Microsoft 365 Copilot can make Teams meetings easier to catch up on: attendees can ask questions about a meeting, find key points and follow up on actions. That convenience also makes the basics matter more. Copilot can only be as safe as the information it can access and the meeting settings, permissions and sharing habits around it.

For Australian organisations, the right starting point is not a tenant-wide switch-on or a polished demo. It is a https://itwire.com/guest-articles/guest-opinion/copilot-readiness-for-smes-fix-the-foundations-before-you-buy readiness assessment: understand what information is where, who can access it, how meetings are handled and what staff expect Copilot to do. Then run a small pilot, fix what it exposes and expand with clear ownership.



This guide focuses on the first controls to review for Microsoft 365 Copilot Business and Teams meetings. The aim is practical: reduce accidental exposure without blocking useful work. At each step, ask the question that often gets missed: **who owns this and by when?**

Start with a readiness assessment, not the purchase order

Before buying Microsoft 365 Copilot Business, check that the organisation is ready to use it responsibly. Licensing is only one part of the decision. You also need to know whether your Microsoft 365 environment is organised well enough for people and AI features to find the right information—and avoid information they should not see.

Begin with a short, cross-functional assessment involving IT, security, privacy, records management and business representatives. A focused workshop is usually more useful than a big product demo. Ask participants to map a few common workflows: a project meeting, a customer call and an internal leadership meeting. Identify which records are created, where they are stored and who should have access.

Readiness questions to answer

- Which users will be in the pilot, and what tasks are they expected to improve?
- Are Teams, SharePoint, OneDrive and Exchange being used with consistent ownership and access rules?

- Are there sensitive, regulated or commercially confidential topics that need special handling?
- Do meeting organisers understand transcription, recording, recap and participant notification settings?
- Can your support team explain what Copilot can access and where users should report an unexpected result?
- Who will review access, guest accounts and sharing links after the pilot starts?

Check licensing and plan eligibility against current Microsoft terms before committing. A Microsoft 365 business plan and the Microsoft 365 Copilot Business add-on are separate parts of the licensing picture; do not assume a business plan alone includes every Copilot capability. Confirm the intended users, prerequisites and available features with your Microsoft partner or Microsoft's current product information.

For budgeting, an example price is **Copilot Business add-on (Australia): AU26.91**, on offer until **31 December 2026**. Monthly billing costs more, and prices change, so check the current figure before you approve a quote. Record the price, billing term, eligible plan and review date in the purchase decision rather than relying on a screenshot or an old proposal.

Map where your data lives before inviting Copilot in

Teams meetings do not sit in isolation. Depending on your configuration and the feature being used, meeting-related information may include chat messages, recordings, transcripts, notes, files and calendar details. Other organisational information may sit across SharePoint sites, OneDrive accounts, Teams channels and Exchange mailboxes. Your readiness work should map the important information across these Microsoft 365 apps, not just inspect the Teams meeting itself.

Make a simple data-location map. For each information type, note the system or location, business owner, sensitivity, intended audience, retention requirements and the permissions that apply. Include content that is easy to overlook, such as old project sites, meeting recordings, shared channel content and documents stored in an individual's OneDrive but used by a team.

Information to map Where to check First question Meeting chat, transcript and recap Teams meeting settings and associated Microsoft 365 storage Who can access it, and how long should it be retained? Shared meeting documents SharePoint, Teams files and OneDrive Does access match the meeting's intended audience? Project and departmental information Teams-connected SharePoint sites and standalone sites Are old members, guests or broad groups still included? Personal or business communications OneDrive and Exchange Is ownership clear if the staff member changes role or leaves?

Copilot does not make a poorly organised information estate safe by itself. If a user already has permission to a document, that permission may affect what they can discover through Microsoft 365 experiences. The practical control is to correct access at the source, not to hope that content is obscure or hard to find.

Fix permissions hygiene and least privilege

Permissions hygiene is one of the highest-value controls to address before a pilot. Review access to the sites, Teams, folders and files your pilot users work with. Look for broad groups, inherited permissions that no longer make sense, former staff, stale guests and documents shared far beyond their intended audience.

Apply least privilege: give people the access they need for their role, for only as long as they need it. That does not mean adding friction to every collaboration task. It means making ownership and membership intentional, and reviewing them when a project ends or a person changes role.

Prioritise these permission checks

- Identify Teams and SharePoint sites with no active business owner.
- Review broad access groups and confirm they are still appropriate.
- Check whether sensitive libraries or folders have unique permissions that are understood and documented.
- Remove access for leavers and people who no longer need it.
- Replace shared logins with named accounts and appropriate role-based access.
- Confirm administrator accounts have multifactor authentication and are not used for routine work.

Do not treat a channel as a filing cabinet. Teams channels are useful for collaboration, but files and records need an information structure, an owner and a lifecycle. If a team has accumulated years of material with names such as “final_v7”, first decide what is current, what should be retained and what can be archived or deleted under your records rules. Copilot can make information easier to surface; untidy content can make that a problem rather than a benefit.

Assign an owner and due date to each remediation item. For example: “Project site owner to review all members and guests by 15 September.” That is actionable. “Clean up permissions” is not.

Review shared links and guest access controls

Shared links and guest access controls deserve their own review. A document may be well protected inside a Team but exposed through a link created months ago. Likewise, a guest may still be able to access a project site after their work has finished. Neither risk is solved by keeping the link difficult to guess. Obscurity is not security.

Inventory external sharing settings and identify how links are created across SharePoint and OneDrive. Check whether anonymous or “anyone” links are allowed, who can create them, whether expiry is enforced and whether recipients can edit or only view. Set defaults that suit the organisation’s risk, then provide a safe, approved way to share externally when there is a genuine business need.

Guest access review checklist

- List guest users and identify their sponsor or internal contact.
- Confirm each guest has a current business purpose and access only to the required resources.
- Set a review date or expiry process for guest access, rather than leaving accounts indefinitely.
- Review sharing links for sensitive or high-value sites and files, including old links.
- Confirm external sharing settings align with your privacy, contractual and information-security requirements.
- Tell project owners how to request, approve and remove guest access.

Keep a recurring checklist for link expiry and guest access reviews. A quarterly review can be a reasonable starting point for many small organisations, but higher-risk projects may need more frequent checks. Choose a cadence based on your information and obligations, then record who performs the review and how exceptions are handled.

Set expectations for meeting notes sensitivity

Meeting notes sensitivity is not just a technical setting. People need to understand that a transcript, recording, recap or AI-generated summary may contain personal information, commercially sensitive material or candid discussion. Agree what kinds of meetings should be recorded or transcribed, who decides, how participants are informed and where resulting content should be stored.

Before the pilot, define a simple meeting classification approach. For example, routine internal project meetings may be suitable for a transcript when participants are informed and the content is appropriate. Sensitive HR, legal, health or confidential customer discussions may require stricter handling or may be excluded from the pilot. Confirm the approach with your privacy and records specialists, especially where industry or contractual requirements apply.

Make clear that Copilot-generated content needs human checking. A summary can omit nuance or misstate an action. Meeting owners should verify important decisions, owners and dates before treating notes as an official record. Do not let generated notes silently become the source of truth for commitments or compliance evidence.

Run a controlled Teams pilot

Once the highest-risk access issues are addressed, start with a small group of users and a defined set of use cases. Choose people who can give useful feedback and are willing to follow the meeting rules. Include a mix of meeting types, but avoid starting with the most sensitive conversations.

1. **Choose the pilot scope:** name the users, Teams and meeting scenarios included.
2. **Set guardrails:** document what can be transcribed, how participants are notified and where outputs belong.
3. **Check access:** test that pilot users can reach only the sites and files intended for their roles.
4. **Train in short sessions:** show users how to use Copilot appropriately, verify outputs and report a concern.
5. **Review results:** collect feedback, check access issues and decide what must be fixed before expansion.

Use the pilot to test real behaviour, not just feature availability. Can a meeting organiser explain the settings? Do participants know when a transcript is being created? Are summaries being saved in an appropriate place? Does a user encounter information they did not expect to see? Any surprising access result should be investigated and permissions corrected before broadening the rollout.

Make ownership visible

Microsoft provides the platform, but your organisation sets the rules for its information and collaboration. Australian organisations may also draw on guidance and industry discussion from groups such as the Australian Information Industry Association (AIIA). A Microsoft partner such as Netway can help with licensing, configuration or a readiness review, but internal owners still need to approve the business rules and maintain them.

Put names and dates against the work. A basic register might include the control, accountable owner, action, due date, evidence and next review date. Keep it short enough that someone will actually maintain it.

Control Suggested owner Evidence to retain Data-location map Information or site owners Locations, classifications, owners and access notes Teams permissions review IT with business owners Membership

decisions and remediation dates Guest and link review Site owners or security Guest sponsor, purpose, expiry and link action Meeting guidance Privacy, records and business leads Approved rules, user guidance and review date

What to lock down first

In order, assess readiness and licensing, map data across Microsoft 365, fix permissions, review shared links and guests, then set clear rules for meeting notes sensitivity. After that, run a small Teams pilot and review what users actually do.

Copilot in Teams can save time, but it is not a substitute for clear ownership or sound access controls. Tidy the information estate first, make the meeting rules easy to follow and expand only when the pilot shows the basics are working. For every open item, finish with the question that turns advice into action: **who owns this and by when?**

