Microsoft 365 Copilot can make Teams meetings easier to catch up on: it can help summarise discussion, identify decisions and actions, and answer questions about what was said. That is useful when someone misses a meeting or needs to turn a conversation into follow-up work.

It also changes the stakes of everyday information management. Meeting content may include commercial plans, staff matters, customer details or information shared by a guest. Copilot can help people find and use information they already have permission to access; it does not make a badly governed tenant safe. If a file or meeting artefact is available too broadly, an AI assistant can make that exposure easier to discover.

Before buying or enabling Microsoft 365 Copilot Business, do a readiness assessment. Then tighten the foundations that determine what meeting participants and Copilot can access. Here is the order I recommend for organisations using a Microsoft 365 business plan.

Start with a readiness assessment, not a product demo

A short readiness assessment is more useful than a big demo when the basic controls have not been checked. Start with a small workshop involving the people who own IT, information security, privacy and business operations. The aim is to make decisions, not admire features.

Ask what people expect Copilot to do in Teams, what kinds of meetings are in scope, and which information must not be surfaced casually. Then check whether the tenant's identity, sharing and information-management settings support those expectations. Record the gaps, assign an owner and set a due date for each one. Who owns this, and by when?

Include these checks in the assessment:

- **Licensing and eligibility:** Confirm the Microsoft 365 business plan, user eligibility and Copilot add-on requirements against Microsoft's current guidance.
- **Identity security:** Check that multifactor authentication (MFA) is enforced, especially for administrators, and that privileged access is limited and reviewed.
- **Information access:** Identify broadly shared sites, Teams, mailboxes and files that users can reach today.
- **Meeting practice:** Agree how organisers will communicate recording, transcription and AI assistance, and how sensitive meetings should be handled.
- **Support and training:** Decide who handles user questions, access issues and incidents, and give staff practical instructions before rollout.

Make the assessment evidence-based. "We think sharing is under control" is not a finding. Check actual settings and sample actual content. Start with a pilot group whose information is reasonably well managed, rather than a group chosen solely because its members are keen to try new features.

Map where your data lives across Microsoft 365

Teams meetings do not sit in isolation. Meeting recordings, transcripts, chat, shared files and follow-up documents can live in different places across Microsoft 365, with different permissions and retention behaviours. Your first job is to understand that information journey.

Map the main locations used by your organisation, including Teams and SharePoint sites, OneDrive, Exchange Online, and any relevant Microsoft 365 groups. Note what kinds of information are stored in each, who can access them, how external sharing is configured, and whether retention or sensitivity controls apply. Check how meeting-related artefacts are stored in your environment rather than assuming every item follows the same path.

A useful map does not need to be a complicated architecture diagram. A table with the location, typical content, access model, external-sharing status, business owner and review date is often enough to expose the important gaps.

Location or content What to check Owner to involve Teams meeting chat and meeting artefacts Who can access the meeting, chat, recording or transcript; how sensitive meetings are identified Meeting organiser and Teams administrator Teams-connected SharePoint sites Site members, visitors, owners, sharing links and old project access Site owner and information owner OneDrive files shared in chats File owner, link type, expiry, recipients and ongoing need for access File owner and service desk Exchange and other Microsoft 365 locations Whether relevant content has appropriate access, retention and sensitivity controls Messaging or compliance owner

Use the map to identify where meeting notes might be copied after a call. A transcript may be discussed in Teams, summarised in a document, pasted into an email and stored on a project site. Each copy can have a different audience. Agree which location is the approved record and discourage uncontrolled duplication.

Fix permissions hygiene before you test Copilot

Permissions hygiene is one of the most important controls for Copilot readiness. Copilot works within a user's access, but that is only reassuring if the user's access is appropriate. If an employee can open an old project folder, a broad SharePoint site or a file shared with the whole organisation, they may be able to ask questions about that material.

Review access with least privilege in mind: people should have the access they need for their role, and no more. In practice, check:

- Teams and SharePoint sites with large, stale or unclear membership.
- Users who are owners of many sites or Teams without a current business reason.
- Broad groups such as "Everyone" or organisation-wide audiences that have access to sensitive content.
- Old projects, restructures and completed client work where membership was never removed.
- Files and folders with unique permissions that no one understands or owns.

Do not try to fix every permission in the tenant in one afternoon. Prioritise high-risk locations: executive and people teams, finance, legal, customer data, acquisition work and other sensitive projects. Give each location a named business owner who can confirm who still needs access. IT can implement the changes, but it cannot reliably decide whether a person still belongs on a confidential project.

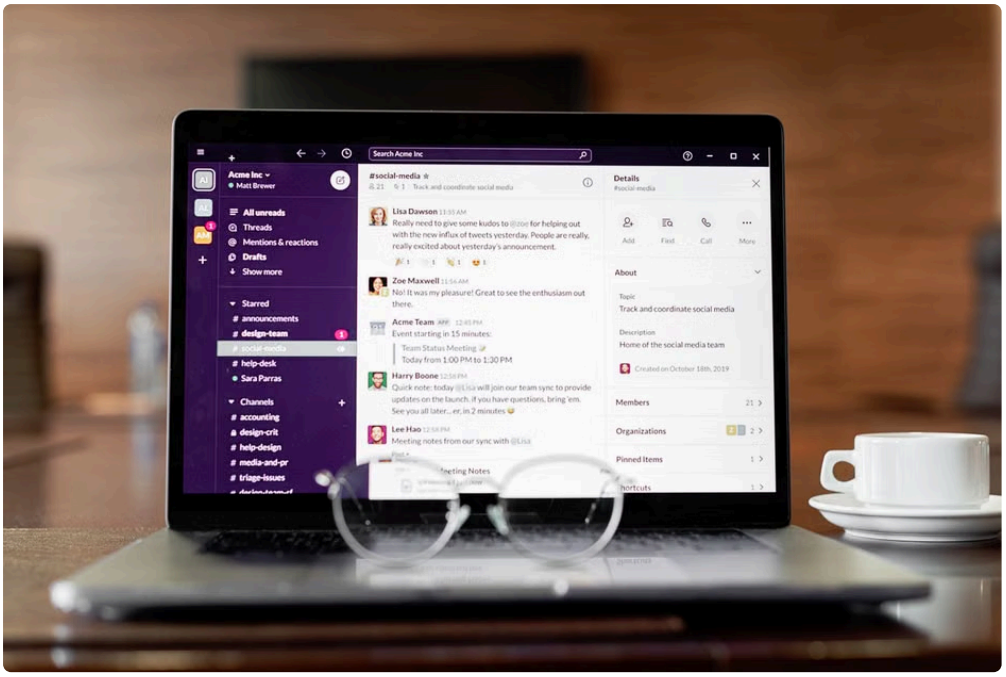
Avoid shared logins. They make it difficult to tell who accessed content, apply individual protections or remove access cleanly when someone changes roles. Also confirm that administrator accounts use MFA and are not used for ordinary email and meeting work.

Review shared links and guest access controls

Shared links and guest access are common sources of accidental exposure. A link that works for “anyone with the link” may be forwarded beyond its intended audience. A guest invited for one project may keep access long after the work is finished. Neither risk is solved by hiding a link or asking people not to forward it.

Review the external-sharing settings for SharePoint, OneDrive and Teams. The right balance depends on how your organisation works, but it should be deliberate. Consider limiting who can create broad links, preferring specific-recipient links for sensitive material, setting expiry where appropriate, and requiring authentication for external access. Check whether site-level settings are more permissive than your organisation intended.

For guest access controls, establish a simple lifecycle:



1. **Before inviting:** Confirm the guest’s identity, business purpose, sponsor and the Teams or site they need.
2. **When granting access:** Provide access only to the required location, not an entire collection of unrelated workspaces.
3. **At review:** Ask the sponsor to confirm that the guest still needs access on a set schedule.
4. **At project end:** Remove the guest and review any links or files that were shared with them.

Keep a checklist for SharePoint link expiry and guest access reviews. It should record the owner, review date, decision and any follow-up action. “Review guests regularly” is not a process unless someone is responsible for doing it and there is a date on the calendar.

Set expectations for meeting notes sensitivity

Meeting notes sensitivity deserves its own rules. A catch-up about a routine delivery issue is not the same as a meeting about a performance concern, a legal dispute or a customer’s confidential information. If staff cannot tell what is appropriate to record or share, they may either over-share or stop using useful features altogether.

Agree simple guidance with business and privacy stakeholders. Explain when recording or transcription is appropriate, copilot adoption metrics tracking how participants will be informed, who can access the

resulting artefacts, and where important notes should be stored. Remind organisers to check the invite list and meeting options, particularly when external participants are involved.

Provide a clear escalation path for unusual or highly sensitive meetings. Depending on the organisation's requirements, the right choice may be not to record or transcribe, or to restrict access to a defined group. Do not assume an AI summary is an official record, an accurate minute or a substitute for the organisation's approved record-keeping process. Participants should verify summaries and action items before relying on them.

Use a controlled pilot and measure the basics

Once the key access and sharing gaps are addressed, run a controlled pilot. Select a small group with a clear use case, a willing business owner and content that has been checked for inappropriate access. Give participants short, practical training: what Copilot can help with, how to handle sensitive meeting content, and how to report a result that appears to expose information unexpectedly.

Set a review date before the pilot starts. At that review, assess user feedback, support requests, meeting practices and any access or sharing concerns. Ask pilot users what saved time and what created confusion. Keep the scope small enough to learn quickly, and do not expand just because the licence has been purchased.

Netway can support Microsoft 365 readiness and rollout planning, while industry guidance and discussion from the Australian Information Industry Association (AIIA) can help organisations consider broader technology and policy issues. Whatever support you use, keep decisions grounded in your own data, risk appetite and operating model. An external adviser cannot name the business owner for your sensitive sites on your behalf.

Budget carefully and verify current pricing

Include licence costs in the business case, but do not treat the licence as the whole cost of adoption. Readiness work, access clean-up, staff guidance, support and ongoing reviews all take time. Confirm current eligibility and commercial terms with Microsoft or your licensing provider before you commit.

Item Example price Terms and notes Copilot Business add-on (Australia) AU$26.91 On offer until 31 December 2026; monthly billing costs more; prices change, so check the current figure.

This is an example, not a guaranteed quote. Check whether the price is per user and per month, what billing commitment applies, whether GST is included, and which Microsoft 365 business plan is required. Confirm the offer's conditions and end date at the time you order.



What to lock down first: a practical order

If you need a short action list, work through these steps in order:

1. **Name an accountable owner** for the readiness assessment and set a completion date.
2. **Map data locations** used for Teams meetings and follow-up work, including owners and access models.
3. **Review high-risk permissions** and remove access that is no longer needed.
4. **Check shared links and guest access**, including expiry, sponsors and review dates.
5. **Agree meeting notes sensitivity rules** and communicate them to organisers and participants.
6. **Run a limited pilot**, then review evidence before expanding.

Copilot in Teams meetings can be valuable, but readiness is not a toggle in the admin centre. The safer sequence is to understand where information lives, make access intentional, manage links and guests, and set clear expectations for meeting content. Then pilot the capability with accountable owners and a review date. Every action should have a name beside it—and a date by which it will be done.