Microsoft Copilot Readiness Guide

Why an Audit is Critical Before Using Copilot

Microsoft Copilot is a powerful tool that can boost productivity by making your organization's data more accessible and usable. However, without proper preparation, it can also surface sensitive information that was never meant to be widely accessible. Before you enable Copilot for your business, you must ensure your environment is secure, compliant, and ready.

This readiness audit protects your business from data leaks, compliance violations, and security risks while setting your team up for safe, productive use of Copilot.

Key Concerns to Address

1. Data Exposure Risks

Copilot can pull data from SharePoint, OneDrive, Teams, and Outlook. If permissions are too broad (e.g., "Everyone" access), sensitive files could be exposed.

2. Compliance & Regulations

Industries with requirements such as HIPAA, PCI DSS, and GDPR need guardrails in place. Without proper controls, Copilot could expose regulated data.

3. Identity & Access Security

Weak authentication, inactive accounts, or missing Conditional Access rules increase the risk of unauthorized access to sensitive data.

4. Legacy & Orphaned Data

Old files, sites, or accounts may contain sensitive information. If not cleaned up, Copilot may surface this outdated or unused content.

5. User Awareness

Employees may not realize that Copilot will show them **anything they already have access to**—even if it's data they shouldn't normally use.

Steps You Perform in the Audit

Step 1: Identity & Access Audit

- Enforce Multi-Factor Authentication (MFA) for all accounts
- Review Conditional Access policies
- Remove or disable inactive accounts

Step 2: Permissions & Data Access Review

- Audit permissions in SharePoint, OneDrive, and Teams
- Identify and correct over-permissive access (e.g., "Everyone" or anonymous links)
- Align permissions with business needs

Step 3: Data Classification & Protection

- Apply sensitivity labels (Confidential, Internal, Public)
- Set up Data Loss Prevention (DLP) policies
- Ensure encryption policies are in place

Step 4: Information Lifecycle Management

- Archive or delete obsolete data

- Apply retention and records management policies
- Clean up orphaned sites and mailboxes

Step 5: Compliance & Security Checks

- Run Microsoft's Copilot Readiness Assessment
- Validate regulatory requirements for your industry
- Confirm security baselines are in place

Step 6: User Training & Governance

- Educate employees about what Copilot can and cannot do
- Provide guidance on responsible use
- Establish escalation paths if sensitive data is surfaced

Step 7: Pilot Rollout

- Begin with a controlled pilot group
- Monitor usage, queries, and security logs
- Expand only after validating protections and governance

The Bottom Line

Before enabling Copilot, your environment needs to be **secure, compliant, and governed**. Our Copilot Readiness Audit ensures that your business is prepared, so you can take advantage of Copilot's productivity benefits—without compromising your security or compliance.

Would you like to schedule a Copilot Readiness Audit for your organization?