because it is not ours, and it is the number a customer can check for themselves at any time.

Secure Score	**214 of 512 (41.8%)**	Graph /security/secureScores
As of	**13 Sept 2026**	

> **Recommended fix:** Work through the highest-value controls first. The Microsoft 365 admin centre orders them by the points they carry, which broadly follows the risk they address.

MEDIUM **Registering a new sign-in method is protected only by a prompt the caller can talk someone through**

"Require MFA to register security info" applies to registering security information, which is the right place for a policy, and it is enforced. What it asks for is the "Multifactor authentication" authentication strength, which the employee satisfies with the same Authenticator prompt they approve for everything else — and the attack this guards against begins with the employee approving prompts because a caller asked them to. It stops a stolen password from registering a method. It does not stop a persuaded person from doing so.

Enforced policies protecting registration	**1**	userActions: registersecurityinfo
Requiring a compliant device or phishing-resistant method	**0**	

> **Recommended fix:** Change the grant to require a phishing-resistant authentication strength, or a compliant device, or a trusted location. Any of those constrains where and with what a method can be added, which is the constraint a phone call cannot talk its way past. Keep a temporary access pass as the deliberate exception for people registering their first method.

Hand-over document: The first hour: a sign-in method nobody can account for →

MEDIUM **21 accounts have no multi-factor method registered**

Nothing is enforcing multi-factor on this tenant, and these accounts could not satisfy a requirement if one were introduced. That ordering matters: getting people registered first is what makes enforcement a switch rather than an incident.

Accounts in the registration report	**69**	Graph /reports/authenticationMethods/userRegistrationDetails
Not MFA-capable	**23 (33%)**	isMfaCapable = false
Multi-factor enforced by Conditional Access	**No**	

> **Recommended fix:** Run a registration campaign before enforcing anything. Microsoft can prompt people to register at next sign-in, which does the work for you.

MEDIUM **11 accounts have no registered recovery method**

Every one of these is a future call to whoever resets passwords, at a moment when the person cannot work. Self-service reset only removes that call for people who registered a method before they needed it.

Accounts in the registration report	**69**	
With no self-service reset method	**11**	isSsprRegistered = false

> **Recommended fix:** Enable registration prompting at sign-in and let the population close the gap on its own over a fortnight.

MEDIUM 8 recommended controls are not in place

These are Microsoft's own recommendations for this tenant, and nothing has been recorded against them — neither implemented nor deliberately set aside. Many are settings rather than purchases, and a good number are covered by licences this organisation already holds.

Recommended controls	11	Graph /security/secureScoreControlProfiles
Not implemented	8	

Recommended fix: Review them by area. The identity ones usually give the largest improvement for the least work.

MEDIUM CALCULATED 6 accounts hold full administrative control

A Global Administrator can do anything in the tenant, including granting themselves access to anybody's mailbox or files and removing the record that they did. Every one of these accounts is worth more to an attacker than any ordinary account, and the number tends to grow because adding one solves an immediate problem and removing one never does.

Accounts holding Global Administrator	6	Graph /directoryRoles members
Microsoft's guidance	fewer than 5, more than one	

Recommended fix: Reduce to two or three named people. Where somebody needs to do one specific job, a narrower role usually exists for it — user administration, or helpdesk, rather than everything.

MEDIUM 5 endpoint protection controls are not implemented

Microsoft's own assessment of this tenant reports these as unimplemented. They matter to this path specifically: once a remote-support session has been used to run something on a machine, endpoint detection is what turns an incident into an alert rather than into a discovery weeks later.

Endpoint and app protection controls not implemented	5	Graph /security/secureScoreControlProfiles, Device and Apps categories

Recommended fix: Work through these in Microsoft's own order — they are ranked by effect, and the assessment behind them has already been done.

MEDIUM 4 administrators hold no phishing-resistant method

These accounts can change anything in the tenant, and every method registered against them can be handed to an attacker by the person who holds it. A convincing sign-in page relays the code as it is typed; a stream of prompts gets one approved. Neither works against a security key, Windows Hello or a passkey, because those are bound to the site that issued them and produce nothing on a page that only looks like it.

Administrator accounts	5	Graph /reports/authenticationMethods/userRegistrationDetails
Without a phishing-resistant method	4	no FIDO2, passkey or Windows Hello registered

Recommended fix: Issue a security key or enable Windows Hello for these accounts, then require phishing-resistant authentication for administrative roles through a Conditional Access authentication strength. Administrators are few enough that this is an afternoon, not a project.

MEDIUM Guests can invite further guests

An external person who has been given access can invite other external people, who can invite more. Nobody inside the organisation approves any of it, and the resulting list is not one anybody is reviewing.

Guests can invite	**Allowed**	Graph /policies/authorizationPolicy allowInvitesFrom

> **Recommended fix:** Restrict invitations to administrators, or to a named group of people who understand what they are granting.

MEDIUM Any user can register an application

Ordinary accounts can create applications that request access to company data. This is how consent-phishing works: the victim is asked to approve an app rather than to hand over a password, and multi-factor authentication does not help because nothing was stolen — it was granted.

Users can register applications	**Allowed**	Graph /policies/authorizationPolicy defaultUserRolePermissions

> **Recommended fix:** Restrict application registration to administrators, and require admin consent for applications requesting access to data.

MEDIUM 1 third-party application has access to SharePoint and OneDrive content

These hold organisation-wide access to files, and read what they can reach. That is the same content the rest of this report assesses for over-sharing, reached by something that does not appear in any sharing list.

Third-party applications with consent	**3**	Graph /servicePrincipals appRoleAssignments
Tenant-wide read of SharePoint and OneDrive	**1**	Files.Read.All / Sites.Read.All application permission

> **Recommended fix:** Confirm each application is still in use and still supplied by who you think it is. Remove the ones that are not.

MEDIUM 1 application carries no publisher details in Entra

Entra records no verified publisher for these, so who supplied them cannot be confirmed from the tenant alone. That is not an accusation: publisher verification is optional, and reputable vendors — particularly ones sold through IT providers rather than direct — routinely skip it. Applications built in-house never have it at all. The point is that each of these holds broad access and Entra cannot tell you who stands behind it, so somebody has to.

Third-party applications with consent	**3**	
With no verified publisher	**1**	servicePrincipal verifiedPublisher absent

> **Recommended fix:** Name the supplier and the internal owner for each. Recognising the vendor is enough; the ones to worry about are those nobody can account for.

MEDIUM Temporary access passes can be used more than once

A temporary access pass is a complete sign-in on its own — no password, no second factor — issued so that somebody can register their first method. Set to be reusable, one pass read out over the phone lets the caller in as many times as they like until it expires, and an administrator may issue one that lives for 30 days.

Temporary Access Pass	**Enabled**	Graph /policies/authenticationMethodsPolicy
One-time use	**No**	
Default lifetime	**8 hours**	

> **Recommended fix:** Set passes to one-time use with a default lifetime of an hour or less. Onboarding does not need longer; the pass is used once, at the desk, to register a passkey, and is then finished with.

MEDIUM Text message can still be registered as a sign-in method

The methods a person can be persuaded to add are the methods the policy leaves open. A phone number is the easiest of all: it is registered in seconds, it survives a password reset, and the code it receives can be relayed by the person who holds it to anyone convincing enough to ask. Whoever is currently registered on one is reported under Multi-Factor Coverage; this is about closing the door for everyone else.

Text message	**Enabled**	Graph /policies/authenticationMethodsPolicy
Phone call	**Disabled**	

> **Recommended fix:** Disable text message and voice in the authentication methods policy once the people relying on them have moved to the Authenticator app or a passkey — the registration campaign below does that work. Disabling the method does not lock anyone out who holds another.

LOW 2 policies are in report-only mode

These were probably switched to report-only for testing. Left that way they record activity without preventing anything.

Policies	**3**	
Enforced	**1**	
Report-only	**2**	state = enabledForReportingButNotEnforced

> **Recommended fix:** Confirm whether each is still being evaluated, and enable or remove the ones that are not.

LOW CALCULATED 2 applications have held access for more than 2 years

Consent does not expire. These were approved at some point, for some reason, and have held their access ever since — through staff changes, supplier changes and system replacements. Long-lived access is not wrong; long-lived access nobody has reviewed is how an estate accumulates doors that nobody remembers fitting.

Third-party applications with consent	**3**	
Granted more than 2 years ago	**2**	servicePrincipal createdDateTime

> **Recommended fix:** Add an annual review of consented applications. Anything without a current owner and a current reason should be removed.

LOW 2 passwordless credentials issued to people by somebody else

Registered since 19 July: 2 temporary access passes. Passes and passkeys issued by an administrator are how new starters get going, so on their own these are routine. What makes them worth a glance is whether the issuer expected to be issuing them: a helpdesk account whose session has been taken over issues exactly the same passes.

Security-info changes in the audit log, last 30 days	9	Graph /auditLogs/directoryAudits
Strong methods registered by somebody other than the account holder	2	initiatedBy differs from target

Recommended fix: Check that each was raised through the normal joiner or reset process, and that the issuing accounts are the ones meant to be doing it.

LOW Authenticator prompts do not show which application is asking or where the sign-in is coming from

A prompt that arrives while the caller is on the line, saying "approve this to finish setting up your passkey", is approved. The same prompt showing "Microsoft Graph — from Lagos" is refused, or at least questioned. The context costs nothing and is switched off by default.

Authenticator shows the application	No	Graph /policies/authenticationMethodsPolicy microsoftAuthenticator featureSettings
Authenticator shows the location	No	

Recommended fix: Enable application name and geographic location in the Microsoft Authenticator settings of the authentication methods policy.

LOW People cannot report a prompt they did not ask for

Report suspicious activity puts a button on the prompt that the employee did not initiate. Pressing it marks the account high-risk and raises an alert. Without it, the first unexpected prompt is a shrug, the tenth is approved.

Report suspicious activity	Disabled	Graph /policies/authenticationMethodsPolicy reportSuspiciousActivitySettings

Recommended fix: Enable report suspicious activity in the authentication methods policy, and make sure somebody receives the resulting alert.

LOW No registration campaign is nudging people to a stronger method

Microsoft can prompt people at sign-in to set up the Authenticator app, which is how a tenant gets off text messages without a project. It is off here, so the estate moves only as fast as somebody chases it.

Registration campaign	Disabled	Graph /policies/authenticationMethodsPolicy registrationEnforcement

Recommended fix: Enable the registration campaign in the authentication methods policy. A short snooze period and a modest daily prompt is enough.

LOW The legacy multi-factor and password-reset policies still apply

Microsoft has three places a method can be permitted, and this tenant has not finished consolidating them into one. Until it does, a method disabled in the modern policy can remain allowed by the legacy one, and the settings reported here describe only part of what is in force.

Policy migration state	**migrationInProgress**	Graph /policies/authenticationMethodsPolicy policyMigrationState

> **Recommended fix:** Complete the authentication methods migration in the Entra admin centre. Microsoft has announced the legacy policies are being retired; doing it deliberately beats having it done to you.

INFO 1 control has been marked as covered elsewhere or not applicable

Somebody has reviewed these and decided they are handled by another product or do not apply. That is a legitimate answer, and they are listed here only so the decision is visible rather than invisible.

Recommended controls	11	
Marked third-party, alternative or ignored	1	controlStateUpdates

> **Recommended fix:** Worth confirming the third-party product named is still in place, since these decisions outlive the arrangements that prompted them.

INFO CALCULATED 1% of accounts hold a phishing-resistant method

Phishing-resistant methods are present but not yet the norm. The order that works is administrators first, then the people who handle payments and supplier details, then everybody — rather than a tenant-wide switch that generates enough exceptions to undo itself.

Accounts in the registration report	69
Holding a phishing-resistant method	1 (1%)

> **Recommended fix:** Set a target of every privileged account on a phishing-resistant method, then extend by role rather than by percentage.

INFO 1 passkey registered in the last 30 days

Passkeys are the right direction, and these are reported so that each can be recognised rather than because any is wrong. The attacks this dimension exists for end with a passkey being registered; an organisation that knows which passkeys it expected to see is the one that spots the extra one.

Security-info changes in the audit log, last 30 days	9	Graph /auditLogs/directoryAudits
Passkeys registered on non-administrator accounts	1	

> **Recommended fix:** Nothing to fix. Keep a habit of reviewing new passkey registrations weekly, which takes a minute in the audit log.

INFO NOT ASSESSED Remote-support governance was not assessed

Whether Quick Assist is restricted, whether Remote Help is scoped to the helpdesk, and which third-party remote tools are permitted are not readable through the interface this assessment uses, so they form no part of the score above. They are the step the documented attacks actually turn on: the employee grants the session willingly.

> **Recommended fix:** Answer three questions internally. Which remote-support tools are permitted, who is allowed to initiate a session, and how would an employee verify that the person asking really is the helpdesk. If the last one has no answer, that is the place to start.

Email & Domain

6 FINDINGS · 4 NEEDING ATTENTION

CRITICAL 2 mailbox rules send company mail to an outside address

Mail arriving in these mailboxes is copied or redirected to an address outside the organisation, automatically and without anybody being told. Some rules like this are legitimate — a person forwarding to their own second address, or to an accountant. The rest are how a compromised mailbox keeps paying out long after the password has been changed, and the two are indistinguishable from here. Each one needs an owner who recognises it.

Mailboxes with rules examined	3	Graph /users/{id}/mailFolders/inbox/messageRules
Enabled rules forwarding outside the organisation	2	

Recommended fix: Ask each mailbox owner whether they created the rule. Anything nobody recognises should be removed, that mailbox's sign-in history reviewed, and its sessions revoked.

CRITICAL 1 domain has no DMARC record, so anybody can send email as this organisation

Without DMARC, a receiving mail server has no instruction about what to do with a message that claims to come from this domain but did not. Most will deliver it. That is how a supplier receives an invoice from the finance director's address with different bank details on it, and how staff receive a request from the managing director that the managing director never sent. The forged message is not a copy of the domain — it is the domain.

Custom domains checked	2	Graph /domains, excluding onmicrosoft.com
Without a DMARC record	1	public DNS, _dmarc.<domain> TXT

Recommended fix: Publish a DMARC record starting at p=none to see who is currently sending as you, then move to p=quarantine and p=reject once the legitimate senders are accounted for. It is a DNS change and costs nothing.

HIGH 1 mailbox rule deletes incoming mail automatically

These rules delete matching mail before the recipient sees it. Used honestly this is tidiness. Used dishonestly it is the second half of an invoice fraud: the rule quietly removes the replies querying the changed bank details, so the person being impersonated never learns of it and the conversation continues without them.

Mailboxes with rules examined	3	Graph /users/{id}/mailFolders/inbox/messageRules
Enabled rules that delete incoming mail	1	

Recommended fix: Confirm each rule with the mailbox owner, paying particular attention to any keyed on words like invoice, payment, bank or the name of a supplier.

HIGH DMARC is published but set to take no action on 1 domain

A policy of p=none means forged mail is reported and then delivered anyway. This is the correct place to start and the wrong place to stop, and it is where most organisations stop — the record exists, the box is ticked, and nothing is being blocked. Anyone checking whether this domain is protected will be told it is.

Custom domains checked	2	Graph /domains, excluding onmicrosoft.com
DMARC published with p=none	1	public DNS, _dmarc.<domain> TXT

Recommended fix: Review the DMARC reports for legitimate senders that would fail, fix those, then move the policy to quarantine and finally to reject.

MEDIUM **DKIM signing is not configured for 1 domain**

DKIM adds a signature that survives forwarding, where SPF does not. Without it, legitimate mail that has been forwarded — through a mailing list, or a client's own rules — can fail checks and be treated as forged. This becomes the reason DMARC enforcement gets rolled back after complaints.

Custom domains checked	2	Graph /domains, excluding onmicrosoft.com
Without DKIM selectors for Microsoft 365	1	public DNS, selector1/selector2._domainkey.<domain> CNAME

Recommended fix: Enable DKIM for these domains in the Microsoft 365 Defender portal and publish the two CNAME records it gives you. Do this before moving DMARC to reject.

INFO **1 rule of this kind is present but switched off**

These rules would forward or delete mail if they were enabled. They are not, so nothing is happening today. They are listed because a rule that was switched off can be switched back on, and one nobody remembers writing is worth asking about now rather than later.

Rules of this kind, switched off	1	messageRule.isEnabled = false

Recommended fix: Delete the ones nobody recognises. There is no cost to removing a rule that is doing nothing.

Content & Protection

19 FINDINGS · 9 NEEDING ATTENTION

CRITICAL INFERRED **37 likely-sensitive files with no sensitivity label**

Without a label these files carry no protection that travels with them — no encryption, no "do not summarise", and no DLP rule can act on them. Anything with access treats them like any other document, Copilot included.

Files crawled	389	
Without a sensitivity label	210	driveItem sensitivityLabel
Of which look sensitive	37	file name and type heuristics

Recommended fix: Run auto-labelling policies (or apply labels manually) to sensitive content. Consider a default label on high-risk libraries (HR, Finance, Legal).

CRITICAL **20 files shared via anonymous "anyone with the link" links**

Anonymous links bypass identity entirely — anyone holding the URL can open the file, and the link can be forwarded outside the organisation without leaving a trace. Nothing records who has it, so there is no way to answer who has seen a file, and no way to withdraw it from one person without breaking the link for everybody.

Files crawled	389	
With an anonymous sharing link	20	driveItem permissions, link.scope = anonymous
Sites crawled	8 of 8, 100% of content by volume	

Recommended fix: Disable anonymous link creation at the tenant/site level and expire existing anonymous links. Replace with specific-people or company-wide links where sharing is genuinely needed.

CRITICAL INFERRED

9 likely-sensitive files over-shared

These files look like they hold personal, financial or HR data, and are reachable org-wide or anonymously. That combination is the one worth fixing first whatever else is going on — it is a live exposure today, not a risk that begins when something new is switched on.

Files shared anonymously or organisation-wide	56	
Of which look sensitive	9	sensitivity label or classification signal

Recommended fix: Restrict access and apply a sensitivity label to these before anything else on this list.

HIGH

36 files shared org-wide ("Everyone")

Company-wide sharing means every member of staff can open these files, whether or not that was ever the intention. Sharing set up for convenience is rarely revisited once it works. It is also a common cause of Copilot answering from something it should not have.

Files crawled	389	
Shared with Everyone / organisation-wide	36	driveItem permissions, link.scope = organization or an Everyone claim

Recommended fix: Review org-wide shares and scope them to the owning department or a security group. Prioritise anything flagged as containing sensitive information.

HIGH

The tenant permits anonymous "anyone with the link" sharing

This setting is why 20 files in this scan are reachable by anybody holding a URL, with no sign-in and no record of who opened them. Those files can be fixed one by one, but while the setting stands the next person to press Share will create more.

Tenant sharing capability	**externalUserAndGuestSharing**	Graph /admin/sharepoint/settings sharingCapability
Files in this scan shared by anonymous link	20	

Recommended fix: Restrict sharing to guests who sign in, so that access is attributable and can be withdrawn. Where anonymous links are genuinely needed, set an expiry on them.

HIGH CALCULATED

14 guest accounts over a year old

Long-lived guest accounts are rarely reviewed and often outlast the project they were invited for, leaving standing external access to your content.

Guest accounts	18	Graph /users userType = Guest
Created over a year ago	14	user createdDateTime

Recommended fix: Run an access review of external guests and remove those no longer needed. Enable Entra access reviews to recertify guests on a schedule.

HIGH

2 workspaces with no owner

Ownerless sites and Teams have nobody accountable for their content, access or lifecycle. They accumulate risk silently and are a common audit finding.

Workspaces (Microsoft 365 groups)	7	Graph /groups owners
With no owner	2	

Recommended fix: Assign at least two owners to every workspace. Use an ownerless-group policy so Microsoft 365 prompts members to take ownership automatically.

HIGH Sharing defaults to the widest option rather than the narrowest

When somebody presses Share, the link they are offered first is one that works for more people than they probably intend. Most sharing is done quickly and accepts whatever is offered, so this single setting shapes most of what ends up over-shared.

Default sharing link type	**anonymous**	Graph /admin/sharepoint/settings defaultSharingLinkType

> **Recommended fix:** Change the default to specific people. Anyone who needs a wider link can still choose one; they will simply have to mean it.

HIGH INFERRED 1 account synced far more files than the rest of the organisation

The typical person here synced 26 files to a device in the last 30 days. user61@kirkwell.co.uk synced 4,180 — 4,180 of the 5,773 files synced across the whole tenant. Syncing is how a library leaves the tenant in bulk: one click, every file, to whatever machine holds the session. A new starter setting up a laptop looks exactly like this. So does the first day of an intrusion. No enforced policy requires a managed device, so the machine it went to could be anyone's.

People active in SharePoint or OneDrive, last 30 days	**59**	Graph /reports getSharePointActivityUserDetail
Files synced across the organisation	**5,773**	
Accounts far above the rest	**1**	
Enforced policy requires a managed device	**No**	

> **Recommended fix:** Ask. Each of these is a person whose manager can say in a sentence whether that volume makes sense this month. Where it does not, revoke the account's sessions and check its sign-ins before anything else. Then require a compliant device for SharePoint and OneDrive, which turns the question from "who" into "which of our machines".

MEDIUM 173 further files with no label

Where most content is unlabelled, data-governance controls cannot be applied with any precision — DLP, retention and any AI-access restriction all key off the label. Broad coverage is what makes the rest of it enforceable.

Files crawled	**389**	
Without a sensitivity label	**210**	driveItem sensitivityLabel

> **Recommended fix:** Define a simple label taxonomy (e.g. Public / Internal / Confidential) and drive coverage up with auto-labelling.

MEDIUM CALCULATED 79 files not modified in over 2 years

Of these, 26 are more than 4 years old. Superseded documents do not announce themselves — they sit in search looking identical to the current version and get quoted in good faith. Anything reading the library, staff and Copilot alike, treats them as current.

Files crawled	**389**	
Not modified in over two years	**79**	driveItem lastModifiedDateTime
Of which over four years	**26**	

> **Recommended fix:** Archive or move superseded content out of active libraries, or apply a retention or archive label so it can be scoped out of search. Establish a review-by date for key documents.

MEDIUM CALCULATED

53 duplicate copies across 21 sets of identical files

The most duplicated file exists in 6 places. When the same content lives in several locations nobody can tell which one is authoritative — including the people relying on it, and any search or assistant reading across them.

Files with a content hash	389	driveItem file.hashes.quickXorHash
Sets of identical files	21	
Redundant copies	53	

Recommended fix: Consolidate to a single source of truth and replace copies with links. Prioritise duplicate sets that span multiple sites or departments.

MEDIUM INFERRED

49 poorly named files

Generic and versioned names ('Document1', 'Copy of…', 'FINAL v3') carry no meaning to search. If someone cannot find a document by name they recreate it, which is how duplicate sets start. The same missing signal makes search return the wrong file.

Files crawled	389	
Named like a scan, a version or a draft	49	file name pattern

Recommended fix: Adopt a naming convention and rename the worst offenders. Encourage descriptive titles and use metadata columns instead of encoding version/status into the filename.

MEDIUM CALCULATED

1 SharePoint site inactive for 12+ months

Abandoned sites still hold their data and still appear in search, long after anyone stopped maintaining them. They widen the surface that has to be secured and reviewed, and they are where content nobody has looked at in years quietly stays reachable.

SharePoint sites	8	Graph /sites
Inactive for twelve months or more	1	site lastModifiedDateTime

Recommended fix: Confirm ownership, archive or delete abandoned sites, and set an inactivity policy so they are caught automatically in future.

MEDIUM

Anonymous links never expire

A link shared for one afternoon keeps working indefinitely. Nobody revisits them, so the set of live anonymous links only ever grows, and each one outlives the reason it was created.

Anonymous link expiry	Never	Graph /admin/sharepoint/settings anonymousLinkExpirationInDays

Recommended fix: Set an expiry — 30 days suits most work. Existing links are unaffected, so this stops the problem growing rather than fixing what is already there.

MEDIUM INFERRED

1 account shared far more files externally than the rest of the organisation

The typical person here shared 1 file outside the organisation in the last 30 days. user9@kirkwell.co.uk shared 46. Sharing a file to an outside address is the other way an estate leaves quietly: nothing is downloaded, the link simply works from wherever the recipient is, and it keeps working after the account is cleaned up. Some roles do this all day. The question is whether these are those roles.

People active in SharePoint or OneDrive, last 30 days	59	Graph /reports getSharePointActivityUserDetail
Accounts sharing externally far above the rest	1	

Recommended fix: Confirm the role. Where it does not fit, review what was shared and to whom in the SharePoint sharing reports, and remove the links that should not exist. The tenant-wide sharing defaults reported elsewhere decide how easily this can happen at all.

LOW CALCULATED **2 Teams with no recent activity**

Inactive Teams keep their SharePoint document libraries live and indexable long after the work has stopped.

Teams	6	Graph /teams
Inactive for twelve months or more, not archived	2	

Recommended fix: Archive dormant Teams to freeze their content while preserving it for reference.

LOW **2 workspaces with only one owner**

A single owner is a continuity risk — if they leave, the workspace becomes ownerless.

Workspaces (Microsoft 365 groups)	7	Graph /groups owners
With exactly one owner	2	

Recommended fix: Add a second owner to each of these workspaces.

INFO **18 guest accounts in the tenant**

Guests make up 9% of all accounts. Each is an identity outside the organisation that can hold access to sites and files, and that nobody inside manages day to day.

Accounts in the tenant	200	Graph /users
Of which guests	18	userType = Guest

Recommended fix: Confirm every guest is still required and governed by expiry / access-review policies.

Licensing & Devices

5 FINDINGS · 2 NEEDING ATTENTION

HIGH INFERRED **69 people are licensed for device management, and 14 devices are enrolled**

Device management is included in the subscriptions this organisation already holds. Where a device is not enrolled, none of it applies: company data on that machine cannot be protected, wiped if it is lost, or held to any standard. This is capability that is already paid for and is not being used.

People licensed for device management	69	Graph /subscribedSkus, service plans containing INTUNE
Devices enrolled in Intune	14	Graph /deviceManagement/managedDevices
Unaccounted for	55	

Recommended fix: Enrol company devices in Intune, starting with laptops that hold or access company data. No additional licence is needed — the entitlement is already there.

HIGH CALCULATED **15 licences paid for and assigned to nobody**

These subscriptions are being billed in full every month regardless of whether anyone holds them. Keeping a seat or two spare for a new starter is sensible; beyond that it is a standing cost with nothing behind it. The most common cause is somebody leaving and the licence never being released.

Paid seats bought	86	Graph /subscribedSkus prepaidUnits.enabled
Paid seats assigned	71	Graph /subscribedSkus consumedUnits
Microsoft 365 Business Premium	61 of 68 assigned, 7 spare	
Microsoft 365 E3	8 of 12 assigned, 4 spare	
Visio Plan 2	2 of 6 assigned, 4 spare	

Recommended fix: Review each subscription against current headcount and reduce the quantity at the next billing date, keeping a small buffer for new starters. Your Microsoft partner or the Microsoft 365 admin centre can adjust the counts.

MEDIUM **2 enrolled devices fail the organisation's own policy**

These devices are enrolled but do not meet the rules this organisation has itself set — commonly a missing update, disabled encryption, or no screen lock. A device failing policy is usually a device that has drifted rather than one that was never set up.

Enrolled devices	14	
Marked non-compliant by the tenant's own policy	2	Graph managedDevice.complianceState

Recommended fix: Review the failures by reason in the Intune admin centre. Most resolve by bringing the device up to date rather than by changing any policy.

MEDIUM CALCULATED **2 devices have not checked in for over 30 days**

An enrolled device that has stopped contacting Intune is managed on paper only. It will not receive policy, will not report its state, and cannot be wiped remotely if it is lost. The usual causes are a machine that has been retired without being removed, or one that has quietly fallen out of management.

Enrolled devices	14	
Not checked in for over 30 days	2	Graph managedDevice.lastSyncDateTime

Recommended fix: Retire devices that are genuinely gone so the estate reflects reality, and investigate any that should still be in use.

LOW **Microsoft 365 Business Premium already includes device and identity protection**

61 users hold Microsoft 365 Business Premium, which entitles this organisation to capabilities that are frequently bought again elsewhere or simply left switched off — device management, conditional access and information protection among them.

Subscription	**Microsoft 365 Business Premium**	Graph /subscribedSkus
Seats assigned	61	
Included capabilities	**Intune device management, Conditional Access (Entra ID P1), Information protection, Defender for Business, Multi-factor authentication**	servicePlans on the subscription

Recommended fix: Before considering additional security products, confirm which of these are actually switched on. Turning on something already paid for is the cheapest security improvement available.

Workplace Experience

7 FINDINGS · 2 NEEDING ATTENTION

HIGH CALCULATED **10 intranet pages not updated in over 2 years**

Outdated pages make an intranet feel abandoned, and staff stop checking it — which is usually when people start keeping their own copies instead. Search and Copilot both cite the content as though it were current.

Published intranet pages	30	Graph /sites/{id}/pages
Not updated in over two years	10	page lastModifiedDateTime

Recommended fix: Assign page owners and a review-by date, refresh or retire stale pages, and consider page-level expiry on time-sensitive content.

HIGH 1 site is running a business process on retired technology

These sites hold form libraries — the shape of an application rather than a document store. Somebody built a form, connected it to a process, and the business has been running on it since. InfoPath, which is what these libraries were built with, has been out of support for years, and the classic surfaces around it are dated for read-only from October 2028. The risk is not the deadline. It is that nobody currently employed knows what the form does or what depends on its output.

Sites with legacy markers inventoried	8	site list templates
Running a business process on retired technology	1	InfoPath form libraries or workflow lists

> **Recommended fix:** Find the owner and the process for each one now, while there is time to rebuild rather than react. Power Apps and Power Automate cover most of what these were built to do. Where nobody can say what a form is for, that is the answer — but confirm it before deleting it.

MEDIUM 1 active site with no published landing page

These sites hold real content but present visitors with a bare document library instead of a modern page with navigation, news and context — a poor front door.

Sites in active use	8	content crawled and 5+ files
With no published landing page	1	

> **Recommended fix:** Add a modern home page to each active site with clear navigation, key links and an owner. Use a site template to make this consistent.

MEDIUM 1 site uses classic publishing and is still active

These sites keep their pages in a classic publishing library rather than in Site Pages, and 34 classic pages were found in them. Microsoft has set March 2027 and October 2028 as the milestones for classic page retirement, with affected pages becoming read-only for existing tenants in the later phase. Because these sites are in use, doing nothing means somebody discovers they cannot edit an important page, at short notice, without a plan.

Sites with legacy markers inventoried	8
Classic publishing, still active	1
Classic pages between them	34

> **Recommended fix:** Work through them in order of use rather than in order of age. Most classic pages are a communication site and an afternoon; the ones that resist are the ones carrying custom code, and those are worth identifying early.

LOW 2 pages stuck in draft

Draft pages are invisible to visitors — someone started them but never published. They clutter authoring views and represent unfinished intranet work.

Intranet pages	32	Graph /sites/{id}/pages
In draft	2	publishingState = draft

> **Recommended fix:** Review draft pages: publish the ones that are ready and delete the abandoned ones.

LOW CALCULATED **1 classic site has not been touched in over two years**

Classic markers, and no activity since before the retirement dates were announced. These are almost certainly finished work rather than live systems, and migrating them would be paying to move something nobody opens. They still carry whatever was shared out of them, which is the reason to close them rather than simply ignore them.

Sites with legacy markers inventoried	8	
Classic sites untouched for over two years	1	site lastModifiedDateTime

> **Recommended fix:** Confirm there is no retention or legal obligation, export anything worth keeping, then archive or delete. This is the cheapest item on the list and it shrinks everything that follows.

INFO NOT ASSESSED **Custom script permissions were not assessed**

Whether a site permits custom script is not readable through the interface this assessment uses, so it forms no part of the result above. It matters for the same sites: custom script is how most classic customisation was delivered, and it is what makes a migration hard rather than routine.

> **Recommended fix:** Check the setting directly on the sites listed above before scoping any migration work, and disable it wherever nothing depends on it.

Copilot Readiness

5 FINDINGS · 3 NEEDING ATTENTION

CRITICAL INFERRED **9 likely-sensitive files are readable across the organisation before Copilot is switched on**

Copilot answers with whatever the person asking is already allowed to see. These files are already open to everyone; today that is only a risk if somebody goes looking. With Copilot, asking "what do we pay people?" or "what were the board's concerns?" is enough to find them, and it will answer honestly.

Files crawled	389	
Reachable anonymously or organisation-wide	56	
Of which look sensitive	9	sensitivity label or classification signal

> **Recommended fix:** Resolve the sharing on these before any Copilot rollout. This is the single most common reason an AI pilot has to be paused after launch rather than before.

HIGH **2 third-party applications can already read the content Copilot would draw on**

These applications hold standing consent to read files across the tenant. They were approved once, by somebody, at some point, and they do not require a person to be signed in to use it. Any governance decision taken about what Copilot may see is incomplete while these hold the same access with less visibility over what they do with it. 1 of them has an unverified publisher.

Third-party applications with tenant-wide file read	2	Graph /servicePrincipals appRoleAssignments — Files.Read.All / Sites.Read.All
Of which unverified publisher	1	verifiedPublisher absent

> **Recommended fix:** Review each one against a named business owner and a reason. Remove consent where neither exists — an application nobody can account for is not one to leave reading everything. This review belongs in the same conversation as the Copilot rollout, not a separate one.

HIGH Sign-in protection is not enforced, and Copilot raises what an account is worth

A compromised account currently gives an intruder whatever that person can reach, if they know where to look. With Copilot it gives them a research assistant over the same material. The account becomes a more valuable target without becoming better defended.

Enforced Conditional Access policies covering sign-in	0	Graph /identity/conditionalAccess/policies

Recommended fix: Enforce multi-factor authentication before rollout rather than after.

LOW CALCULATED 38 people work in Teams and documents daily — the natural first group

Of 52 licensed users active in the last 30 days, these also work across Teams and files, which is the material Copilot draws on. Starting with people who already collaborate is what makes a pilot look successful; starting with everyone is what makes it look expensive. A further 17 licensed 17 accounts have shown no activity at all, which is worth resolving before adding anything to them.

Licensed users active in the last 30 days	52	Graph /reports getOffice365ActiveUserDetail
Of which active daily in Teams and documents	38	
Licensed but inactive	17	

Recommended fix: Pilot with this group first and measure it before widening. Copilot is charged per user per month, so who goes first is a cost decision as much as a technical one.

INFO NOT ASSESSED Web grounding governance was not assessed

Copilot and Copilot Chat answer from the public web as well as from this organisation's own content, and web grounding is on by default for every licensed person. Which sites it may draw on is decided in two places, neither of which this assessment can read: the "Allow web search in Copilot" policy, which says whether web grounding is on and for whom, and the domain exclusion list, which lets an administrator name up to a thousand sites Copilot must never cite. No tenant has an exclusion list unless somebody has deliberately created one, and both are readable only by a signed-in administrator.

Recommended fix: Answer three questions before the licences are bought. Is web grounding meant to be on, and for everyone or for named groups? Which sources should Copilot never cite — competitors, content farms, anything the organisation's own policies already bar? And has anyone configured the exclusion list? If the last answer is no, the list is empty, and every answer with a web citation in it can cite anything.

Hand-over document: Copilot web source policy — a one-page template →

VITALS
A product by Innova Group

NEXT STEPS

What to do next

The findings above are in priority order, each with the reasoning behind it. You are free to work through the list yourself or hand it to your existing IT provider — it is yours either way. If you would rather we carried out the remediation, Innova Group can do that and re-scan afterwards so you can see exactly what changed. Where there is nothing meaningful to fix, we will tell you that instead.

GET IN TOUCH

hello@innovagroup.tech · innovagroup.tech