A Microsoft 365 Copilot pilot can make useful work easier to find and summarise. It can also make existing access problems more visible. If a staff member can already open an old SharePoint file, a Teams conversation or a document shared too broadly, Copilot may be able to use that content when responding to them.

That does not mean Copilot gives users new permissions. It works with the access a user already has. The practical risk is that people may not know they have access to a document, or may not realise how widely it has been shared. That is why a **teams guest access** review belongs in readiness work before you buy licences or invite a pilot group.

This guide https://itwire.com/guest-articles/guest-opinion/copilot-readiness-for-smes-fix-the-foundations-before-you-buy is for Australian organisations preparing to assess Microsoft 365 Copilot Business. It covers data location, permissions, shared links and **external users microsoft 365** administrators should account for. The aim is a usable governance checklist, not a big demo and a vague promise to "tidy things up later".

Start with readiness, not the licence order

Before purchasing, check whether your tenant, people and information are ready for a controlled pilot. Copilot is not a substitute for records management, access reviews or clear ownership. If your SharePoint sites are full of "final_v7" documents and Teams channels are being used as filing cabinets, fix the most important issues first.

Microsoft 365 Copilot Business is an add-on, and your underlying Microsoft 365 business plan matters. Confirm current eligibility and requirements with Microsoft or your provider before you commit. A pricing example supplied for Australia is:

Item Example price Terms and notes Copilot Business add-on (Australia) AU26.91 On offer until 31 December 2026. Monthly billing costs more; prices change, so check the current figure.

Confirm whether a quoted price is per user, what billing term applies, and whether GST or other charges affect the amount. Treat the figure above as an example to verify, not a standing price promise.

Set a pilot boundary

A small pilot gives you a chance to check real workflows without enabling the whole organisation at once. Pick a group with a clear business purpose, a manager who will support participation, and information that is suitable for testing. Avoid starting with users whose access is difficult to understand or who work extensively with sensitive material.

Write down what the pilot is meant to prove: for example, whether staff can find approved procedures faster, or whether meeting summaries reduce follow-up work. Define what is out of scope, who can approve expansion, and what would cause you to pause. A short workshop with users and site owners will usually reveal more than a large product demonstration.

Map where the information lives

Copilot's usefulness depends on the information a user can access across Microsoft 365. Before the pilot, map the important locations and identify who owns them. Do not assume that all business content lives in Teams or that a Teams guest list tells you who can reach every file.

Include the main places where staff create, store and share information:

- **SharePoint:** team sites, communication sites, document libraries, sharing settings and site owners.
- **OneDrive:** business files, shared folders, old project material and links created by individuals.
- **Teams:** standard, private and shared channels, their associated files, meeting content and guest membership.
- **Exchange and Microsoft 365 groups:** mail, calendars, group membership and connected resources relevant to the pilot.
- **Other connected services:** any additional data sources your organisation has connected or plans to use.

Record the location, business purpose, owner, sensitivity and intended audience for each in-scope area. Note where information is stored and where users or guests are allowed to access it. If you have data residency or regulatory requirements, validate the relevant Microsoft service commitments and your tenant configuration directly. Do not infer data location from a user's office address or from a Teams team name.

For Australian organisations, a data map is also a useful conversation starter with privacy, legal and security stakeholders. The Australian Information Industry Association (AIIA) provides a broader industry context for discussions about responsible technology adoption, but your own obligations and risk assessment should guide your decisions.

Review Teams guest access and external sharing

"Guest access" is often used as shorthand for several different ways an external person can work with your organisation. A guest in a Team is not the same thing as every possible external sharing link. SharePoint and OneDrive can share files with people outside your organisation, while Teams settings govern who can participate in teams and meetings. Review the paths separately.

Check who the guests are and why they still need access

Export or review guest accounts and Team membership. Look for people whose organisation or project has changed, accounts with no clear sponsor, and guests who have not been used for a long time. For each active guest, confirm a business reason, an internal owner and an expiry or review date. Remove access when it is no longer needed.

Also check whether the guest can access more than the specific project requires. A guest added to a Team may have access to its shared resources; membership should not be treated as a casual way to give someone one document. If they only need a particular file, use the narrowest approved sharing method.

Inspect sharing links, not just the guest list

Review SharePoint and OneDrive sharing policies and a sample of actual links. Pay particular attention to "Anyone" links, links that allow editing, links without an expiry date, and links created by former staff. An anyone link can be used by someone who obtains it; obscurity is not security. Prefer links for named people where appropriate, set expiry dates, and limit editing to people who genuinely need it.





Check whether site owners understand the link settings they use and whether default link types align with your policy. A tenant-wide setting may permit a sharing option that individual sites should not use. Where business needs justify broader sharing, document the exception, owner and review date.

Permissions hygiene: least privilege in practice

Copilot can surface information that is technically available to a user but practically forgotten. Before the pilot, check whether access groups reflect current roles and whether sensitive sites have clear boundaries. Review direct permissions, nested groups and broad groups such as “Everyone except external users”. Watch for inherited permissions that make a site or library more open than its owners expect.

Prioritise these checks:

- Remove access for departed staff, old project members and guests without a current sponsor.
- Replace ad hoc individual permissions with managed groups where that is practical.
- Check that sensitive libraries are not broadly available through a parent site or group.

- Confirm that private and shared Teams channels have the right membership and named owners.
- Review admin roles separately; use named administrator accounts, least privilege and MFA.
- Check whether employees can create teams and sites without an owner or review process.

Do not use a Copilot pilot as the first time anyone looks at permissions. Start with the content most likely to appear in pilot users' work: operational procedures, customer or supplier material, HR content, finance documents and project sites. If a site owner cannot explain who should have access, pause and resolve that before including it.

Build a practical governance checklist

Use this checklist to turn the review into tasks someone can complete. Each item needs a named owner and a due date. "IT to tidy access" is not an action plan.

Review area Check Evidence or outcome Owner and due date Pilot scope Define users, use cases, exclusions and success measures. Approved pilot brief and user list. Business sponsor: name and date. Data map Identify in-scope SharePoint, OneDrive, Teams and other relevant locations. Location, sensitivity, owner and audience recorded. Information owners: names and dates. Guest accounts Confirm each guest has a current purpose and internal sponsor. Access retained, reduced or removed; review date set. Team or site owner: name and date. Sharing links Review broad, editable and non-expiring links. Risky links removed, replaced or documented as exceptions. Site owner: name and date. Permissions Check group membership, inheritance and sensitive areas. Least-privilege changes completed and tested. IT and information owner: names and dates. Operations Agree how access reviews, expiry and incidents will be handled. Repeatable review schedule and escalation path. Service owner: name and date.

Run the pilot with clear guardrails

Tell pilot users what Copilot can and cannot do, which work scenarios are in scope, and how to report a result that looks wrong or exposes unexpected content. Ask them to verify important outputs against the source material. Copilot-generated text can be incomplete or mistaken; it should not become an unreviewed decision or official record simply because it is convenient.

During the pilot, review feedback and access issues at a regular, short check-in. If someone sees material they should not have been able to access, treat it as a permissions issue: record the source, restrict access where needed, and investigate how the permission was granted. Do not assume that changing a Copilot setting will correct an underlying SharePoint or Teams access problem.

Netway can be part of the conversation if you need help planning a Microsoft 365 readiness assessment or reviewing your configuration. Whether you use a partner or handle the work internally, agree the deliverables in advance: which locations are assessed, how findings are prioritised, who approves changes and how completion is verified.

Decide whether you are ready to proceed

A pilot is in a better position to proceed when its users and use cases are defined, key data locations have owners, guest access has been reviewed, risky links are addressed, and permissions for sensitive content have been tested. You do not need a perfect tenant, but you do need to know what remains open, who accepts the risk and when it will be reviewed.

Before adding licences, ask the question that keeps the work moving: **who owns this and by when?** Put the answer beside each governance action, then review progress before expanding the pilot. That is a far more useful starting point than buying first and hoping the tenant sorts itself out.