Data Pros

Making the Most of Copilot

A closer look at the core focus areas that guide secure and responsible adoption

Whether you've already started using Microsoft Copilot or are just exploring its potential, there's more to consider than simply turning it on. From protecting your data to guiding how people use AI day to day, a thoughtful approach helps ensure Copilot works the way it should—for your team and your business. Here are the key areas to focus on:

1. Threat Awareness and Activity Oversight

- [ ] Do you receive alerts and reports that highlight risky behavior or unusual AI activity in your organization?
- [ ] Do you have a unified view of your data security posture to identify and address potential vulnerabilities?
- [ ] Are you monitoring usage patterns and interactions that may need closer attention?
- [ ] Is your company using the available tools to analyze AI-related actions across files, emails, and chats?
- [ ] Have you set up security response practices that include Copilot-generated activity?

2. Data Protection

- [ ] Do you have a way to dynamically preserve deleted files to ensure important data isn't lost or unrecoverable?
- [ ] Are access controls and encryption automatically applied to sensitive content?
- [ ] Do you know where your sensitive data lives and how it's being used?
- [ ] Do you have systems in place to automatically protect sensitive information from risky or unauthorized access across apps, services, endpoints, and on-premises files?

3. AI Oversharing & Internal Security Risks

- [ ] Are you using conditional access to dynamically prevent unauthorized access based on real-time risk and user context?
- [ ] Do you have easy visibility into your overshared content?
- [ ] Do you get notifications when new overshared content occurs?
- [ ] Are you improving Copilot responses by regularly archiving or deleting outdated or unnecessary content?

4. Identity and Access Management

- [ ] Have you configured your permission settings to reflect your current structure and business roles?
- [ ] Do you have the ability to review who has access to what content to support responsible AI usage?
- [ ] Is your organization using access policies to help control how and where Copilot can be used?
- [ ] Are you regularly auditing user access to help maintain proper alignment?

5. Application Safety Settings

- [ ] Are your organization's filters configured to reduce the generation of inappropriate or unsafe content?
- [ ] Have you reviewed how Copilot handles potentially sensitive topics or instructions?
- [ ] Is your internal team supporting internal efforts around content safety and output quality?
- [ ] Are you applying responsible AI principles across your Microsoft environment?

6. User Guidance and Internal Policies

- [ ] Do you have a clear AI usage policy that outlines responsible AI use?
- [ ] Have you shared clear guidelines with the team on what Copilot is intended for and where to use caution?
- [ ] Is your organization encouraging your teams to double-check generated content for accuracy and tone?
- [ ] Are you providing or have you provided training or quick-reference tips to help with everyday AI usage?
- [ ] Is there reinforcement of best practices for sharing, storing, and collaborating on AI-generated content?

7. Data Governance & Risk Mitigation

- [ ] Do you have retention and deletion policies in place for Copilot interactions, meeting recordings, and transcripts, and are they being enforced consistently?
- [ ] Do you know how to use the built-in tools to detect, investigate, and take action on critical risks like data theft, leaks, or security policy violations within your organization?
- [ ] Have you applied or maintained sensitivity labels so that generated content reflects your data classification standards?
- [ ] Are you able to monitor how Copilot interacts with files and emails to surface any unexpected access or patterns?
- [ ] Have you configured data loss prevention to help reduce the chance of sensitive information being included in prompts or responses?

Why These Focus Areas Matter

Even with the right tools in place, it's easy for things to slip through without proper setup and oversight. The core areas outlined in this guide are designed to help organizations avoid common missteps and reinforce responsible use of Copilot.

Here's how these focus areas come into play in real scenarios:

- A user starts drafting an email in Word with Copilot and includes customer credit card information. A data loss prevention policy blocks the action before sensitive data is exposed.
- An employee tries to access an unapproved AI tool flagged as high-risk. Conditional Access prevents the connection, helping avoid security or compliance issues.
- An unusual spike in AI prompt activity is detected from a compromised user account. Security tools trigger an alert and respond automatically to contain the risk.
- A team member uses Copilot to generate and share marketing content without proper review. Communication policies catch the issue and flag it for review, helping maintain compliance.

Review Time

If you left any areas unchecked or weren't fully sure about how to respond, that's okay. It's a signal that there may be areas worth reviewing more closely. This guide is here to bring clarity and highlight what supports a strong Copilot experience. Even small improvements can make a meaningful difference. If you'd like help walking through any part of it, connecting with a Data Pros is a great next step.