TELORIC · AI READINESS

Copilot Guardrails Checklist

Microsoft 365 Copilot — Executive Readiness and Pre-Pilot Diagnostic

EXECUTIVE READINESS SUMMARY

The core risk. Microsoft 365 Copilot doesn't create new access — it inherits what already exists. Point it at a tenant with over-permissive sharing, loose folder access, or unlabeled sensitive files, and it can surface that content to any employee who asks. The exposure isn't created by Copilot; it's revealed by it. Readiness is less about the tool and more about the state of the data underneath it.

The Teloric view. Copilot's value and Copilot's risk come from the same place: the data it can reach. We treat readiness as a governance decision first and a technical project second — aligning permissions, classification, oversight, and training before broad rollout, so adoption accelerates instead of stalling on an avoidable incident.

1 Governance and Accountability

Focus: The policy layer — who decides, and who answers for it.

- **Set the use policy.** Decide what data may and may not be entered into Copilot (e.g., no unencrypted client financials, no HR records), and the limits on generative output.
- **Name an owner.** Assign one accountable leader for Copilot policy, permissions oversight, and change approval — not a standing committee.
- **Define escalation.** Agree in advance how data-exposure incidents are reported, contained, and resolved.

WHY IT MATTERS

Clear ownership converts diffuse liability into a defined chain of accountability, and replaces employee guesswork with a usable playbook.

2 Data Security and Access

Focus: The technical layer that determines what Copilot can actually reach.

- **Tighten sharing.** Audit and remove over-permissive “everyone” and organization-wide links on sensitive sites and folders.
- **Classify and label.** Use Microsoft Purview sensitivity labels and DLP so Copilot respects classification and excludes protected content from its responses.
- **Map identity to role.** Confirm access groups are scoped so people inherit only what their role requires.

WHY IT MATTERS

This is the control that contains exposure. Resolving permission sprawl protects intellectual property and personnel data from internal over-disclosure — the most likely and least visible failure mode.

3 Adoption and Oversight

Focus: The layer that protects ROI and keeps the posture current.

- **Build user judgment.** Require practical guidance on safe prompting, data-handling limits, and verifying output before it's trusted or sent.
- **Govern integrations.** Review any third-party plugin or connector for data handling and security before it touches Copilot.
- **Review on a cycle.** Reassess usage, access, and accuracy quarterly, and adjust as Microsoft ships new capabilities.

WHY IT MATTERS

Capable users and reviewed integrations turn license spend into measurable productivity, while a standing review cycle keeps controls aligned to a tool that changes often.

NEXT STEP FOR LEADERSHIP

Settle the governance decisions in Area 1, then authorize IT to begin the access and labeling work in Area 2. The diagnostic that follows makes each step checkable and assigns an owner.

TELORIC · AI READINESS

Pre-Pilot Diagnostic

This pre-pilot diagnostic is Teloric's standard starting point for governed Microsoft 365 Copilot adoption. Because Copilot inherits the access your people already have, the safest path to value is to confirm your governance, permissions, and oversight before expanding beyond a small pilot. It is designed to be completed jointly by business and IT leadership and worked through together in our first session, not filed away. Once finished, the completed checklist becomes part of your governance record — a documented, defensible baseline of the decisions made and the gaps still open before broader rollout.

HOW TO USE THIS DOCUMENT

- Complete it together — a business lead and IT, side by side.
- Mark each item In place, Needs work, or N/A.
- Use the notes line to capture decisions, owners, and target dates.
- Bring it to session one; we will work from it directly.

COMPANY

COMPLETED BY

EMAIL

ROLE (IT / BUSINESS LEAD)

DATE

OWNER KEY

IT technical configuration

BUSINESS policy and use decisions

SHARED decide together

WHAT HAPPENS NEXT

In our first Teloric session we review your completed checklist together, confirm the high-risk gaps, and align business and IT on the decisions those gaps require. From there we prioritize the first governance actions to take before expanding your pilot — so rollout moves forward on a foundation that has been reviewed, owned, and documented.

01 Governance and Policy

Set the rules and name a human owner before turning Copilot on.

Document an AI use policy covering acceptable use, prohibited use, and escalation. BUSINESS

☐ In place ☐ Needs work ☐ N/A

NOTES

Name one accountable owner for Copilot configuration, oversight, and review. SHARED

☐ In place ☐ Needs work ☐ N/A

NOTES

Define what employees may and may not enter into Copilot. BUSINESS

☐ In place ☐ Needs work ☐ N/A

NOTES

Document high-risk use cases (HR, legal, financial, customer-facing) and require extra approval. BUSINESS

☐ In place ☐ Needs work ☐ N/A

NOTES

Agree a change-management routine for new features and new users. SHARED

☐ In place ☐ Needs work ☐ N/A

NOTES

Decide which workflows are in and out of scope for the pilot. SHARED

☐ In place ☐ Needs work ☐ N/A

NOTES

02 Identity, Permissions and Access

Copilot inherits each user's access — tightening it is the core guardrail.

Enforce MFA and Conditional Access for every Copilot identity. IT

☐ In place ☐ Needs work ☐ N/A

NOTES

Apply least-privilege access across Teams, SharePoint, OneDrive, and repositories. IT

☐ In place ☐ Needs work ☐ N/A

NOTES

Disable legacy authentication and require device compliance. IT

☐ In place ☐ Needs work ☐ N/A

NOTES

Audit access on sensitive locations (financial, HR, incident records). IT

☐ In place ☐ Needs work ☐ N/A

NOTES

Separate administrative accounts from everyday accounts. IT

☐ In place ☐ Needs work ☐ N/A

NOTES

Remediate over-permissive sharing — company-wide groups, “Anyone” links, oversized audiences. IT

☐ In place ☐ Needs work ☐ N/A

NOTES

Confirm source-of-truth data lives in governed SharePoint sites with Owners / Members / Visitors mapped to roles. SHARED

☐ In place ☐ Needs work ☐ N/A

NOTES

03 Data Protection, Safety and Oversight

Protect sensitive data, keep output trustworthy, and watch for misuse.

Classify and label data with Purview so Copilot respects sensitivity. IT

☐ In place ☐ Needs work ☐ N/A

NOTES

Configure DLP for Copilot to exclude protected content from grounding and output. IT

☐ In place ☐ Needs work ☐ N/A

NOTES

Restrict Copilot from highly regulated data (PHI, PII, financial; HIPAA, PCI, legal-hold). SHARED

☐ In place ☐ Needs work ☐ N/A

NOTES

Align retention and lifecycle policies so Copilot-assisted content stays compliant. IT

☐ In place ☐ Needs work ☐ N/A

NOTES

Require human review before any Copilot-drafted external, legal, or financial communication. BUSINESS

☐ In place ☐ Needs work ☐ N/A

NOTES

Enable Copilot usage logging and monitor for unusual prompt behavior. IT

☐ In place ☐ Needs work ☐ N/A

NOTES

Keep a short AI incident-response plan for exposure, harmful output, and misuse. SHARED

☐ In place ☐ Needs work ☐ N/A

NOTES

04 Review, Enablement and Oversight

Keep guardrails current and reviewed as Copilot evolves.

Train staff on safe prompting and verifying output. BUSINESS

☐ In place ☐ Needs work ☐ N/A

NOTES

Add responsible-use guidance to onboarding for all roles. BUSINESS

☐ In place ☐ Needs work ☐ N/A

NOTES

Review third-party plugins and connectors before enabling. IT

☐ In place ☐ Needs work ☐ N/A

NOTES

Confirm tools follow a recognized framework (NIST CSF / AI RMF) and data stays in approved boundaries. SHARED

☐ In place ☐ Needs work ☐ N/A

NOTES

Run a quarterly review of usage, access, and accuracy; update policy as features change. SHARED

☐ In place ☐ Needs work ☐ N/A

NOTES

Track guardrail exceptions with a named owner and expiry date. SHARED

☐ In place ☐ Needs work ☐ N/A

NOTES

Benchmark productivity gains against risk exposure over time. BUSINESS

☐ In place ☐ Needs work ☐ N/A

NOTES