19 Monitoring, Adoption, Training, and Support

Like everything else about M365 apps, the Copilot UX is just the beginning. Ensuring success through adoption, ongoing monitoring, and support makes the service more useful over time.

Copilot and the way people adapt to AI are in their infancy, as are the monitoring tools, training plans, and support processes that surround it. This chapter seeks to outline some steps to get started on the journey.

Monitoring and Adoption Tools and Tips

Monitoring tools in Copilot have matured. It's more than just checking whether people are using it and whether to reassign their license. There's a trend toward analyzing whether people are using it habitually, in which apps, and whether it appears to be improving how work gets done.

Two main tools are at service owners' disposal; the Microsoft 365 Admin Center, and Viva Insights.

To monitor basic usage and licensing of Copilot, you can use the **Microsoft 365 Admin Center** and the Microsoft 365 Reports dashboard.

Under the main Copilot admin ("Copilot Control System") screen, admins can find the capabilities outlined below:

- **Copilot Analytics** – Shows the total number of *active copilot users and percentage change*, a *Copilot Adoption Score* (where "To get a score of 100, all licensed users in your org must have used Copilot for an average of at least 3 days per week over the past 4 weeks," and a satisfaction score

(mainly measuring thumbs up/down). From the satisfaction score, there's a link to the actual feedback submitted by users, which can be comically enlightening! There, you can see Microsoft's response status, including "Open" and "We're working on this."

- **"Usage" Dashboard** - Offers an overview of app activities within the organization, with detailed product-level reports. Nice info here includes usage of Search and Copilot credits.
- **"Health" Dashboard-** Showing the software update channels, app versions, and service issues.

Most data can be exported to Excel for analysis.

A common goal is to ensure the $30 licenses are being used. A helpful data point in the usage report is a list that shows each Copilot enabled user's **last activity date**. The last activity within specific apps can be checked – enabling admins to see, say, if data analysts are using Copilot in Excel and to what degree. This feature can help identify the users who are not using Copilot or using it infrequently, so that they can be provided with training and support to increase their adoption and engagement (or worst, case, have their license reassigned). If privacy is a concern, the report can be anonymized (by a Global Administrator).

Viva Insights adds deeper visibility. Rather than simply reporting activity, it can help leaders understand patterns (beyond logins) of Copilot use across teams, roles, and workflows. When judging adoption, training needs, and ROI, Viva Insights provides richer signals rather than relying only on license counts and last use dates. You must be an authorized Entra ID user to see Viva Insights at an organizational or group level.

Once you have the rights, you'll see a "Readiness" page, an "Adoption and Impact" page with tenant-level and group-level metrics and HR filters, Microsoft 365 Copilot and Copilot Chat insights (similar to the Admin Center), Agent-related insights including Agent Dashboard, benchmarks, intelligent summaries, survey data-based sentiment metrics (if people are providing feedback), and trendlines.[1]

To help judge ROI, check out the **"Copilot assisted value."** This is an estimate of the value of Copilot's impact over the given time period, calculated by multiplying hours by a default of $72/hour. This is average hourly rate based on data compiled by the U.S. Bureau of Labor Statistics. Admins can change the hourly rate and the currency to an organizational/regional basis.

Such insights are helpful during scaling. If one department shows strong usage in Teams and Outlook but little use in Word, that may not mean the tool lacks value there. It may simply mean the team has not yet been shown the right scenarios. In that sense, monitoring should feed training. **The data should tell the Center of Excellence where habits are forming, where they are not, and where more specific examples or coaching are needed.**

Training Copilot Users

That brings us to training, a topic worth its own chapter, or book, eventually. Generative AI is different than other software. It's a mindset, not just a tool. There are no specific sequences of buttons or commands to follow to execute a task to streamline a business workflow.

In fact, the tools and user interfaces are changing so rapidly, one could argue that training in critical thinking and adaptability are the only baselines that matter for ongoing success.

Here are some developing tactics, nonetheless:

1. Whoever provides the trainingshould be familiar with both the technical and the fundamental thinking behind using GenAI. Trainers should be able to answer questions, address concerns, and provide tips and best practices on how to use Copilot effectively and responsibly. Initially, training is led by IT, EdTech, or L&D, but eventually should be distributed to champions with the departments via the Center of Excellence (see chapter 28).
2. Ideally, **people who do similar work should be trained together**. That may be people from the same department, or the same job personas (i.e. admin assistants from different sites or teams). That way, specific and relatable prompts can be discussed. Creating a cohort also fosters a network affect within the team. Eventually, IT and L&D needs to step back from day-to-day training, leaving adoption and training to sustain itself within cohorts or communities of interest.
3. Training should cover both the technical aspects of using Copilot, such as:

    - How and where to activate it
    - Helpful prompts based on the trainee's role
    - Ensuring accuracy and quality of outputs
    - Accepting or rejecting suggestions
    - Understanding why Copilot may be wrong

- Providing feedback (or when not to)
- Ethical and social considerations
- Avoiding plagiarism
- Disclosing the use of AI
- Other aspects of the organization's AI policy

4. Sessions should include practical examples and demonstrations of how to use Copilot in different applications and for different types of content. For instance, users can learn how to use Copilot to write an email, create a presentation, or summarize a meeting. Training should also **encourage exploration and experimentation with Copilot**, and to share their feedback and experiences with others.

Since GenAI is a mindset shift, training is not one and done. In fact, **Microsoft research showed that only after 11 weeks of regular use are people starting to internalize GenAI** (and reap its benefits).[2]

If it's up to IT or L&D provide active, consistent, and frequent training, it's time to staff up! A **more sustainable approach to ongoing training** is to foster champions withing communities of interest. IT or L&D can facilitate this by, for instance:

- Naming and incentivizing champions to continue to the day to day growth of knowledge in the department.
- Providing lunch and learn sessions, but then sending different departments or types/roles of workers into breakout rooms for different departments or types of workers to more casually collaborate. The champions then take over to run a collaborative Q&A session.
- Enabling virtual formats like shared prompts, Teams meetings, recorded tips on demand, Q&A through a Teams Channel.
- Pointing people to Microsoft documentation, videos, blogs, and FAQs. The exception to this recommendation would be during pilot programs.

In addition to training on "where to click" and "how to write a good prompt," highlight the strengths and limitations of Copilot, and **set realistic expectations for its performance and accuracy.** Users should understand that Copilot is not a replacement for human creativity or judgment, but a tool that can augment and assist them. Users should also be aware of the potential risks and challenges associated with using AI-generated content, such as bias, misinformation, or inappropriate content.

Supporting Copilot Users

Like any new technology, users may encounter some issues. Copilot might:

- Not understand the user's intent, context, or reasoning.
- Generate content that is inconsistent, incomplete, or redundant.
- Fail to follow the user's style, tone, or voice.
- Not understand formatting, structure, or conventions.

Some issues may be solvable using the techniques in this book, but some may be inherent constraints of GenAI.

To keep a flood of calls from coming into the help desk, set expectations about support. **Users should be:**

- **Informed** about the scope and limitations of Copilot, and that support may be best effort.
- **Educated** about the responsible and ethical use of Copilot, and the risks and consequences of misuse and abuse.
- **Reminded** that GenAI is still new and may not always work as expected.
- **Told** if they can provide feedback and suggestions to Microsoft to improve the service (or not).

Even with that baseline, people will unleash their problems on the help desk or water cooler, so here are some **tips to reduce tickets and issues**.

1. **The help desk must have a clear understanding** of the types of issues that require escalation to Microsoft, and the types of issues that can be resolved by resetting the user's expectations. For example, if Copilot generates texts that are offensive, harmful, or illegal, they should be reported to Microsoft immediately, and the user approached to take appropriate actions to prevent further damage. On the other hand, if Copilot generates content that is not exactly what the user wanted, but is still relevant and coherent, try to reset the user's expectations and how to improve the results.
2. **Users should also be provided with resources** and best practices on how to use Copilot effectively and efficiently. Point to training from internal and Microsoft resources. You should also point users to internal training sessions, like webinars, newsletters, and guides from your organization's Center of Excellence for AI (defined in Chapter 28).

3. **The organization's Center of Excellence should distribute support throughout the organization** by:
   - Having department champions be an outlet for ad-hoc / how-to support. Identify and empower department champions who are proficient and enthusiastic to act as local mentors for other users.
   - Providing champions with incentives, recognition, and support to help them spread the word and knowledge about Copilot. Enable these champions to communicate and collaborate with each other and with the help desk to share best practices and feedback.
   - Setting up a Teams site for people to ask questions and share their preferred prompts. The CoE should moderate and curate this site to ensure that the content is relevant, appropriate, and useful. Also, use this channel to showcase the success stories and testimonials of Copilot users, and to solicit feedback and suggestions for improvement.

By following these tips, you can help users get the most out of Microsoft 365 Copilot, and create a positive and productive relationship between humans and AI.

Monitoring for Shadow AI

So far, monitoring has focused on use of Copilot. There is also a newer and more important monitoring question: not just "Are people using AI?" but "Are they using it safely?" What if people don't think Copilot is as good as ChatGPT, or insist on using Claude instead? Shadow AI is emerging as the latest chapter in a IT's attempt to control unsanctioned applications.

Here are some strategies to keep that risk under reasonable control.

1. An organization's AI policy, drafted by its Centers of Excellence and/or CISO, should **explicitly state if the organization endorses or prohibits public models** like ChatGPT, Gemini, or Claude. If no statement is made, assume employees assume it's permitted.
2. If the organization hasn't provided M365 licenses to everyone, expect some folks to naturally go off into the shadows. Instead of letting that happen, roll out M365 Copilot Chat (included in most M365 license plans for organizations under 2000 users). This provides a basic set of AI functionality, protected in the M365 ecosystem.
3. Desktop and application security teams should **block the installation of OpenClaw, Atlas or Comet browsers**, and other trending AI

executables until they are proven secure. Set up sandboxes for sanctioned experiments.

4. Leverage Microsoft **Purview Data Security Posture Management** for AI, which is designed to help identify where sensitive data may be overexposed to AI tools, whether sanctioned or unsanctioned, and where the data estate itself creates unnecessary risk.
5. Consider using Defender for Endpoint Web Content Filtering (or something similar like Forcepoint) to **block obviously undesirable sites**, like deepseek.com. Realistically, though, this is going to be a futile effort, so addressing responsible / acceptable use is more scalable.
6. Leverage Defender for Cloud Apps to affect the policies and risks discovered by DSPM, monitor for anomalous activity within AI applications, and flag any unusual behavior. Other Cloud App Security Brokers (CASBs) offer similar capabilities to provide end-to-end AI security posture management and threat protection.
7. Come up with a process for approving/denying peoples' requests to such apps, so that expectations can be managed consistently.

In this evolving front, the key is to create the organizational structure to sustainably manage aspects like training and monitoring, over time. Unless it's a specific part of a person's job description or a COE's charter, these important aspects won't get prioritized and can end up increasing risk or eroding ROI. It ***is*** a journey, but every journey needs pilots!

---

[1] **https://learn.microsoft.com/en-us/viva/insights/org-team-insights/copilot-dashboard**

[2] **https://www.microsoft.com/en-us/worklab/ai-data-drop-the-11-by-11-tipping-point?msockid=21464d22cfce67252c815bd7cea6666d**