If your organisation has fewer than 300 users, Microsoft 365 Copilot Business may look like a straightforward add-on purchase. The catch is the phrase *eligible plan*. It does not mean every Microsoft 365 subscription qualifies, nor does it mean your tenant is ready to get useful results safely.

For Australian small and mid-sized organisations, it helps to separate three questions: Do you meet Microsoft's licensing conditions? Is your Microsoft 365 environment prepared? And can you confirm the current price and commercial terms before ordering?

This guide explains what "eligible plan" means in practical terms, what to check before buying the Copilot add-on licensing, and how to reduce the risk of Copilot surfacing information to the wrong people. The key principle is simple: Copilot works with information people can access. If permissions and sharing are untidy, an AI assistant can make that untidiness easier to discover.

What "eligible plan" means

Microsoft 365 Copilot Business is designed for eligible Microsoft 365 business customers, generally organisations with up to 300 users. To use it, a person needs a qualifying base subscription as well as the Copilot Business licence. The base subscription provides the Microsoft 365 services and user identity that Copilot builds on; the add-on enables Copilot features for that user.

Microsoft's eligible base-plan list and commercial terms can change. So don't rely on an old quote, a third-party comparison table or the fact that a user can sign in to Microsoft 365. Check the current Microsoft documentation and the terms shown for your tenant, region and buying channel. If you purchase through a partner such as Netway, ask them to confirm the exact qualifying plan and any minimum, commitment or billing conditions in writing.

In other words, "eligible" is a licensing condition, not a general description of your tenant. An organisation can be under 300 users and still need to check whether its specific Microsoft 365 business plan qualifies. A qualifying base plan also does not automatically include Copilot: the Copilot Business licence is a separate purchase unless the offer or agreement explicitly says otherwise.

Check the user count and the individual licence

Confirm which users are in scope, how Microsoft counts the organisation's eligible users, and whether each person assigned Copilot has the required base licence. Avoid assuming that a licence assigned to one person covers a shared mailbox, a generic account or another colleague. Shared logins are poor practice for security and accountability, and they make licensing and access reviews harder.

For a clear purchase decision, get written answers to these questions:

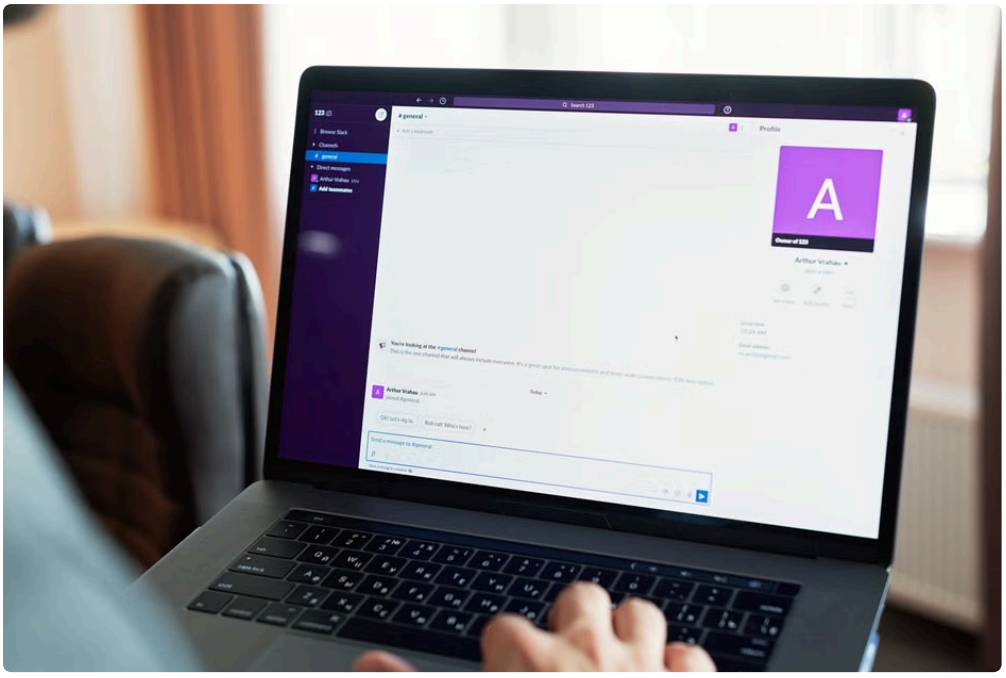
- Does our exact base subscription qualify for Microsoft 365 Copilot Business today?
- Does the under-300-user condition apply to our organisation as configured and contracted?
- Which users will receive the Copilot Business add-on, and do they each have a qualifying base licence?
- What are the billing frequency, commitment period, renewal terms and cancellation conditions?
- Is the quoted price promotional, and when does the offer end?

Price example: confirm the offer and billing terms

For budgeting, an Australian price example is:

Item 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.

Treat that as an example, not a guaranteed quote. Confirm whether the displayed amount is per user, per month, inclusive or exclusive of GST, and tied to annual commitment or another billing arrangement. Ask for the total cost for the number of users you plan to license, including any price changes at renewal. Microsoft and reseller pricing can change, so check the current figure before approval.



Eligibility is not readiness

Having an eligible Microsoft 365 business plan answers a licensing question. It does not answer whether your data is well organised, whether users have appropriate access, or whether the business has a sensible rollout plan.



Copilot can help users find, summarise and work with content they are permitted to access. That makes existing permissions especially important. If someone has access to an old project folder, a broad SharePoint site or a file shared with “anyone” links, Copilot may make that content easier to locate. It does not replace access controls or fix poor information management automatically.

Before ordering at scale, run a short readiness assessment. This is not a reason to delay indefinitely. It is a way to identify what is safe to pilot, what needs remediation, and who owns each action. A focused workshop with IT, information owners and a few representative users is usually more useful than a large feature demo.

Readiness assessment: what to check before purchase

1. Map where business data lives

Start with a practical itwire.com data location map across Microsoft 365 apps. Identify where the organisation stores working documents, formal records and sensitive information, including:

- SharePoint sites and document libraries
- OneDrive accounts, especially files shared outside the organisation
- Teams channels and the SharePoint sites behind them
- Exchange Online mailboxes and calendars
- Microsoft 365 groups and other collaboration spaces

For each location, note the business owner, the kinds of information held, the people or groups with access, and any external sharing. Don’t treat Teams as a filing cabinet: a channel may point to a SharePoint library, but that does not make it a well-governed records location. Likewise, “it’s in OneDrive” is not a data classification or retention plan.

Use the map to spot high-risk or confusing locations before a pilot. These might include former project sites, broad “all staff” libraries, folders with sensitive HR or finance material, and content whose owner has left the organisation. You do not need a perfect inventory to begin; you do need to know where the important and risky content is.

2. Review permissions and apply least privilege

Check whether access is limited to people who need it for their role. Pay particular attention to nested groups, inherited permissions, broad access groups, old project membership and files shared directly with individuals. Remove access that no longer has a business reason, and document any exceptions.

Least privilege means giving users the minimum access they need, for the period they need it. It is easier to apply consistently when access is granted through well-owned groups rather than a collection of one-off permissions. Confirm that someone is responsible for reviewing memberships and that changes are recorded.

Also review administrator accounts. Admin access should be limited, protected with multifactor authentication (MFA), and used deliberately. No MFA on admin accounts is an avoidable risk, whether or not you are deploying Copilot. Copilot readiness is a good prompt to improve the basics rather than an excuse to skip them.

3. Check shared links and guest access

External sharing deserves its own review. Look for “anyone” links, links that remain active longer than needed, guest accounts with no current sponsor, and collaboration spaces where nobody can explain who the guests are or why they are there.

Set sharing controls that fit the organisation’s needs, and agree how link expiry and guest access will be reviewed. Keep a checklist: who owns each guest relationship, when was it last reviewed, and when should the link expire? If external collaboration is business-critical, manage it with clear ownership and expiry rather than disabling it blindly.

Obscurity is not security. Hiding a site name or assuming nobody will find a link does not make over-broad access safe. The control is the permission itself, plus a reliable process to review it.

4. Confirm identity, security and governance basics

Before a pilot, check that user accounts are individual, MFA is enabled in line with your security policy, and leavers’ access is removed promptly. Confirm that your organisation understands its retention, sensitivity and records-management requirements. Copilot does not replace those policies, and a licence should not be treated as a shortcut around them.

Decide how users can report an unexpected result or a suspected permission issue. Make sure someone can investigate it, adjust access and communicate the outcome. These are operational requirements, not just project paperwork.

A sensible rollout for an organisation under 300 users

A pilot can validate both usefulness and readiness without assigning licences to everyone at once. Choose a small group with varied roles and realistic tasks. Include people who work with shared documents, not only IT staff who already know where everything lives.

1. **Confirm the licence.** Verify the eligible Microsoft 365 business plan, user count and current Copilot Business terms with Microsoft or your reseller.
2. **Choose a bounded pilot.** Set a clear user group, a duration and a few work scenarios, such as preparing a meeting summary or finding approved project information.
3. **Remediate priority access issues.** Review the sites, groups, shared links and guest accounts that pilot users can reach.
4. **Brief the users.** Explain what Copilot can access, how to handle sensitive information, and how to report content that appears to be incorrectly accessible.
5. **Measure the result.** Record useful outcomes, user feedback, support requests and any permissions or data-quality issues discovered.
6. **Make an expansion decision.** Fix the blockers, agree ongoing governance, and only then decide whether to assign more licences.

For each action, name an owner and a due date. “Review SharePoint” is not an action plan. “Priya to review guest access on the Finance site and remove or renew unowned guests by 15 May” is. Who owns this and by when?

Questions to ask your Microsoft partner

Whether you work directly with Microsoft or through a partner such as Netway, ask for a practical licensing and readiness discussion. In Australia, the Australian Information Industry Association (AIIA) is another useful point of reference for broader industry perspectives, but your organisation still needs to confirm its own Microsoft licensing and security position.

- Which exact base plans are eligible for Microsoft 365 Copilot Business under the current terms?
- Can you show the current Australian price, billing options and the offer end date?
- What changes if we bill monthly rather than choose another available commitment?
- Can you help us scope a short readiness workshop and a bounded pilot?
- What work is included in the quote, and what remains our responsibility?

The practical answer

For an organisation under 300 users, “eligible plan” means your Microsoft 365 business plan must meet Microsoft’s current licensing conditions before you add Microsoft 365 Copilot Business for each intended user. It is a specific product and contractual check, not a blanket promise that every business subscription qualifies.

Then comes the readiness check: map data across Microsoft 365 apps, tighten permissions using least privilege, review shared links and guest access, and confirm security and ownership basics. A small, well-scoped pilot can reveal whether Copilot is useful and whether your information environment is ready to support it safely.

Verify the current price and terms before purchase, assign an owner and date to each remediation task, and expand only when the results and controls justify it. That is a much better foundation than buying licences first and hoping the tenant is tidy.