

COPILOT READINESS • FIELD GUIDE

The AI Governance Checklist

15 controls to put in place **before** you turn on Microsoft Copilot — so your AI only ever sees the data each person is already allowed to see.

[For mid-market IT & security leaders](#)[Microsoft 365 • Purview • Copilot](#)

01 Data foundation — do this first

Copilot inherits your permissions. If access is messy, Copilot surfaces the mess faster. Fix the substrate before the model.



DATA-01

CRITICAL

Sensitivity labels published and auto-applying

Classify and encrypt sensitive content so protection travels with the file — Copilot honors label permissions. [Microsoft Purview Information Protection](#)



DATA-02

CRITICAL

Oversharing remediated on high-risk sites

Find SharePoint/OneDrive sites shared org-wide or with 'Everyone' and tighten them before Copilot can read across them. [SharePoint Advanced Management](#)



DATA-03

FOUNDATIONAL

Stale and orphaned sites archived

Old content nobody owns is where Copilot finds outdated or sensitive answers. Inventory and retire it. [SharePoint Advanced Management · Data Access Governance](#)



DATA-04

FOUNDATIONAL

DLP policies cover Copilot-reachable data

Stop sensitive data from being summarized into the wrong chat or leaving via the wrong channel. [Microsoft Purview DLP](#)



DATA-05

FOUNDATIONAL

Restricted Content Discovery on the riskiest sites

A stopgap that hides specific sites from Copilot while you remediate access properly. [SharePoint Restricted Content Discovery](#)

02 Identity & access

Least privilege limits what any single compromised account — or its Copilot — can reach.



IAM-01

CRITICAL

Least-privilege access reviews completed

Remove standing access nobody needs; run recurring access reviews on groups and sites.

[Microsoft Entra ID Governance](#)



IAM-02

CRITICAL

Conditional Access gates Copilot-capable apps

Require compliant devices and phishing-resistant MFA to reach M365 and Copilot. [Microsoft](#)

[Entra Conditional Access](#)



IAM-03

FOUNDATIONAL

Guest & external access reviewed

Confirm guests can't reach content Copilot might surface to internal users, and vice versa. [Entra](#)

[External ID · Access Reviews](#)

03 Copilot & agent governance

Govern not just Copilot, but every agent and connector your teams stand up around it.



COP-01

CRITICAL

Audit logging on for Copilot interactions

Every prompt and response is captured for investigation, eDiscovery, and compliance. [Microsoft Purview Audit](#)



COP-02

FOUNDATIONAL

Copilot Studio agents inventoried and owned

Know every custom agent, its data sources, and who is accountable for it — shadow agents are the new shadow IT. [Copilot Studio · Power Platform admin](#)



COP-03

FOUNDATIONAL

Connector & plugin governance defined

Control which third-party connectors agents may use to pull or push data. [Power Platform DLP connector policies](#)



COP-04

FOUNDATIONAL

eDiscovery & retention cover AI content

Copilot interactions are discoverable records — make sure retention and hold policies include them. [Microsoft Purview eDiscovery](#)

04 Responsible AI & policy

The controls that keep humans accountable and keep you ahead of emerging regulation.



POL-01

CRITICAL

Acceptable-use policy for AI published

Tell people what they can and can't put into AI, with clear ownership of outputs. [Governance policy](#) · [communicated](#)



POL-02

FOUNDATIONAL

Human-in-the-loop for consequential decisions

No AI output drives a customer, HR, credit, or safety decision without a human check. [Process control](#)



POL-03

FOUNDATIONAL

Regulatory posture mapped (NIST AI RMF / EU AI Act)

Know which obligations apply and evidence your controls against a recognized framework. [NIST AI RMF](#) · [EU AI Act readiness](#)

Want a second set of eyes before you flip the switch?

We run a fixed-scope Copilot readiness & AI governance assessment for mid-market teams — data access, labeling, and guardrails mapped in weeks, not quarters.

0–5 ✓

Start with data access & oversharing first

6–11 ✓

Pilot Copilot with a scoped group

12–15 ✓

Ready for broad, governed rollout

Book a 30-minute intro call →

collabpointllc.com

AI Governance Accelerator

© 2026 CollabPoint LLC