

Is Your Microsoft 365 Tenant Ready for Copilot?

A practical readiness guide for London businesses

Ten checks to run before you turn Copilot on — and what to do about what you find



Secure. Protect. Thrive.

The Cloudscape Success Pathway

August 2026

Microsoft Solutions Partner | 25+ years supporting London business

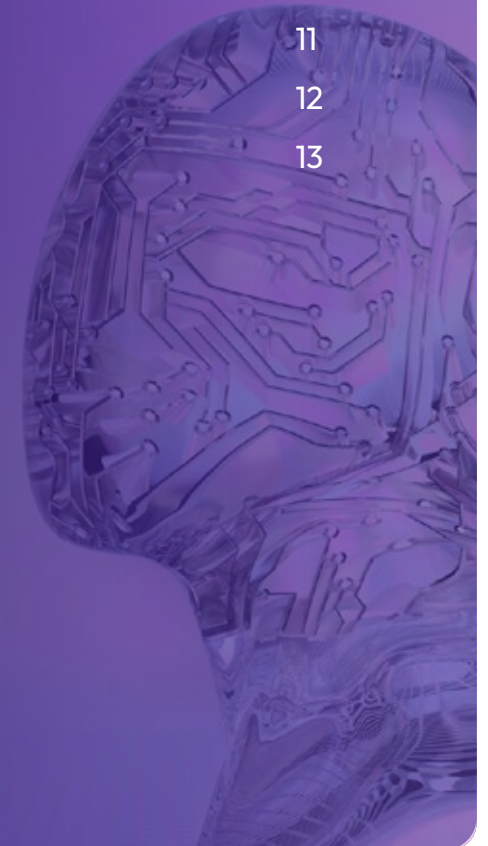
Who is this guide for

This guide is written for business owners, finance directors, practice managers and operations leads at London firms of roughly 20 to 250 people — the person who has been asked to “look into Copilot” and wants to understand the risk before committing budget.

It assumes no technical background. Where we name a Microsoft tool, it is so that you can ask your IT provider a specific question about it.



1.	Executive summary	3
2.	The risk is not the AI. It is the permissions.	4
3.	What Copilot can actually see	5
4.	The licensing picture in 2026	6
5.	The ten readiness checks	7
6.	The remediation sequence	9
7.	Sector notes: financial services, legal, professional and creative	10
8.	Timescales and effort	11
9.	Self-assessment scorecard	12
10.	Where to start	13



1. Executive summary



Microsoft 365 Copilot is not unsafe. It respects the permissions you already have. That is precisely the problem.

Copilot answers questions by retrieving whatever the person asking is already allowed to open — email, calendar entries, SharePoint documents, OneDrive files, Teams messages and meeting transcripts. It does not break your permissions. It uses them, at speed, across your entire estate, in response to a plain-English question.

In most organisations, permissions have accumulated over years without review. Files shared with “everyone in the organisation” during a project in 2019 are still shared that way. Sites created for a tender have no owner. A departed employee’s access was never fully unwound. None of this caused a visible problem, because finding those files by hand required knowing they existed.

Copilot removes that obstacle. It will find them, summarise them, and present them to anyone who asks the right question — without malice, and without any breach having occurred.

What the evidence shows

- Industry research indicates that more than 15% of business-critical files are exposed through oversharing, misconfigured access permissions or inappropriate classification.
- Around 67% of enterprise security teams report concerns about AI tools exposing sensitive information.
- IBM has found that 63% of organisations that suffered a breach either had no AI governance policy or were still developing one.
- Microsoft’s own deployment guidance puts oversharing remediation first — before rollout — across a three-phase model: Pilot, Deploy, Operate.

Our position

Copilot is worth deploying. The productivity gains are real, and firms that hold back indefinitely will be at a disadvantage. But the sequence matters enormously, and the sequence most businesses follow is the wrong way round: buy licences, switch it on, discover the problem.

The right sequence is: assess what Copilot would be able to see, contain the worst

of it quickly, remediate the underlying permissions properly, then deploy — and keep governing it afterwards.

This guide sets out ten checks you can use to judge your own readiness, the Microsoft controls that address each finding, and a realistic view of the time and effort involved. Section 9 is a scorecard you can complete in about twenty minutes.



THE ONE-SENTENCE VERSION

If you would be uncomfortable with any member of staff being able to ask a question and receive a tidy summary of everything they technically have access to, you are not ready to deploy Copilot — and the work required is permissions work, not AI work.

2. The risk is not the AI. It is the permissions.



There is a great deal of anxiety about whether AI tools are safe to use with confidential information. For Microsoft 365 Copilot specifically, the common fears are largely misplaced, and the actual risk sits somewhere less dramatic but far more likely.

What Copilot does not do

- It does not train Microsoft's foundation models on your business data.
- It does not give users access to anything they could not already open themselves.
- It does not send your documents outside the Microsoft 365 service boundary in normal operation.

What Copilot does do

It collapses the effort required to find information. Where an employee would previously have needed to know that a file existed, guess its name, and search for it, they can now ask a question in ordinary language and receive a synthesised answer drawn from across the tenant.

Years of accumulated governance debt — harmless while it stayed hard to find — becomes immediately accessible.

Five questions that go wrong in an unprepared tenant

These are the kinds of prompts that surface problems. None of them requires bad intent.

- **“What is everyone's salary?”** Returns the compensation spreadsheet HR shared with a hiring manager eighteen months ago and never unshared.
- **“Summarise what we know about the redundancy plan.”** Returns draft board papers stored in a SharePoint site whose permissions were inherited from a parent site.
- **“What are our margins on the Henderson account?”** Returns commercially sensitive pricing that account team members were never meant to see across client boundaries.

- **“Has anyone raised concerns about my manager?”** Returns grievance correspondence held in a site shared with “everyone except external users”.
- **“What did the partners discuss about my performance?”** Returns meeting transcripts and chat threads that were never intended to be discoverable.



WHY THIS MATTERS COMMERCIALY

A Copilot deployment that surfaces the wrong information does not just create a data protection problem. It creates an employee relations problem, a client confidentiality problem and, for regulated firms, a reportable one.

It is also entirely avoidable, and the remediation work has value regardless of whether you ever deploy Copilot — you are fixing permissions that should not have been that way in the first place.

3. What Copilot can actually see



Copilot retrieves information through Microsoft Graph, the layer that connects your Microsoft 365 services. When someone asks a question, it draws on:

- Email in Exchange Online
- Files in SharePoint Online and OneDrive for Business
- Teams chat messages and channel conversations
- Meeting transcripts and recordings, where these are enabled
- Calendar entries

In every case, the boundary is what the signed-in user has permission to access. So the practical question is not “what can Copilot see?” but “what can each of my staff currently reach?” Most organisations have never answered that question precisely.

Where oversharing comes from

Six patterns account for the overwhelming majority of exposure. Your IT provider should be able to report on each.

Pattern	What it means	Why it happens
Everyone-except-external-users	Content shared with a built-in group covering every internal account, so any licensed user can reach it.	The default path of least resistance when someone wants colleagues to see a file.
Broken permission inheritance	A subsite or folder no longer follows its parent's permissions, so access has drifted.	One-off changes made years ago to solve an immediate problem.
Organisation-wide sharing links	"Anyone in the organisation with this link" URLs that never expire.	Convenient for collaboration; invisible afterwards.
Ownerless and inactive sites	Sites whose owners have left, with no one reviewing membership.	Project sites outlive projects. Nobody archives them.
Legacy migration debt	Old file-share permissions carried wholesale into SharePoint during a cloud migration.	Lift-and-shift migrations that prioritised speed over restructuring.
Unclassified sensitive content	Confidential material with no sensitivity label, so no control can distinguish it.	Labelling was never rolled out, or was optional and therefore ignored.

A NOTE ON AI AGENTS

The same logic now applies to AI agents, not just Copilot chat. Agents built in Copilot Studio, and the agent management capabilities Microsoft introduced with Agent 365 in 2026, all operate against the same permission model.

An agent scoped to specific SharePoint sites is far safer than one with tenant-wide reach. If your provider is proposing agents, ask what they are scoped to.



4. The licensing picture in 2026



Copilot licensing changed substantially through 2026, and the changes affect the business case as much as the technology does. The table below reflects Microsoft list pricing as at August 2026.

Option	List price (USD, per user/month)	Notes
Microsoft 365 Copilot Business	£19	For tenants on Microsoft 365 Business plans with up to 300 users. Available since 1 December 2025. The relevant option for most SMEs.
Microsoft 365 Copilot add-on	£24	For E3 and E5 tenants. Requires a qualifying Microsoft 365 base licence — Office 365 E3/E5 alone is not sufficient.
Microsoft 365 E3 (base)	£32	Increased from \$36 on 1 July 2026.
Microsoft 365 E5 (base)	£54	Increased from \$57 on 1 July 2026.
Microsoft 365 E7 "Frontier Suite"	£90	Generally available from 1 May 2026. Bundles E5, Copilot, Agent 365 and the Entra Suite. Worth modelling if you are already on E5 with Copilot.

The storage change nobody mentions

From 1 July 2026 Microsoft moved SharePoint storage towards pay-as-you-go billing. This matters more than it sounds for anyone running a Copilot readiness exercise: the dormant sites and abandoned project libraries that create your oversharing risk are now also a line item on your invoice.

That is unusually convenient. The clean-up that reduces your AI exposure also reduces your storage bill, which makes the business case considerably easier to put to a board.

Licence only who will use it

Copilot is most cost-effective when deployed to roles that will use it daily rather than across the whole business. Usage reporting in the Microsoft 365 admin centre lets you reassign licences from dormant users. We would rather help you deploy forty licences that get used than a hundred that do not.

TWO THINGS THAT CATCH PEOPLE OUT

1. SharePoint Advanced Management — the toolset that finds your oversharing problems — is included with a Microsoft 365 Copilot licence. You may already own the assessment tools you need.
2. Copilot Cowork, generally available since 16 June 2026, is billed in Copilot Credits on top of a Copilot licence. Usage-based costs need a budget owner.



5. The ten readiness checks



These are the checks we run during a Copilot readiness assessment. You can use them as a set of questions to put to your current IT provider. In each case, “we don’t know” is a finding in itself.

Check 1 ☐

Content shared with everyone in the organisation

What to check: How many sites and files are shared with “Everyone”, “Everyone except external users”, or broad security groups — and which of those contain sensitive material.

Why it matters: This is the single largest source of Copilot exposure. Content shared this way becomes part of the queryable surface for every licensed user in your tenant.

Good looks like: A report quantifying it, a plan to remove the group from sensitive sites, and specific named exceptions rather than blanket use.

Check 2 ☐

Broken permission inheritance

What to check: Which sites, libraries and folders have had inheritance broken, and whether anyone can explain why.

Why it matters: Broken inheritance is where access quietly diverges from intent. It is also where nobody thinks to look during a review.

Good looks like: Inheritance intact by default, with documented exceptions that have an owner and a review date.

Check 3 ☐

Sharing links that never expire

What to check: Volume and age of “anyone” and organisation-wide sharing links, and whether default expiry is configured.

Why it matters: A link created for a three-week project is still live four years later, and the person who created it has left.

Good looks like: Default expiry set on new links, a clean-up of historic ones, and the more permissive link types disabled where they are not needed.

Check 4 ☐

Ownerless and inactive sites

What to check: How many SharePoint sites have no active owner, and how many have not been touched in twelve to twenty-four months.

Why it matters: Nobody is reviewing who can reach this content, and Copilot has no way of knowing it is stale. It will happily summarise a superseded draft as though it were current.

Good looks like: Group expiration policies in place, ownership reassigned, and dormant sites archived or deleted — which also reduces your storage cost.

Check 5 ☐

Sensitivity label coverage

What to check: Whether sensitivity labels exist, whether they are applied to your genuinely confidential material, and whether labelling is automatic or relies on staff remembering.

Why it matters: Labels are the mechanism by which you tell Copilot what to leave alone. Without them, every control you might apply has nothing to act on.

Good looks like: A short, comprehensible label set — three or four options, not twelve — with automatic application for recognisable content types such as client identifiers, payment card data or HR records.

Check 6 ☐

Legacy migration debt

What to check: Whether your move to SharePoint restructured permissions or replicated the old file-share model wholesale.

Why it matters: Lift-and-shift migrations import decades of accumulated access decisions, most of which nobody has ever reviewed.

Good looks like: A permissions model that reflects how the business works now, rather than how the shared drive was organised in 2014.

Check 9 ☐

Audit and retention readiness

What to check: Whether Copilot interactions will be captured in your audit logs, how long they are retained, and who can review them.

Why it matters: If you cannot show what was asked and what was returned, you cannot investigate an incident, answer a subject access request, or satisfy a regulator.

Good looks like: Copilot interaction events captured in the unified audit log, retention aligned to your existing policy, and a named person with the access and the remit to review them.

Check 7 ☐

Guest and external access

What to check: Which external parties hold guest accounts, what they can reach, and whether their access was ever time-limited.

Why it matters: Guest access granted for a transaction or a matter frequently outlives it. Former advisers, contractors and counterparties accumulate.

Good looks like: Access reviews on a defined cycle, guest accounts with expiry, and a clear record of who granted what and why.

Check 10 ☐

Policy, ownership and training

What to check: Whether there is a written AI acceptable use policy, a named individual accountable for AI use, and any staff training beyond a launch email.

Why it matters: Technical controls fail without them. This is also the first thing a regulator, insurer or client due-diligence questionnaire will ask to see.

Good looks like: A policy of two or three pages in plain English, a named owner at leadership level, role-appropriate training, and a review cycle.

Check 8 ☐

Shadow AI

What to check: Which AI tools your staff are already using, on which devices, with what data — including consumer chatbots on personal phones and laptops.

Why it matters: This is usually the largest real exposure and the least measured. A properly governed Copilot deployment often reduces total risk, because it gives people a sanctioned tool and removes the incentive to use an unsanctioned one.

Good looks like: An AI register listing every tool in use, an acceptable use policy that staff have actually read, and technical controls on unmanaged devices.



SCORING YOUR ANSWERS

If you can answer checks 1 to 4 with specific numbers, you are in better shape than most. If checks 5, 8 and 10 draw a blank, start there — they are the cheapest to fix and they carry the most weight with regulators and clients.

Section 9 turns these ten checks into a scorecard you can complete yourself.

6. The remediation sequence



Microsoft's own deployment guidance follows three phases — Pilot, Deploy, Operate — and places oversharing remediation before rollout. The sequence below follows that model and names the specific controls involved, so you can ask your provider precise questions.

Stage 1 - Assess

- Run data risk assessments in Microsoft Purview Data Security Posture Management (DSPM) for AI to identify overshared sites holding sensitive data, risky sharing links and frequently accessed content.
- Run the SharePoint Advanced Management Content Management Assessment to surface sites with oversized audiences, everyone-except-external-users usage, broken inheritance, inappropriate sharing, and sites that are inactive or ownerless.
- Build an AI register covering every AI tool already in use across the business, sanctioned or otherwise.

Stage 2 - Contain

These controls reduce exposure quickly while the underlying permissions work is still in progress. They are containment, not a cure.

- Enable Restricted Content Discovery to exclude specified SharePoint sites from Copilot and agent discovery, regardless of who has permission to them. Useful for high-risk sites while remediation is scheduled.
- Apply restricted access control policies to limit an entire site to a named group of users, so its content only surfaces in Copilot for that group.
- Configure Microsoft Purview Data Loss Prevention for Copilot to prevent labelled content being used as grounding data, and to stop Copilot responding to prompts containing defined sensitive information types.

Stage 3 - Remediate

- Fix permissions at source: remove broad groups from sensitive sites, restore inheritance where it was broken without reason, and rebuild access around how the business actually works.
- Apply and, where possible, automate sensitivity labels on confidential material.
- Archive or delete dormant sites and stale content — reducing both exposure and storage cost.
- Set default expiry on sharing links and put guest access reviews on a cycle.

Stage 4 - Deploy

- Start with a defined pilot group and a limited content scope. Validate that restricted content is genuinely not surfacing before widening access.
- Train the pilot group properly, then use them to train everyone else.
- Scope any agents narrowly to the sites and connectors they actually need.

Stage 5 - Operate

- Monitor Copilot interaction events in the unified audit log and align retention to your existing policy.
- Use communication compliance to monitor for policy breaches and sensitive content in responses.
- Where you need hard separation between teams — a conflict wall between corporate finance and research, for instance — configure information barriers so Copilot cannot retrieve across the boundary.
- Review permissions, labels and the AI register on a defined cycle. Governance debt reaccumulates.

7. Sector notes



The technical work is broadly the same across sectors. The evidence you need to produce, and the person who will ask for it, is not.

Financial services

The FCA has been consistent that it does not intend to introduce AI-specific rules. Regulated firms are expected to manage AI through existing frameworks — which means the obligations are already live rather than pending.

- Where AI influences product design, pricing, eligibility, servicing or customer communications, Consumer Duty outcome requirements apply and outputs should be tested for fairness and foreseeable harm.
- Accountability under SM&CR needs to be explicit: a named individual owning AI use-case approval, model and data risk, third-party AI oversight and operational resilience.
- In May 2026 the Bank of England, FCA and HM Treasury issued a joint statement urging firms to

strengthen cyber resilience against frontier AI threats — noting that the cyber capability of current frontier models already exceeds what a skilled human attacker could achieve, at greater speed, scale and lower cost.

- The FCA reopened its AI Input Zone consultation in May 2026, and the Treasury Committee has asked for practical guidance on how consumer protection rules apply to AI by the end of 2026. Expect the expectations to become more specific, not less.

Legal

The SRA updated its compliance guidance on AI and technology on 9 February 2026. It introduced no new rules; it restated how the existing Standards and Regulations apply.

- Clients must be told where they are interfacing with AI.
- Client confidentiality obligations under the Code of Conduct apply in full when client data is processed by an AI vendor — which makes it essential to know where your data goes.
- The COLP is responsible for regulatory compliance when new technology is introduced.
- The SRA frames AI governance around leadership and oversight, risk and impact assessments, documented policies, staff training and ongoing monitoring — which maps closely onto checks 8, 9 and 10 in this guide.
- Many firms are now revising IT policies to control which AI tools are permitted for which categories of work. Matter-level separation makes information barriers particularly relevant.

Professional services and creative

You may not have a sector regulator, but you increasingly have clients who act like one. AI governance questions now appear routinely in supplier due diligence questionnaires, and the vendor whose documentation is complete and immediately available wins on trust before the commercial conversation concludes.

For creative businesses there is a second consideration: intellectual property and client confidentiality in generated output. Which client material may be used as input, and what happens to what comes out, should be a written position rather than an assumption.



ONE POINT THAT APPLIES TO EVERYONE

UK data protection law changed in February 2026. The Data (Use and Access) Act 2025 replaced Article 22 of the UK GDPR with new Articles 22A to 22D, making solely automated decisions about individuals lawful in more circumstances — but only where transparency, human review and the right to contest are in place and documented.

The safeguards are the condition, not an optional extra. If AI touches decisions about people, this applies to you.

8. Timescales and effort



Every environment differs, but the shape of the work is reasonably predictable. The table below reflects a typical 50 to 150 user Microsoft 365 tenant that has not previously been through a permissions review.

Stage	Typical duration	What drives it
Assess	1–2 weeks	Largely tool-driven. The output is a report, not a change. Fastest stage.
Contain	1–2 weeks	Configuration work. Quick, but requires decisions about which sites to restrict.
Remediate	4–12 weeks	The variable. Depends on volume of oversharing, whether labelling exists, and how quickly the business can make decisions about content ownership.
Pilot deployment	2–4 weeks	Runs in parallel with later remediation. Pilot group size and training appetite.
Full deployment	2–6 weeks	Licence provisioning and training, phased by department.
Operate	Ongoing	Quarterly permissions and label review; AI register maintenance.

Where projects go wrong

- Buying licences first. This creates pressure to deploy before the environment is ready, and the pressure usually wins.
- Treating containment as completion. Excluding sites from Copilot discovery hides the problem from the AI, not from your staff.
- Labelling everything. An over-complicated label set gets ignored. Three or four labels applied consistently beat twelve applied sporadically.
- Deploying to everyone at once. Licences go unused, training does not land, and any problem surfaces at maximum scale.
- Skipping the policy. It is the cheapest item on the list and the first thing anyone external will ask for.

What it costs

Assessment is inexpensive relative to the licences — and if you already hold Microsoft 365 Copilot licences, you already own SharePoint Advanced Management, which is the toolset that does most of the assessment work. Remediation is where the effort sits, and it is a function of accumulated debt rather than headcount.

The important commercial point: this work has value independent of Copilot. You are fixing permissions that should never have been that way, reducing storage cost, and producing governance evidence you will be asked for regardless.

9. Self-assessment scorecard



Score each row honestly. “We don’t know” scores zero — and is a legitimate answer that tells you something useful.
2 = in place and evidenced | **1** = partly in place | **0** = not in place or unknown

#	Question	Score
1	We know how many sites and files are shared with everyone in the organisation, and sensitive content has been removed from them.	
2	We know where permission inheritance has been broken, and each case has a documented reason.	
3	Sharing links expire by default, and historic links have been reviewed.	
4	No SharePoint site is ownerless, and dormant sites are archived on a defined cycle.	
5	Sensitivity labels exist, are applied to confidential material, and application is largely automatic.	
6	Our SharePoint permissions reflect how the business works now, not our old file-share structure.	
7	Guest accounts have expiry dates and external access is reviewed on a cycle.	
8	We have a register of every AI tool in use across the business, including on personal devices.	
9	Copilot interactions would be captured in our audit log, retained appropriately, and reviewable by a named person.	
10	We have a written AI acceptable use policy, a named accountable owner, and staff have been trained.	

Interpreting your score

Score	Where that leaves you
16–20	Strong position. Proceed to a pilot deployment with confidence, and focus on the operating disciplines that keep it this way.
10–15	Typical, and workable. Containment controls will let you pilot within weeks while remediation continues underneath.
5–9	Do not deploy tenant-wide yet. Assess properly first — the exposure is likely to be greater than you expect, and the assessment is quick.
0–4	Copilot is not your most urgent problem. The permissions position needs attention on its own merits, and fixing it will deliver value whether or not you ever deploy AI.

IF YOU SCORED LOW, THAT IS THE NORMAL RESULT

Most organisations score in the middle. Permissions debt is a consequence of people collaborating under time pressure over many years, not of anyone being careless.

The reason it matters now is simply that AI removes the obscurity that used to keep it harmless.

10. Where to start



If you take one thing from this guide, take the sequence: assess, contain, remediate, deploy, operate. In that order. The organisations that run into difficulty are almost always the ones that bought licences first.

What you can do this week, without us

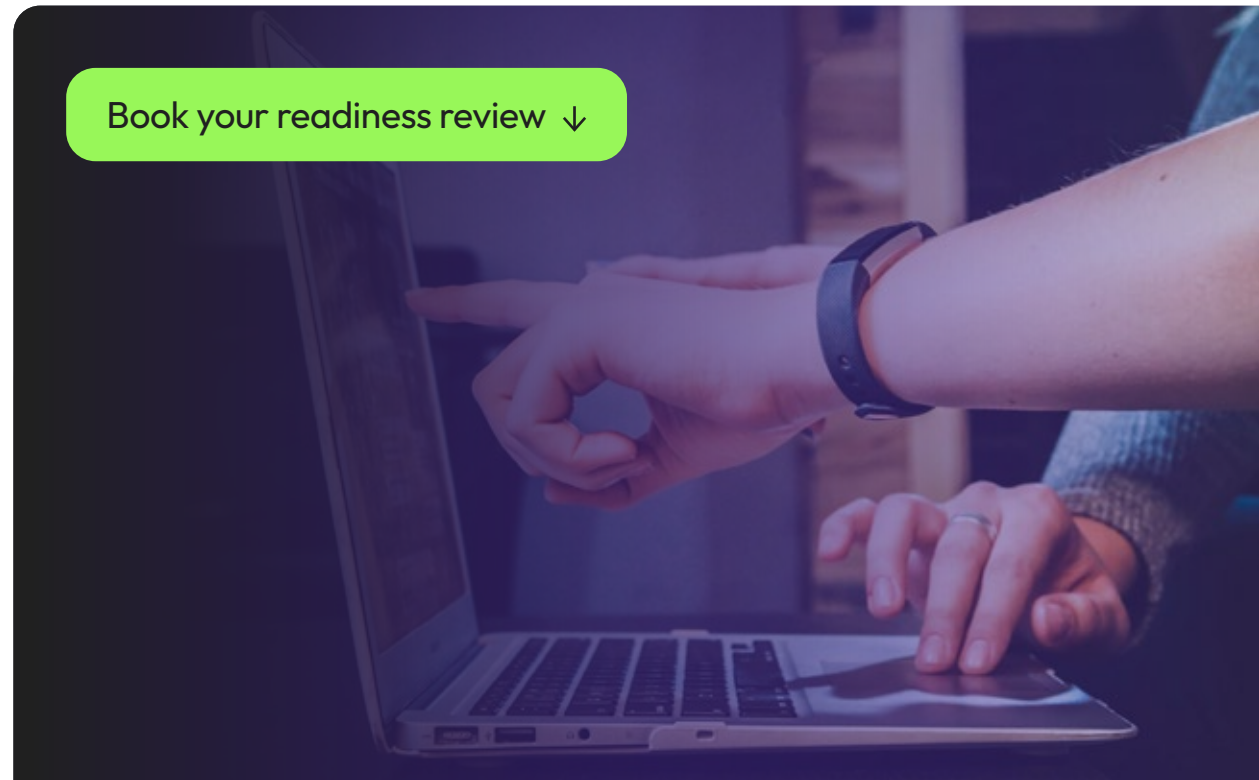
- Ask your IT provider for a report on how much of your content is shared with everyone in the organisation. If they cannot produce one, that is your answer.
- Ask which AI tools your staff are already using. Ask them directly, not through a survey.
- Complete the scorecard in section 9 with whoever knows your systems best.

The Cloudscape Copilot Readiness Review

We run a structured readiness assessment against all ten checks in this guide. It produces a written report covering what Copilot would currently be able to surface, a prioritised remediation plan, a costed licensing recommendation, and a realistic timeline.

It is designed to be useful whether or not you go on to deploy Copilot, and whether or not you work with us.

[Book your readiness review ↓](#)





Cloudscape has supported London businesses for over 25 years, working with growing SMEs and UK offices of international companies across financial services, legal, professional services and creative sectors. We are a Microsoft Solutions Partner, and we support mixed Windows and Apple Mac environments equally well.

Our Success Pathway: Secure. Protect. Thrive.

takes clients through operational security, protection from cyber threats, and the streamlined, responsive business that follows. Adopting AI safely sits squarely in the Thrive stage, and it only works if the first two are in place.

Secure. Protect. Thrive.
The Cloudscape Success Pathway

Book your **readiness review**



A straightforward conversation first — 30 minutes, no obligation. We will tell you honestly whether this is a priority for your business, and what we would expect to find.

Call 0207 952 8123 | Email info@cloudscape.it | Web cloudscapeit.co.uk