Microsoft Teams

Governance Checklist

Pre-Copilot Readiness Assessment · 2026

Most businesses have been running Microsoft Teams since 2020 without formal governance rules. That was fine — until Copilot. Once Copilot is enabled, it searches everything your users can access. Without tidy governance, that becomes a data risk.

Work through each section below. Tick what's already in place and note anything that needs attention. If you'd like help working through any of it, we're here.

1 Team Creation Controls

- ☐ Only designated users or IT admins can create new Teams — not everyone by default
  Without this control, Teams sprawl is almost inevitable. Every new Team creates a SharePoint site and mailbox behind it.
- ☐ A clear process exists for requesting a new Team
- ☐ Templates are used so new Teams are set up consistently from day one

2 Naming Conventions

- ☐ All Teams follow a consistent naming pattern — for example, DEPT–Client–Project–Year
  Consistent names mean Copilot results make sense. Users can tell internal from client from HR content at a glance.
- ☐ Channels within Teams are named clearly and consistently
- ☐ SharePoint sites linked to Teams follow the same naming convention

3 Team Ownership

- ☐ Every Team has at least two owners assigned

A single owner who leaves makes a Team ownerless — no one can manage membership, review guests, or clean it up.

- ☐ Owners understand they are responsible for managing membership and guest access
- ☐ A process exists to reassign ownership when staff change roles or leave

4 Guest & External Access

- ☐ You have a clear policy on when external guests can be invited to Teams
- ☐ Guest access settings are configured deliberately — not left at Microsoft's defaults
- ☐ Guest accounts are reviewed at least every 180 days
- ☐ Former suppliers and partners no longer have active guest access
  Guest access from old projects is one of the most common governance gaps — and one of the riskiest once Copilot is live.
- ☐ Approval is required before guests are added to Teams containing sensitive content

5 Lifecycle & Inactive Teams

- ☐ Inactive Teams are identified and reviewed regularly (every 90–180 days)
- ☐ A process exists to archive or delete Teams when projects end
- ☐ Expiration policies are configured to notify owners before a Team expires
- ☐ Ownerless or abandoned Teams have been identified and actioned

6 SharePoint Permissions

- ☐ You know which SharePoint sites contain sensitive data — HR, finance, legal
- ☐ Sensitive sites are not shared with "Everyone" or broad company-wide groups
  40–60% of SharePoint sites have at least one oversharing pattern — often set up years ago and forgotten.

- ☐ External sharing on sensitive SharePoint sites has been reviewed
- ☐ Anonymous sharing links have been audited and removed where not needed
- ☐ Permissions follow the principle of least privilege — people can only see what they need

7 Data Classification & Retention

- ☐ Sensitivity labels are applied to Teams containing confidential or restricted content
  Sensitivity labels are how Copilot knows what it should and shouldn't surface. Without them, Copilot treats all content as equally accessible.
- ☐ Staff know which Teams should never be shared with external guests
- ☐ Retention policies are configured for Teams chat and channel messages
- ☐ Retention settings align with your legal and regulatory obligations

8 Third-Party App Governance

- ☐ Only IT-approved apps can be installed in Teams
- ☐ App permissions across Teams have been reviewed in the last 12 months
- ☐ Unused or unauthorised apps have been removed

The 5 Copilot Readiness Checks

Copilot searches everything your users can access. Before you turn it on, confirm all five are in place.

- ☐ Every Team has at least two owners
- ☐ Guest access has been reviewed in the last 180 days
- ☐ All Teams follow a consistent naming convention
- ☐ Inactive Teams have been archived or deleted
- ☐ People can only see what they need — least privilege is applied throughout

Need help with any of this?

Our Copilot Security Review covers all of the above — we audit your Microsoft 365 environment, identify governance gaps, and give you a plain-English remediation plan. For clients who want ongoing governance after going live, our AI Security Pack (which includes Microsoft Purview and AvePoint workspace management) keeps things clean automatically.

Book a free review: wedoyour.it | 0117 911 8808 | support@wedoyour.it