Copilot Readiness Assessment — Sample Report

A sanitized example of the Pro IT NW deliverable

Pro IT NW · Seattle, WA · proitnw.com · leads@proitnw.com

> **This is a sanitized sample of the Pro IT NW Copilot Readiness Assessment deliverable. The organization and figures are illustrative.** No real client, tenant, or personally identifiable data appears in this document. We use one fictional representative organization, **Northwind Advisory (illustrative)**, throughout. All counts, scores, and dollar figures are representative examples, not measurements of any real environment.

Executive summary

Subject organization: Northwind Advisory (illustrative) — a professional-services firm of roughly 600 seats, all on Microsoft 365, with a mature SharePoint Online and OneDrive footprint accumulated over several years.

Overall readiness verdict: Not ready. Three critical blockers must be cleared before enablement.

Microsoft 365 Copilot answers prompts using the same content the signed-in user can already reach. That is the entire point of the product, and it is also the entire risk. Copilot does not grant new access. It removes the friction that previously kept reachable-but-forgotten content from surfacing. A file a user *could* have found with enough digging now arrives in a tidy summary, with citations, in seconds.

In an environment where sharing has grown organically, "everything a user can technically reach" is far larger than anyone assumes. For Northwind Advisory (illustrative), our read-only scan modeled that a single representative knowledge-worker account could reach content governed by roughly **12,000 distinct permission entries** across sites, libraries, and individually shared items. The large majority of those were never deliberate. They are the residue of "Anyone with the link" sharing, "Everyone except external users" grants applied at the site level, and guest accounts that should have been removed long ago.

The headline risk is **oversharing-driven exposure at query time.** Once Copilot is enabled, an HR analyst asking "what are we paying senior associates" can surface a compensation worksheet that was technically reachable but practically invisible. A junior consultant asking about an acquisition can surface a draft term sheet from a legal site that inherited a broad sharing link three reorganizations ago. None of this requires a breach. It requires a prompt.

Go / no-go recommendation: Do not assign Copilot licenses to general users yet. Clear the three critical blockers below, then enable in a controlled pilot of 25 to 40 users with elevated monitoring before broad rollout.

The three critical blockers:

1. **Broad sharing links are pervasive** ("Anyone with the link" and "Everyone except external users" applied at scale, including on sensitive sites).
2. **No information-protection baseline.** Sensitivity labels are effectively unused, so there is no signal Copilot or Purview can act on to keep restricted content out of responses.
3. **No AI-specific governance.** Restricted SharePoint Search is not enabled, and Purview Data Security Posture Management (DSPM) for AI is not configured, so the organization has neither a containment lever nor visibility into what Copilot is actually surfacing.

Scope and method (the 2-week assessment)

This assessment is **read-only and non-disruptive.** We make no configuration changes, assign no licenses, and move no data. We use native Microsoft admin surfaces and reporting (the Microsoft 365 admin center, SharePoint admin center, Microsoft Purview, Microsoft Entra ID, and tenant-level reports) plus our own analysis to model exposure before a single Copilot prompt is ever run.

Over two weeks we examine the following areas.

Tenant and content exposure

- **SharePoint and OneDrive oversharing scan.** We model the effective reach of representative user personas and quantify how much content each can access versus how much they plausibly need.
- **Broad sharing links.** We inventory "Anyone with the link", "Everyone", and "Everyone except external users" links and grants, and we flag where they land on sensitive sites.
- **Site- and library-level permissions.** We identify over-permissioned sites, broken inheritance, and orphaned permissions.

Identity and external access

- **Stale guest and external access.** We inventory guest accounts, last-activity signals, and external sharing posture, and we flag accounts that should be removed or reviewed.

AI containment posture

- **Restricted SharePoint Search.** We confirm whether this tenant-level control is enabled and assess whether it is an appropriate interim containment lever during rollout.
- **Microsoft Purview DSPM for AI.** We check whether DSPM for AI is configured to give the organization visibility into Copilot interactions and sensitive-data exposure.

Information protection

- **Sensitivity-label coverage.** We assess whether labels exist, whether they are published, whether they are applied (manually or automatically), and what proportion of sensitive content carries a label Copilot can respect.

Licensing and admin readiness

- **Microsoft 365 Copilot license eligibility and readiness.** We confirm prerequisite licensing and identify assignment gaps and base-license mismatches.

- **Admin and governance controls.** We review who can assign Copilot, how data-handling and retention settings are configured, and whether change control exists for an AI rollout.

Deliverable: this report, a findings scorecard, a readiness-by-domain rating, and a phased remediation roadmap.

Findings scorecard

The following findings are illustrative and representative of what we typically surface in a ~600-seat environment with organically grown sharing. Counts are examples, not measurements.

#	Area	Finding	Severity	Recommended remediation
1	Data governance	"Anyone with the link" and "Everyone except external users" sharing links are widespread (modeled ~1,400 active broad links), including on sites holding internal-only material	**Critical**	Disable or restrict org-wide default to "specific people"; bulk-remediate existing broad links; require justification for new ones
2	Data governance	Sensitive-function sites (HR, finance, legal) are reachable by far more users than role requires; several inherit broad grants from parent sites	**Critical**	Re-scope sensitive sites to dedicated security groups; break inheritance; remove "Everyone except external users" from these sites first
3	Information protection	Sensitivity labels are effectively unused (modeled <2% of eligible content labeled); no auto-labeling policies in place	**Critical**	Publish a minimal label taxonomy; pilot auto-labeling on sensitive sites so Copilot and Purview have a signal to act on
4	AI containment	Restricted SharePoint Search is not enabled; no interim containment lever exists for the rollout window	**High**	Enable Restricted SharePoint Search scoped to a vetted allow-list of sites for the pilot; relax as sites are remediated
5	AI governance / visibility	Microsoft Purview DSPM for AI is not configured; the organization has no visibility into what Copilot would surface or how it is used	**High**	Onboard DSPM for AI before pilot; turn on AI interaction reporting and sensitive-data-in-prompts visibility
6	Identity and access	Stale guest and external accounts persist (modeled ~180 guests, ~40% with no activity in 90+ days), several retaining access to internal sites	**High**	Run an access review; remove inactive guests; apply expiration and re-attestation; cap external sharing on sensitive sites
7	Data governance	Over-permissioned SharePoint sites with broken inheritance and orphaned permissions create unpredictable effective access	**Medium**	Restore inheritance where safe; consolidate to group-based access; remove orphaned and direct user grants
8	Licensing	Copilot license eligibility and assignment gaps: a subset of intended pilot users lack a qualifying base license; no documented assignment process	**Medium**	Confirm base-license prerequisites; close assignment gaps for pilot cohort only; document an assignment and approval workflow

Readiness by domain

Domain	Rating	Rationale
Data governance	Red	Broad sharing links and oversharing of sensitive sites mean Copilot would surface content most users were never meant to see
Identity and access	Amber	Core identity is sound, but stale guests and lingering external access widen the exposure surface and need cleanup
Information protection	Red	No usable sensitivity-label coverage, so there is no signal for Copilot or Purview to keep restricted content out of responses
Licensing	Green	Tenant qualifies for Copilot; only minor base-license and assignment gaps remain for the pilot cohort

Admin controls	🟡 Amber	Admin roles are reasonable, but there is no AI-specific governance, no DSPM for AI visibility, and no change control for an AI rollout

Legend: Red = blocker, remediate before enablement · 🟡 Amber = address during controlled pilot · 🟢 Green = ready, minor cleanup only.

Remediation roadmap

The goal is not to fix everything before turning Copilot on. That can take months and stalls the project. The goal is to clear the blockers that cause query-time exposure, stand up containment and visibility, then expand coverage steadily while users are already getting value in a controlled pilot.

Before you enable Copilot (clear the blockers)

Action	Addresses findings	Relative effort
Re-scope HR, finance, and legal sites; break inheritance; remove broad grants from sensitive sites first	#2, #7	Medium
Disable broad sharing as the org-wide default and bulk-remediate the highest-risk existing broad links	#1	Medium–High
Enable Restricted SharePoint Search scoped to a vetted allow-list for the pilot	#4	Low
Onboard Purview DSPM for AI and turn on AI interaction and sensitive-data visibility	#5	Low–Medium
Publish a minimal sensitivity-label taxonomy and apply it to sensitive sites	#3	Medium
Confirm base-license prerequisites and close assignment gaps for the pilot cohort only	#8	Low

First 30 days (controlled pilot, then expand)

Action	Addresses findings	Relative effort
Run the pilot with 25–40 users under elevated DSPM for AI monitoring; review what Copilot surfaces weekly	#5	Low (ongoing)
Begin auto-labeling on sensitive sites and expand label coverage beyond the manual pilot	#3	Medium
Execute a guest and external-access review; remove inactive guests; apply expiration and re-attestation	#6	Medium
Widen the Restricted SharePoint Search allow-list as sites are remediated and verified	#4	Low (ongoing)
Continue bulk broad-link remediation beyond the highest-risk set	#1	Medium

Ongoing (keep it from drifting back)

Action	Addresses findings	Relative effort
Quarterly access reviews for sensitive sites and guest accounts	#2, #6	Low
Default-deny sharing posture with justification	#1	Low

required for broad links		
Auto-labeling coverage targets tracked over time	#3	Low
Monthly DSPM for AI review of Copilot usage and sensitive-data exposure	#5	Low
Change control gate for new sites, label changes, and Copilot scope expansion	#7, #8	Low

What the full engagement delivers, and the next step

This sample shows the shape of the deliverable. The paid engagement is a **fixed-fee, two-week Copilot Readiness Assessment ($15,000)** run against **your real Microsoft 365 tenant**, not an illustrative one. It produces:

- A findings scorecard and readiness-by-domain rating grounded in your actual SharePoint, OneDrive, identity, and Purview posture.
- A quantified exposure model showing what Copilot would surface for representative users in your environment before you enable it.
- An **enablement-ready remediation plan** phased the way this sample is, mapped to your sites, your sharing patterns, and your licensing.

The assessment is read-only and non-disruptive. We do not change configuration, assign licenses, or move data during the engagement. The output is yours to execute with your own team, with us, or with whoever you choose. We do not resell licenses and we hold no vendor quota, so the recommendations reflect your risk, not a product line.

Next step: to scope a Copilot Readiness Assessment for your tenant, contact **leads@proitnw.com** or start a project at **proitnw.com**.

Pro IT NW — senior-led Microsoft project work. Vendor-neutral, labor-only. Sanitized sample; organization and figures are illustrative.