



Microsoft 365
Copilot

Get started deploying Copilot and agents

A playbook for IT and Security leaders and practitioners to prepare, deploy, and manage Microsoft 365 Copilot and agents with Copilot Control System and Agent 365.



Table of contents

Chapter 1

Introduction

- 02 Executive summary
- 04 About this playbook

Chapter 2

Prepare for deployment

- 10 Reduce risk early: A proactive approach to security and governance for Copilot and agents
- 16 Empower teams and prevent sprawl with management safeguards
- 22 Maximize impact: Design a measurement strategy for tangible results

Chapter 3

Deployment: Copilot and agents rollout

- 29 Stay ahead of risks with automated security and governance guardrails
- 31 Manage at scale: Dynamic controls for evolving AI systems
- 35 Demonstrate and enhance ROI through continuous reporting

Chapter 4

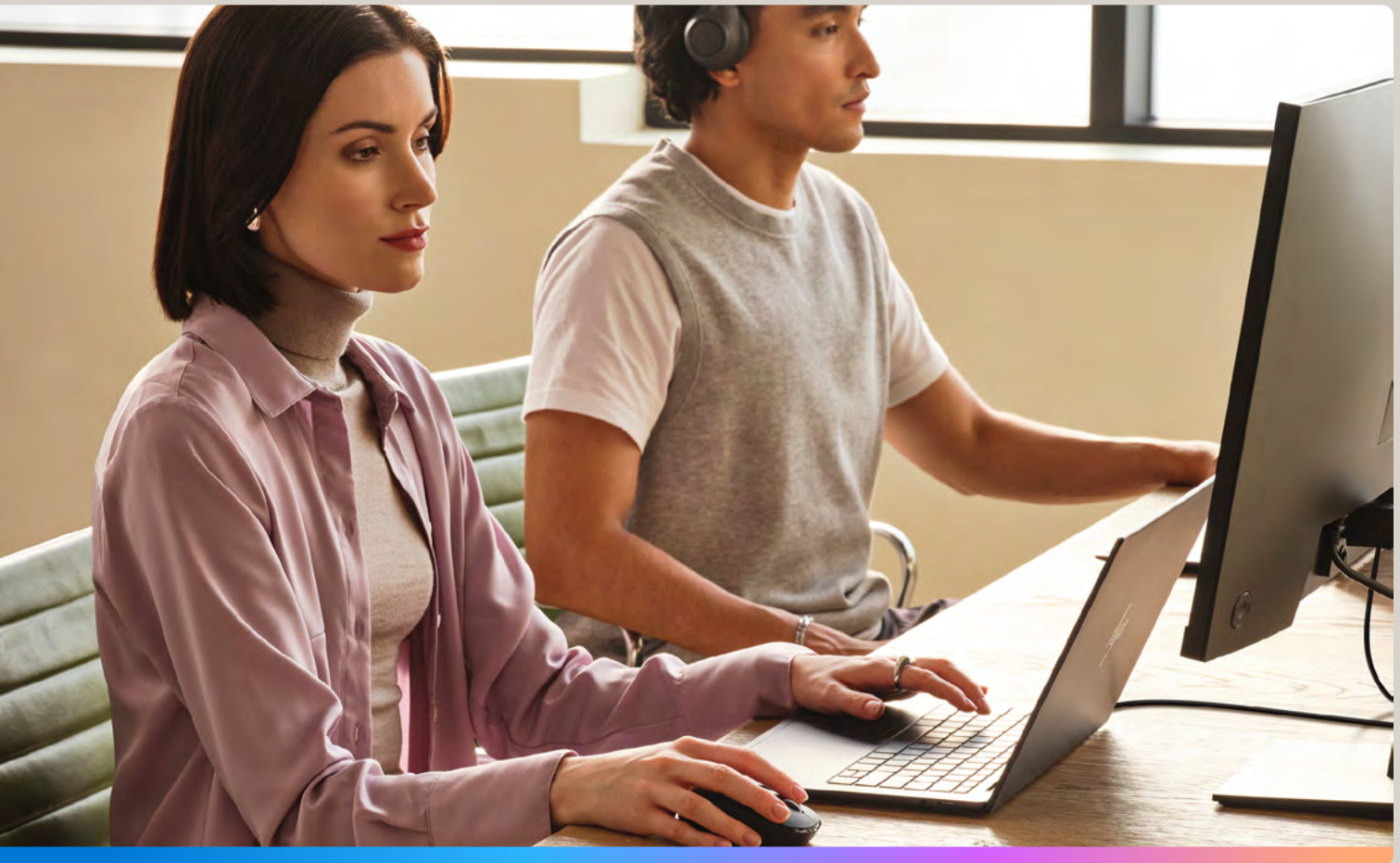
Manage AI: Optimization and value realization

- 42 Maintain continuous protection and compliance as Copilot and agents scale
- 45 Promote high-value use cases that drive strategic outcomes
- 48 Turning data into decisions: Configure an analytics environment that drives lasting value

Chapter 5

Conclusion and additional resources





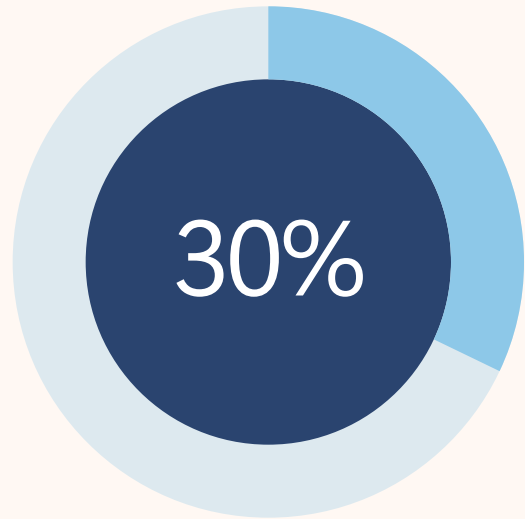
CHAPTER 1

Introduction

Executive summary

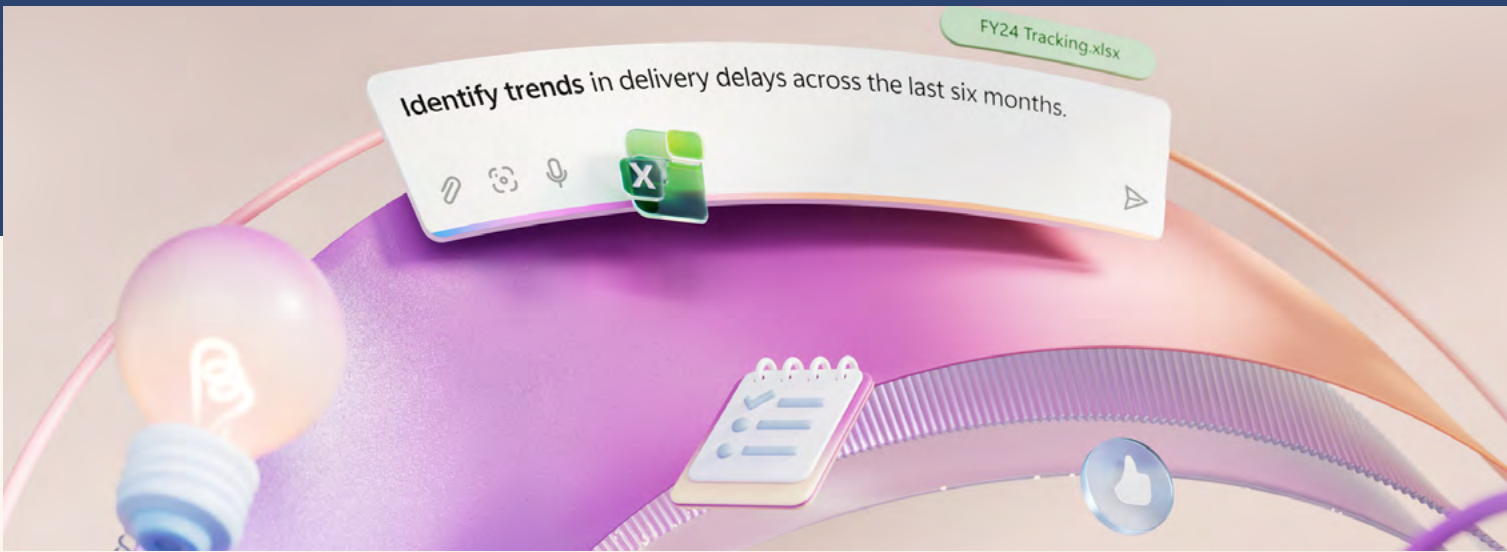
Generative AI is now a defining force in business transformation. In fact, more than 70% of CEOs surveyed by Gartner reported that AI is the technology that will most impact their industry.¹ The potential is enormous, but until now, the path to secure, governed, and measurable generative AI deployment and integration is anything but straightforward.

Across industries, IT and security leaders are under pressure to deliver on the promise of AI without compromising security, compliance, data protection, or operational integrity. Based on its survey of more than 800 business leaders, Gartner reports that “at least 30% of generative AI (GenAI) projects could be abandoned after proof of concept by the end of 2025, due to poor data quality, inadequate risk controls, escalating costs or unclear business value.”²



At least 30% of generative AI projects could be abandoned by the end of 2025

Organizations are wrestling with fragmented administration controls, disconnected security and governance tools, and informal measurement practices that make it difficult to determine ROI. Without a unified approach, AI deployments risk becoming siloed experiments—hard to scale, harder to secure, and nearly impossible to measure with confidence.



Copilot Control System (CCS) and Agent 365 are Microsoft's solutions that address these challenges. CCS provides integrated, enterprise-grade controls that empower IT administrators and security professionals to secure, manage, and measure Microsoft 365 Copilot, Copilot Chat, and Copilot Studio. Agent 365* is the control plane for managing AI agents, enabling organizations to extend their existing infrastructure for users to agents with purpose-built capabilities tailored for agent needs—all without reinventing processes.

CCS and Agent 365 give IT, security, and compliance teams comprehensive control over the entire Copilot and agent management practice—before, during, and after deployment. In a recent Accenture report, based on a survey of more than 2,000 security and technology executives on the state of cybersecurity, the firm reported that more than 75% of organizations lack the foundational data and AI security practices needed to safeguard critical models, data pipelines, and cloud infrastructure.³

CCS and Agent 365 enable organizations to gain the clarity, oversight, and assurance required to unlock the full value of Copilot and agents.

Bolted-on solutions delivered through a network of disconnected tools are not adequate for the AI era. A secure, manageable, and measured approach to AI provides the built-in controls you need, integrated into the environment and tools you already manage. This is the foundational principle of CCS and Agent 365—enterprise-grade controls within trusted solutions already familiar to your organization, optimized for use by experienced IT, admin, and security professionals.

CCS and Agent 365 deliver the visibility, control, and assurance organizations need to protect sensitive data, help enforce governance requirements, manage access and usage across Copilot experiences, and measure Copilot adoption and ROI—enabling you to unlock the full potential of Copilot and agents as a strategic asset that drives innovation, efficiency, and competitive advantage.

* Agent 365 is currently available in Microsoft Admin Center with Frontier, Microsoft's early access program for the latest AI innovations. Visit the [Agent 365 webpage](#) to learn how to turn on Frontier features and enable Agent 365 for your entire tenant or specific users.

About this playbook

This playbook is intended to be a practical, actionable guide for IT and security professionals, to confidently adopt and deploy Copilot and agents. In it, we'll show you how to leverage familiar Microsoft technologies to exercise control without inhibiting innovation. The guidance, real-world best practices, and built-in capabilities explored in this playbook are intended to help organizations:

- 1 Prepare** your tenant for Copilot and agents with the right security, compliance, and readiness baselines to speed adoption and address oversharing.
- 2 Deploy** Copilot and agents with centralized controls, guardrails, and governance for optimal license allocation, cost control, and lifecycle management.
- 3 Manage** adoption to optimize performance and prove value to stakeholders through policy enforcement, audit readiness, and measurable ROI.

This playbook serves as a reference guide for each phase of the process for preparing, deploying, and managing Copilot and agents throughout your organization.

Copilot Control System and Agent 365: Tools at a glance

Copilot Control System (CCS) and Agent 365 run on the Microsoft solutions you already know and trust—integrated across security, compliance, management, and analytics. Each tool plays a distinct role in helping to secure, manage, and measure Copilot and agents at scale. The table below describes the capabilities these tools contribute to the three phases of value-driven AI adoption.

● Copilot Control System ● Agent 365

1. Establishing Security & Governance

Microsoft Defender for Cloud Apps



A comprehensive SaaS security solution that provides visibility, control, posture management, data protection, and integrated threat defense. Helps organizations discover and manage apps, protect sensitive data in use, at rest, and in motion, and defend against advanced attacks.

Microsoft Entra



A suite of identity and network access solutions that enable secure, unified Zero Trust access across identities, endpoints, apps, and networks. Supports conditional access, least privilege, identity governance, and seamless access—helping organizations modernize security and reduce reliance on legacy tools.

Microsoft Entra Agent ID



Secure authentication and role-based permissions for Copilot and agents. Controls connector/action access for agents built in Copilot Studio or Power Platform.

Microsoft Purview



A unified platform for data security, governance, compliance, and privacy. Helps organizations dynamically secure data across its lifecycle, discover and manage data for analytics and AI, and comply with corporate and regional regulations.

SharePoint Advanced Management (SAM)



A premium set of governance controls for SharePoint and OneDrive. Helps organizations manage site lifecycle by assigning ownership, identifying inactive sites, preventing oversharing, restricting access, and monitoring apps and agents accessing content.

● Copilot Control System ● Agent 365

2. Implementing Management Controls

Microsoft 365 admin center



A centralized, web-based portal for managing Microsoft 365 services, including Copilot and agents. Provides tools to configure settings, assign licenses, monitor service health, and configure billing—simplifying day-to-day operations and enhancing control.

Power Platform admin center



A unified portal to manage apps, flows, pages, Copilot Studio agents, and select Dynamics 365 apps. Supports environment management, governance controls, security settings, deployment pipelines, licensing visibility, and monitoring—all from a single interface.

3. Measuring & Reporting

Copilot and Agent Analytics



A suite of insights spanning operational reports in the Microsoft 365 admin center, the Copilot Dashboard, and advanced reporting in Viva Insights. Enables organizations to track readiness, adoption, and cost control, as well as assess productivity impact and customize Power BI reports to measure ROI and business outcomes.

Microsoft 365 admin center reports



Operational reporting tools within the Microsoft 365 admin center. Enables admins to track license deployment, Copilot and agent usage, readiness, adoption, and cost control to better manage rollout and adoption at scale.

Microsoft Copilot and Agent Dashboard



A pre-built dashboard designed for AI adoption teams, leaders, and analysts to understand how Copilot is used across the organization. Understand how groups and teams are using Copilot to improve adoption and impact. Understand impact with Copilot-assisted hours calculations.

Viva Insights (advanced reporting)



Customizable reporting capabilities that combine Copilot and agent usage data with business metrics. Data analysts can use Power BI to build tailored reports, measure ROI and productivity shifts, and publish insights across the organization.



CHAPTER 2

Prepare for deployment

Preparing to deploy Copilot and agents begins with building a strong operational and governance foundation. This section explores the essential early steps, such as:



Cleaning up and securing your data estate so Copilot can deliver accurate, relevant, secure, and compliant results



Defining the scope and phasing of the rollout to match organizational priorities



Establishing clear security baselines to protect sensitive information from the start



Assigning ownership roles, so responsibilities for Copilot and agent adoption, security, governance, and measurement are clear

These actions not only reduce risk but also can accelerate time-to-value by helping ensure that Copilot is rooted in high-quality, well-governed data and deployed purposefully. By implementing strong access controls, compliance policies, and data and AI security practices from the outset, IT and security leaders set their teams up for sustained success and innovation.

Cultural considerations: AI readiness is a team sport

Preparing to deploy Copilot and agents is as much a cultural exercise as it is a technical one. While IT teams lead the implementation, successful AI adoption depends on deep partnership across the organization—from the C-suite to functional leaders to frontline teams.

In this early phase, CIOs and CISOs should anchor AI strategy in business outcomes and work closely with peers in HR, finance, marketing, operations, legal, and customer service to define priorities and use cases. This alignment helps ensure AI readiness is not seen as an “IT project,” but as a shared business transformation initiative.

Ongoing communication with executive leadership is critical. Regular updates, shared success metrics, and open discussions about risks and governance help maintain trust and momentum. C-suite sponsorship signals that AI is a strategic priority, while functional leaders can translate that vision into practical workflows and adoption plans for their teams.

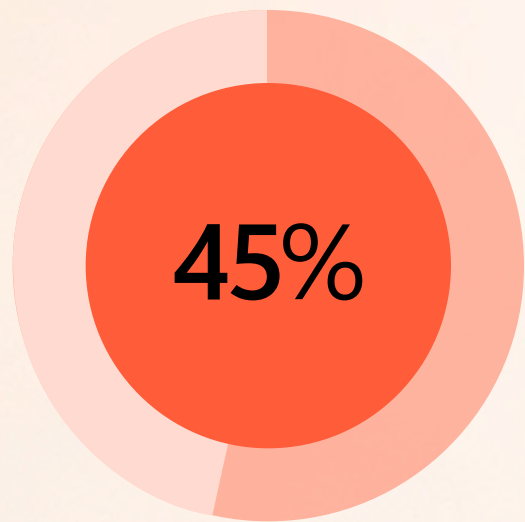
One way to embed this shared commitment is to establish a Copilot Center of Excellence (CoE) from the outset. A CoE serves as the organization’s cross-functional hub for AI governance, enablement, and advocacy—bringing together IT, security, compliance, and business unit leaders to make balanced, informed decisions. By owning agent governance, promoting high-value use cases, and coordinating training and adoption strategies, the CoE helps ensure that AI efforts remain aligned with enterprise priorities while accelerating innovation. Introducing the CoE early in the readiness phase helps institutionalize collaboration, create clear accountability, and provide a single point of leadership for scaling Copilot and agents responsibly.

Finally, make readiness a shared responsibility. Every stakeholder should see themselves as part of the AI journey, which will lay the cultural and operational groundwork for long-term success.

Reduce risk early: A proactive approach to security and governance for Copilot and agents

Security and governance are the cornerstones of a successful Copilot deployment. In the era of AI, existing risks are amplified and new risks are introduced. Based on a survey of more than 400 business leaders, Gartner's 2025 maturity findings reported that more than 45% of high-maturity organizations cite security threats among their top three AI implementation barriers.⁴ Without strong, proactive controls, AI usage can inadvertently expose sensitive information, violate compliance requirements, and erode trust before adoption reaches scale.

To prepare for Copilot and agents, organizations need to provide secure access, data protection, and content safety guardrails, while protecting against AI threats. Copilot Control System (CCS) and Agent 365 each offer a combination of security and governance controls to address these challenges, found in familiar tools including Microsoft Purview, SharePoint Advanced Management (SAM), Microsoft Defender for Cloud Apps, and Microsoft Entra. This comprehensive, better-together approach to security and governance enables organizations to secure data, govern access, and enforce compliance from the outset.



More than 45% of high-maturity organizations cite security threats among their top three AI implementation barriers

1. Protect sensitive data with Microsoft Purview to prevent data loss and insider risks

A secure Copilot deployment starts with protecting your organization's sensitive data and giving you control over how it's used by Copilot.

- **Get visibility to sensitive data in Microsoft 365**, including the type of sensitive data and location such as SharePoint, Teams, Exchange, and Copilot.
- **Automatically classify and protect sensitive data using sensitivity labels** to enforce file access permissions, including Copilot and agent access.
- **Enforce guardrails for accessing content in sensitive sites**, such as enforcing how content can be shared, whether a site can be accessed from a managed device, and whether the site is open to the whole organization or requires access to be specifically granted.
- **Alert admins immediately when oversharing occurs** and optionally block sharing of sensitive data with Data Loss Prevention.
- **Get notified when a user takes risky actions**, such as mass downloads of sensitive files or attempts to bypass sharing restrictions.
- **Dynamically apply stricter security policies when a user's action reaches a specified risk level**, such as restricting access to sites that contain sensitive data.
- **Understand your actions to meet regulatory requirements** with an actionable checklist of configurations to make in Microsoft 365 for specific regulations.

2. Address oversharing risks with Microsoft Purview and SharePoint Advanced Management (SAM)

SharePoint and OneDrive often hold an organization's richest data and can expose your business to oversharing, typically from configuration issues rather than malicious intent. Because Copilot and agents summarize and surface content across contexts, excess permissions can be quickly amplified.

- **Site governance with SharePoint Advanced Management**
SAM helps to identify potential oversharing risks and manage site ownership so owners can assist with risk remediation.
 - **Discover ownerless sites and run a workflow to identify new owners** so someone is on point to remediate oversharing risks.
 - **Run a site access review** to ask site owners enforcing access to evaluate current permissions for accuracy.
 - **Get visibility into sites that have broad access**, such as everyone sharing links or a high number of users with site access.
 - **View reports of new SharePoint sharing links** created in the past 30 days.
 - **Disable Copilot and agent access to a site** with Restricted Content Discovery or restricted content access.
 - **Apply site lifecycle policies** to archive or delete sites that are no longer needed to reduce the data surface area and improve Copilot response accuracy.



- **Identify and remediate existing oversharing risk and prevent future risks with Microsoft Purview**

Microsoft Purview provides unified data governance, security, and compliance capabilities that help organizations protect sensitive information wherever it lives. Purview helps ensure that Copilot and agents only surface content that meets your organization's protection and compliance standards.

- **Identify your highest-risk SharePoint sites** that contain unprotected sensitive data using Data Security Posture Management (DSPM) for AI Data assessments.
- **Prioritize the most used sites for remediation**, through insights about the number of unique users and files accessed in the past 30 days.
- **If Copilot Studio agents will have access to Dataverse**, identify sensitive data there and apply label protections.
- **Remediate oversharing risks in bulk** by enforcing file access policies via a default sensitivity label.
- **Remove organization-wide access to sites in bulk** by adding site sensitivity labels.
- **Use file lifecycle policies** to archive or delete files that are no longer needed to reduce the data surface area and improve Copilot response accuracy.

Getting started: Run a Purview DSPM for AI Data assessment early in your readiness phase to establish a baseline. Then, remediate risks before enabling Copilot access. This helps ensure Copilot is reasoning over approved, low-risk content exclusively.

This improved accuracy speeds up both adoption and innovation, since end users know they are working with a tool they can trust.

Getting Started with SharePoint Advanced Management (SAM)

SharePoint and OneDrive typically contain an organization's highest-value and highest-risk content, so it's important to use SAM to help govern this data before Copilot is deployed by taking the following three steps:

- **Conduct a site access review**
Run a review to discover potentially overshared sites and identify inactive or "orphaned" content. This provides an immediate, prioritized list of your biggest risk areas.
- **Configure site lifecycle policies**
Set automated policies for site review, archiving, or deletion. This shrinks the data surface area and prevents outdated content from impacting Copilot's accuracy.
- **Remediate first, deploy second**
Address the highest-risk sites before enabling Copilot for those departments. This helps ensure Copilot is reasoning over approved, low-risk content from day one, improving both security and user trust.

3. Strengthen access controls to safeguard Copilot and Agent workflows

To prevent bad actors from using Copilot to more quickly discover and access sensitive data, the first step is to prevent them from gaining access. That's where a zero-trust approach backed by Microsoft Entra plays a key role:

- **Require multifactor authentications for all users** to prevent sensitive data from being compromised by a weak password.
- **Evaluate authentication attempts for risk**, and when the risk is high, enforce additional protections, such as requiring the user to reauthenticate with MFA.
- **Use conditional access** to require that users only access sensitive data using Copilot from a compliant computer or mobile device.
- **Conduct an access review** of specific Microsoft 365 Groups or Teams to keep membership up to date.
- **Enable role-based access** via created security groups, so users can access the information, apps, and workflows needed for their roles.

Getting started: Pair Entra Identity Governance access reviews with Purview's DSPM for AI Data Assessments to identify sites containing sensitive data to target for access reviews. Organizations can add an extra layer of protection with Microsoft Defender for Cloud Apps, which monitors user and agent activity for suspicious or risky behavior in real time. Defender provides visibility into how AI interacts with sensitive data, it detects anomalies such as unusual download patterns or attempts to bypass established controls, and it can enforce threat protection measures.

Implementing Microsoft Purview, SAM, Defender, and Entra controls before deployment is critical to Copilot and agents operating within secure, compliant, and well-governed boundaries. This reduces risk, improves accuracy, and builds the trust needed for long-term adoption.

Empower teams and prevent sprawl with management safeguards

Effective management controls are essential to deploying Copilot and agents in a way that is governed and aligned with business priorities. The Microsoft 365 admin center and Power Platform admin center are the two primary control planes for configuring, monitoring, and managing Copilot and agents across your organization.

- **Microsoft 365 admin center** is the central hub for tenant-wide Copilot configuration, license management, and agent governance. It allows administrators to assign licenses via Entra ID groups, control which apps Copilot can be used in, set agent availability, and manage billing.
- **Power Platform admin center** provides granular governance for agents built in Copilot Studio, including environment creation, connector and data policy enforcement, and lifecycle management to prevent agent sprawl

Together, these tools give IT leaders the ability to phase rollout, manage access, help enforce governance, and monitor usage—all critical to maintaining control of AI adoption, and avoiding security gaps and compliance risks. Beyond that, there are a few important aspects of management controls that are critical to address in the preparation phase that comes before Copilot and agent deployment.



The strategic value of management controls

Think of proactive management controls less as a way to limit AI, and more a way to create the conditions for AI success at scale. The point of establishing a strong management foundation is to help prevent AI from becoming a source of risk and uncontrolled cost so it can become the predictable, manageable, and strategic asset that it's intended to be. The key benefits of management controls include:

- **Enabling innovation, safely**
When IT provides clear guardrails—like dedicated development environments and pre-approved connectors—it gives users confidence to experiment. This freedom within the framework helps prevent the use of unsanctioned tools and channels creativity into designated surfaces that are effectively managed and ready to be used across the enterprise.
- **Driving efficiency**
Microsoft 365 admin center and Power Platform admin center provide a unified view for managing licenses, agents, and policies. This centralized approach reduces administrative overhead, eliminates the need to juggle disparate tools, and helps ensure consistent governance.
- **Optimizing costs**
A phased rollout, combined with consumption monitoring and budget alerts, allows for the alignment of AI spending with strategic priorities, as well as the ability to reallocate licenses to maximize value and demonstrate a clear ROI.

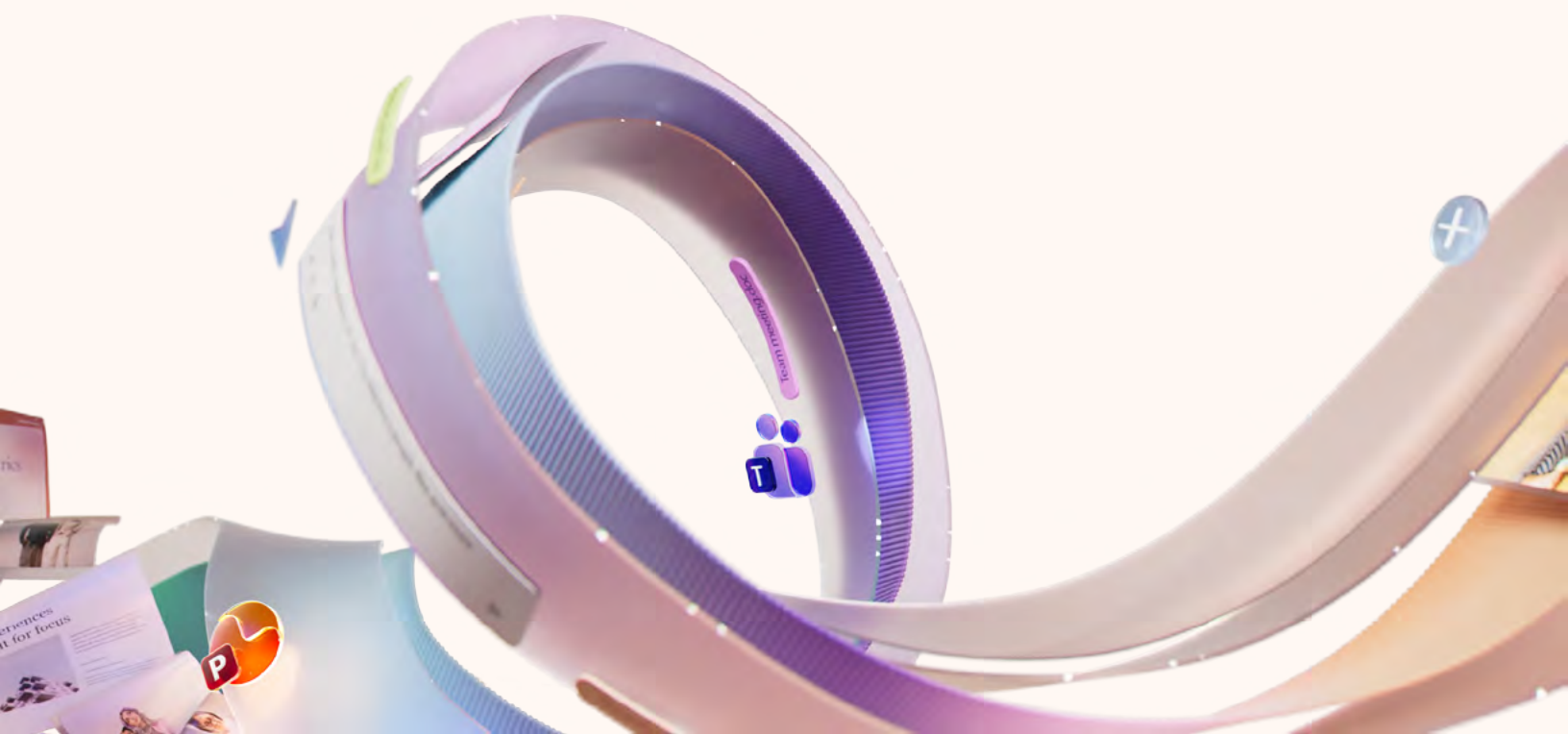
Ultimately, the management controls established during the preparation phase provide the operational backbone for a successful AI program.

1. Establish admin roles and environment setup

Strong role-based administration lays a foundation for accountability and preventing unauthorized changes well before the Copilot rollout, if IT takes these formative steps:

- **Designate an AI administrator**
Use the Global admin account in Microsoft 365 admin center to assign a dedicated AI admin responsible for Copilot and agent management.
- **Assign a Power Platform admin**
Organizations should have at least one administrator holding the Power Platform admin role to create and manage environments, configure governance policies, and oversee Copilot Studio.
- **Create separate environments for development and production**
In Power Platform admin center, create dedicated environments for testing, development, and production to prevent untested agents from being deployed broadly after the rollout.

Clear role assignment and environment separation are important to establish early on as a way of reducing the risk of misconfiguration, unauthorized publishing, and accidental exposure of sensitive data.



2. Set a licensing and feature management approach

A deliberate licensing and feature management strategy helps organizations phase Copilot adoption, manage costs, and reduce risk via:

- **Tiered licensing and pilot groups**
Start with a small, controlled set of users in a pilot group to validate governance, security, and adoption strategies before scaling. This allows you to test policies, gather feedback, and adjust configurations.
- **License assignment via Entra ID groups**
With security groups in Microsoft Entra ID established, admins will ultimately allow IT to assign and revoke Copilot licenses at scale. This makes it easier to onboard/offboard users and align license allocation with business priorities, well before a wider Copilot rollout.
- **Control Copilot use in apps**
In Microsoft 365 admin center, IT can configure which Microsoft 365 apps (Word, Excel, Outlook, Teams, etc.) are available for end users. By taking this action in advance, IT can disable Copilot in certain apps during early rollout or for specific departments.

Without phased licensing and app-level controls, organizations risk overexposure of sensitive data, unplanned costs, and governance gaps. A structured approach to licensing and feature management, however, helps ensure that Copilot is introduced in a secure, compliant, and measurable way.

3. Pre-configure agent management controls

Before enabling agents for broad use, it's important to define governance policies in Microsoft 365 admin center by taking the following basic actions:

- **Set agent availability**
Initially, configure agent availability to "No users" or "Specific users/groups." Once governance, security, and compliance measures are validated, we recommend re-evaluating these settings.

- **Block or allow certain agent types**
Decide whether to allow third-party or custom agents at launch. Restricting these early on helps IT assess risk and readiness before expanding access.
- **Connector and action controls**
In Power Platform admin center, control which connectors and APIs agents can use. This establishes early on that agents can only access approved data sources.

Pre-configuring these controls helps prevent uncontrolled agent creation and helps ensure only vetted agents and connectors are used in production. Later on, this relieves IT of keeping up with agent creation throughout the organization and handling configurations piecemeal.

4. Limit agent sprawl

Uncontrolled agent creation can lead to “agent sprawl,” or when too many agents are created and shared freely, with too little oversight. This can increase security and compliance risks, so it’s important to get ahead of agent sprawl by taking a few formative actions:

- **Dedicated environments for Copilot Studio**
Use Power Platform admin center to create specific environments for agent development, testing, and production.
- **Advanced connector policies (ACP)**
Apply ACP policies in Power Platform admin center to control which data sources custom agents can access.
- **Lifecycle management**
Regularly review and retire unused or redundant agents to maintain a clean, secure environment.

By taking these basic measures, organizations can maintain visibility into which agents exist, what data they access, and whether they comply with security and privacy requirements.

5. Establish sharing and publishing channels

A subset of limiting agent sprawl involves controlling how and where agents are shared and published. That is, there should be a dedicated space and process for maintaining oversight, by enabling key guardrails:

- **Publishing scope**
In Microsoft 365 admin center, set publishing channels to “Specific users/groups” or “Tenant-wide” based on readiness and risk tolerance.
- **Approval workflows**
Require admin review before agents are published to the tenant catalog.
- **Channel restrictions**
Limit publishing to approved environments and block external sharing until governance maturity is achieved.

Taken together, these management controls create a disciplined foundation for Copilot and agent deployment. By assigning admin roles, structuring environments, phasing licensing, pre-configuring governance, and limiting uncontrolled publishing, IT teams can set up individuals and teams for success while reducing risks. Establishing these safeguards early not only paves the way for a smoother rollout, it also builds lasting oversight and accountability as Copilot adoption expands across the organization.



Maximize impact: Design a measurement strategy for tangible results

A successful Copilot and agent deployment depends on setting a framework in advance for measuring adoption, tracking impact, and using insights to drive continuous improvement. Copilot and Agent Analytics equips organizations with a comprehensive reporting suite that provides deep insights into how employees are using Copilot and agents, enabling organizations to make better-informed decisions about how to deploy Copilot, drive adoption, and maximize business impact. It operates across four surfaces:

- **Copilot and Agent Dashboards**
Provides at-a-glance adoption and productivity insights, with the ability to segment by group, role, or region, revealing how Copilot and agents are changing productivity and shifting work patterns across the business.
 - **Viva Insights (advanced reporting)**
Connects usage data with own business metrics to customize reports and measure the tangible ROI of Copilot and agents.
- To realize the full value of Copilot and agents, organizations need more than just adoption—they need a clear, intentional approach to measurement. By establishing a robust measurement strategy from the outset, you can connect usage to business outcomes and drive continuous improvement across your deployment.
- **Microsoft 365 admin center**
Provides operational control, allowing you to understand readiness, efficiently deploy licenses, and manage agent costs.
 - **Power Platform admin center**
Monitors agent usage, performance, and consumption in Copilot Studio.



1. Design your measurement strategy

To determine business value, organizations must define success before deploying Copilot and agents. A well-outlined, three-tier maturity model should span three types of metrics:

TIER 1 Foundational

Before deployment, capture baselines to assess where the organization is starting from. Understand which employees and groups could benefit from Copilot based on current Microsoft app usage. Measure technical readiness (supported apps, licensing, environment setup), employee skill levels, and workflow benchmarks such as average time to complete core tasks. These provide the foundation for meaningful post-deployment comparisons.

TIER 2 Scalable

Track how Copilot and agents are being used across the organization. Key indicators include percentage of licensed users active within a defined timeframe, usage intensity, and feature adoption patterns across apps. Employee feedback and sentiment surveys can also highlight barriers or areas where additional support is needed.

TIER 3 Strategic

Connect Copilot and agent usage to business outcomes. Monitor improvements in productivity (time saved, efficiency gains), operational metrics (case resolution time, sales productivity), and employee experience (engagement and satisfaction scores), so adoption can be tied directly to measurable business value.

Without a defined strategy, it's difficult to demonstrate ROI or identify where interventions are needed. A well-structured plan drives intentional, sustained measurement.

2. Identify business outcomes to track

Copilot business impact reports allow organizations to correlate Copilot usage with function-specific KPIs to demonstrate tangible business impact. Examples include:

- **Sales**
Opportunities pursued, win rate, revenue per seller, deal cycle time
- **Marketing**
Lead conversion rate, campaign response rate, revenue per lead
- **Customer Service**
Case resolution rate, time to first response, customer satisfaction scores
- **Finance**
Forecast accuracy, reporting timelines, deviation from budget
- **HR**
Employee engagement scores, onboarding time, retention rates
- **IT**
Ticket resolution time, ticket closure rate

Across all functions, aligning measurement to business outcomes makes it easier to justify AI investment, secure executive sponsorship, and focus adoption efforts where they will have the most impact.



Case study

During a trial period with Copilot, Microsoft's sales organization leveraged Copilot and Copilot and Agent Analytics to rigorously measure the business impact of AI on seller productivity and revenue growth. By integrating Copilot into daily workflows and tracking usage alongside key performance indicators (KPIs) in the Copilot Business Impact Report, Microsoft was able to quantify how Copilot contributed to core sales outcomes.

Using Copilot and Agent Analytics, the team analyzed metrics such as pipeline hygiene, deal velocity, and revenue per seller. Sellers who actively used Copilot—defined as sellers who use Copilot daily, at least 50% of the time—saw a 9% increase in revenue per seller; and a 20% increase in close rates compared to their peers with a lower usage rate. Additionally, the team saw a 5% increase in sales opportunities.

These results are based on internal Microsoft sales data covering 687 sellers of Microsoft 365 Copilot from January through June 2024, as compared with sellers with low usage of Copilot.

Ultimately, the management controls established during the preparation phase provide the operational backbone for a successful AI program.



Read more here: [How we measured the business impact of Copilot on Sales at Microsoft | Microsoft Community Hub](#)

3. Plan and sequence interventions

Measurement is only valuable if it informs action. That's why analytics should be used to plan targeted interventions that drive adoption and optimize impact in the following ways:

- **Training programs**
Identify low-usage groups and deliver targeted training or role-based learning paths.
- **Behavioral nudges**
Use in-app prompts, success stories, and peer champions to encourage usage of underutilized features.
- **Process redesign**
Where data shows high-value use cases, re-engineer workflows to embed Copilot or agents more deeply.
- **License optimization**
Reallocate licenses from inactive users to high-demand areas to maximize ROI.

Designing a measurement strategy up front matters. As these examples show, the measurement strategy should be aligned to business outcomes, with the focus on sequencing interventions based on data. That way, Copilot and agents can deliver sustained, measurable value for your business.





CHAPTER 3

Deployment: Copilot and agents rollout

With foundations in place for security and governance as well as measurement, the next step is to bring Copilot and agents into active use across the organization.

This phase is about moving from planning to execution—assigning licenses, enabling features, and introducing the new capabilities to the right users at the right times so that Copilot and agents are available where and when you intend. This section also explores how to manage publishing channels, how to restrict access to unapproved connectors or agent types, and how to sequence enablement to avoid uncontrolled sprawl or security gaps.

This section also covers how to monitor usage in real time and use analytics to make informed adjustments during the rollout. By combining the right controls with live adoption insights, leaders can manage the active deployment with confidence.

Stay ahead of risks with automated security and governance guardrails

Set up guardrails and protections for how Copilot and agents can interact with and use sensitive data. The deployment phase is the point at which real-world usage begins and, with it, the need for continuous monitoring, rapid incident response, and proactive policy enforcement.

Microsoft Purview can help with real-time analysis during active rollout of Copilot and agent interactions, as well as incident response for security policy violations.

1. Decide how Copilot and agents are allowed to use sensitive data.

You can use policies to prevent Copilot from accessing certain sensitive files. This includes using the contents of the file to inform a Copilot response during grounding, referencing the files in a response, or asking Copilot to summarize the file or answer questions about it. Set up a Data Loss Prevention policy for Copilot and agents, and specify the sensitivity labels to block or enable this functionality.

2. Real-time visibility into sensitive data use and interaction content for Copilot and agents.

View summary reports for how sensitive data is being used and accessed by Copilot and agents. Click down to view a list of sensitive interactions and the actual prompt response text, including the exact web query text used by Copilot for web grounding, if used. Visit DSPM for AI reports to view this information.

3. Review the security posture for Copilot agents.

Help ensure that guardrails are correctly applied to new agents by using the DSPM for AI apps and agents dashboard. View the agent usage as it relates to security and governance, such as interactions with sensitive data. Also look at the security policies applied to the agent to ensure adequate coverage.





4. Analyze Copilot and agent use for anomalous behavior.

Let's say a user deviates from their usual behavior. For example, they use Copilot to find many sensitive files they don't normally access, view them, and then download the files to their device. This sequence of activities could indicate a data theft. [Insider Risk Management](#) can detect anomalous behavior and then automatically restrict access to sites and files until a security admin can review, so the user cannot continue the theft.

5. Surface data sensitivity to agent makers.

As makers create Copilot Studio agents, sensitivity labels on SharePoint files and Dataverse are surfaced in Copilot Studio, so makers are aware of the data sensitivity. Any actions taken by the agent in Microsoft 365, such as sending emails, are protected by Purview policy guardrails.

6. Flag interactions that may violate use policies for review.

These notifications can happen if an interaction potentially violates a use policy, such as inappropriate content, financial regulation compliance concerns, or conflicts of interest. Once flagged, security admins can visit [Communication Compliance](#) to review the potential violations and take action.

7. Capture and monitor Copilot and agent activity.

To maintain consistent oversight, organizations need visibility into how Copilot and custom agents are being used and how admins are acting on that usage. Microsoft Purview Audit can capture these events and, if needed, feed them into security information and event management (SIEM) platforms like Microsoft Sentinel for correlation and investigation.

8. Support legal discovery and recordkeeping obligations.

Legal teams can use eDiscovery to search and place interactions on legal hold, while using Microsoft Purview [Data Lifecycle Management](#) to enforce retention or deletion of interactions.

9. Security incident investigation and response.

Security teams need to prevent, detect, and respond to threats across your data estate. Microsoft Defender uses signals from Copilot and agent interactions, such as a blocked jailbreak attempt, and correlates them with other signals from endpoints and apps to provide real-time protection and automated remediation to security threats.

Manage at scale: Dynamic controls for evolving AI systems

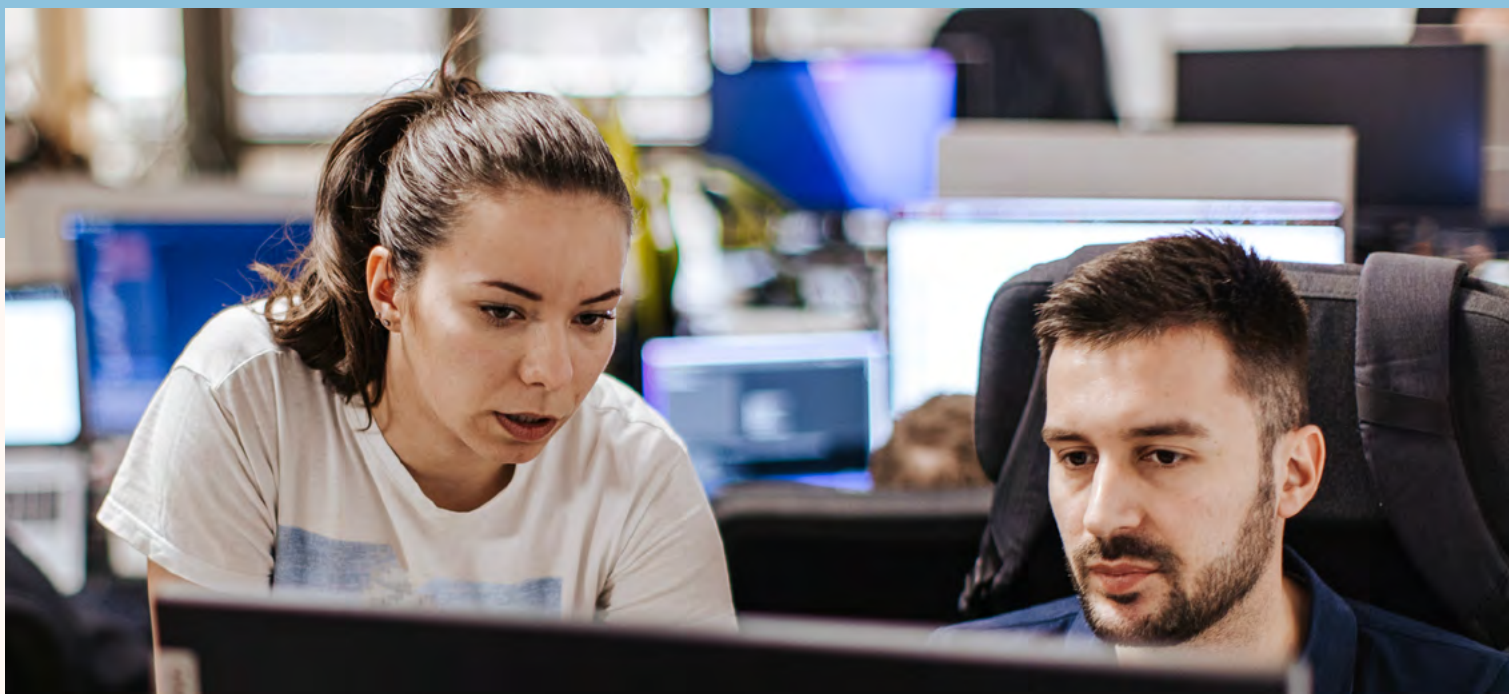
Without strong management controls, the shift to broad use of Copilot and agents can lead to uncontrolled growth, security gaps, and cost overruns. CCS and Agent 365 help to ensure your rollout is deliberate, measurable, and aligned with business priorities.

1. Begin phased pilot rollout and license management

Begin by enabling Copilot and agents for a small, well-defined pilot group through the Microsoft 365 admin center. Assign licenses to these users via Microsoft Entra security groups, which will streamline scaling access up or down. In the early stages, restrict Copilot and agent availability to specific users or groups rather than enabling tenant-wide access. This allows IT to validate governance, security, and adoption strategies before committing to a larger audience.

Use the built-in Copilot usage and cost reports to monitor adoption and feature utilization. For Copilot and agents pay-as-you-go usage, this is where you establish a critical financial guardrail. Use Copilot Billing & Usage in the Microsoft 365 admin center to set up billing policies scoped to departments or user groups, enable specific services like Copilot Chat or SharePoint agents, and configure budget thresholds with alerting rules.

These controls allow for proactive cost management, helping ensure that usage aligns with organizational budgets. Admins can also monitor consumption trends and agent-level usage, enabling informed decisions about license strategy and spend optimization. Only expand access to additional groups after confirming system stability, policy effectiveness, and positive user acceptance.



2. Iterate based on pilot feedback

A pilot program is only as valuable as the insights it generates. Establish a formal feedback channel—such as a Microsoft Forms survey, Teams feedback app, or dedicated channel—where pilot users can report issues, share successes, and suggest new use cases. Review this feedback regularly alongside usage analytics to identify patterns. Use these insights to refine:

- **Policies** such as tightening connector access and adjusting sharing limits
- **License allocation**, meaning moving licenses from low-use to high-demand areas
- **Training content** such as role-specific guidance for emerging use cases

This iterative loop helps ensure that by the time Copilot is rolled out more broadly, it is tuned to your organization's workflows, risk tolerance, and cultural readiness.

3. Instill agent approval and lifecycle governance

During rollout, no Copilot agent should reach production without explicit IT review and approval. Copilot Agent inventory in the Microsoft 365 admin center is your central hub for managing the entire agent lifecycle. This prevents agent sprawl and helps ensure that vetted, compliant solutions are available to end users.

From this single control plane, you can apply a consistent Application Lifecycle Management (ALM) process by taking these key actions:

- **Manage publishing and deployment**
When a developer publishes an agent for approval, it appears in the Agents inventory under 'Requested agents'. From there, you can formally deploy it, making it available either to all users or, more securely, to specific user groups. This controlled deployment is critical for phased rollouts and helping ensure agents are only used by the intended audience.
- **Block risky or noncompliant agents**
If an agent is found to violate security policies, becomes redundant, or is simply not approved for broad use, you can block it. In the Agents inventory in the Microsoft 365 admin center, simply select the agent, select 'block', and confirm. This action promptly prevents all users in your organization from accessing or running the agent, effectively removing it from service while retaining its configuration for potential future review.
- **Remove obsolete agents**
To maintain a clean and secure environment, you must have a process to remove agents that are obsolete, unused, or represent a security risk. Removing an agent permanently deletes it from your tenant, completing its lifecycle and reducing your organization's potential data surface area.

By systematically managing how agents are published, deployed, blocked, and ultimately removed, you maintain control over the AI ecosystem in your tenant. This should be combined with policies requiring development in dedicated non-production environments and tracking ownership to prevent orphaned agents that can become security blind spots.

4. Create mandatory security and functional reviews

Before any custom Copilot solution is published to the production environment, enforce a two-part review process:

- **Security Review**

With Microsoft Purview and built-in security controls, agents are already governed by your organization's data protection policies, approved connectors, sensitivity labels, and DLP policies. Rather than requiring a separate manual review for every agent, validate that your environment's guardrails are properly configured and up to date so all agents inherit these protections by default. Check this in the DSPM for AI apps and agents report.

- **Functional Review**

Confirm that the agent performs as intended, delivers accurate results, and aligns with the intended business process. This includes validating that the agent's description, capabilities, and usage instructions are clear and accurate for end users.

Only after both reviews are passed should the agent be approved for tenant-wide or targeted group publishing. Document the review outcomes in your change management system to maintain an auditable trail.

Enforcing management controls is an ongoing task, requiring continuous updates based on monitoring data, user feedback, and evolving business needs. By combining a phased pilot rollout, structured feedback, strict agent lifecycle governance, and mandatory reviews, organizations can scale Copilot and agents confidently while maintaining security, compliance, and cost control.

Demonstrate and enhance ROI through continuous reporting

Without a structured measurement approach, it's difficult to demonstrate ROI, secure continued investment, or identify where targeted interventions are needed. CCS and Agent 365 provide a measurement framework that helps translate raw usage data into business-centric insights by delivering a complete, quantifiable view of AI's impact—from initial readiness and adoption to tangible productivity gains and financial ROI. More than just proving the value of the investment, the goal should also be to improve the value of the investment over time.

1. Set up your measurement tools

Before deployment begins, assign the appropriate roles and permissions to help ensure your measurement team can access the necessary tools:

- In the Microsoft 365 admin center, grant the Reports Reader or Global Reader role to individuals responsible for adoption tracking.
- In Viva Insights, assign the Analyst or Insights Administrator role to those who will configure dashboards, import organizational data, and build custom reports.
- If agent usage will be measured, ensure that Power Platform admin center access is granted to relevant admins for reviewing agent telemetry.

Next, configure Viva Insights to support advanced reporting by uploading organizational data—such as department, role, region, and tenure information from HR—so that usage can be segmented by meaningful business attributes. Link employee survey data (e.g., from Viva Glint or other engagement tools) to correlate Copilot usage with sentiment and engagement outcomes. This setup enables richer analysis and more targeted recommendations.

2. Begin initial usage tracking

Once Copilot is live for your pilot group, use the [Copilot Dashboard](#) in Viva Insights to track adoption and usage patterns.

Key metrics to monitor include:

- Number and percentage of active Copilot users
- Usage intensity (average actions per user, per app)
- Adoption trends by department, role, or geography

Compare these metrics against your rollout plan to validate whether adoption is meeting expectations and to identify groups that may need additional enablement.

Measuring what matters

The [AI Adoption Score](#) in the Microsoft 365 admin center provides a single source of truth for how effectively Copilot and agents are being integrated across the organization. It goes beyond simple usage counts to provide a holistic score (out of 100) based on three key areas:

- **Setup**
How well you've prepared your technical environment for a successful deployment

- **Activation**
The percentage of licensed users who have been enabled and have started using Copilot
- **Usage**
The depth of engagement, measuring how actively users are leveraging Copilot features across different Microsoft 365 apps

The real power of the score lies in its actionable insights. You can compare your organization's score against peer benchmarks to understand where you stand in your industry. More importantly, it provides concrete recommendations to help you improve adoption, allowing you to pinpoint lagging departments or regions, and focus enablement efforts where they are needed most.

3. Begin analyzing sentiment feedback

Usage data tells you what is happening; sentiment data tells you why. Use Viva Insights to analyze employee feedback from linked surveys, focusing on:

- Satisfaction with Copilot's usefulness and accuracy
- Perceived productivity gains and work quality improvements
- Barriers to adoption (e.g., lack of training, unclear use cases)

Look for correlations between high-usage groups and positive sentiment to identify best practices worth scaling. Likewise, investigate low-usage or low-sentiment areas to uncover adoption blockers. Employee surveys focused on Copilot usage are included via Viva Pulse and accessible within the Copilot Dashboard.

4. Create stakeholder reporting

Translate your findings into clear, actionable reports for executives and business stakeholders, with a focus on:

- Building early adoption scorecards that combine usage metrics, sentiment data, and qualitative feedback
- Highlighting success stories from pilot users or departments, supported by data (e.g., "Finance reduced reporting cycle time by 20% using Copilot in Excel")
- Using visualizations from Viva Insights and the Copilot Dashboard to make trends easy to understand throughout the organization
- Including ROI indicators where possible, such as time saved, revenue impact, or efficiency gains

Share these reports regularly—weekly during pilot, monthly during early scale—to maintain executive sponsorship and demonstrate progress toward business goals.

ROI insights: Copilot business impact report

The Copilot business impact report is designed to draw a connection between AI investments and the bottom line.

By combining your Copilot usage data with KPIs from your own business systems—such as your CRM, ERP, or HR platform—you can:

- **Quantify business outcomes**
Directly measure how Copilot usage correlates with improvements in metrics like sales revenue, customer satisfaction scores, or case resolution times.
- **Understand what Copilot actions drive success**
Dig into the specific Copilot features and actions your teams are taking to drive better business outcomes.
- **Identify high-value scenarios**
Discover which specific Copilot behaviors tie to the most significant KPI improvements, so you can scale best practices.

To conduct an analysis, an administrator needs to upload two .csv files to Viva Insights: one containing organizational data such as department, role, region, and manager hierarchy, and the other containing business outcome data you want to measure, such as sales figures, case resolution times, or employee engagement scores. By linking these datasets, you provide the essential context for the report to correlate Copilot usage with tangible results.

The Copilot business impact report then provides the concrete, data-driven insights needed to demonstrate ROI and help drive informed decisions about where to focus future AI efforts for maximum impact.

The key is to treat measurement not as a snapshot in time, but as a continuous improvement loop. Use Copilot Dashboard data to track adoption, sentiment analysis to understand the “why” behind the numbers, and stakeholder reporting to drive informed decisions on license allocation, training, and feature rollout. This way, Copilot remains a measurable driver of value rather than an unquantified cost.





CHAPTER 4

Manage AI: Optimization and value realization

With Copilot and agents deployed, organizations need strategies in place to keep these capabilities secure, compliant, and aligned with business priorities while continuing to deliver measurable benefits.

The objective is to maximize value realization while maintaining the guardrails that help protect the organization's data, reputation, and compliance posture.

To achieve this, organizations should operationalize lifecycle governance—establishing repeatable processes to monitor, maintain, and evolve Copilot and agent usage over time. This includes tracking and demonstrating AI ROI through robust measurement frameworks, optimizing policies based on real-world usage and feedback, and helping governance controls adapt as new use cases emerge. By embedding these practices into daily operations, Copilot can become a managed value driver.

Maintain continuous protection and compliance as Copilot and agents scale

Once Copilot and agents are in steady-state use, security and governance efforts shift from initial enablement to continuous optimization. It means refining controls based on real-world activity, maintaining a strong compliance posture, and evolving governance alongside Microsoft's rapidly expanding AI capabilities. This requires an operational cadence for policy tuning, access reviews, and adoption of new governance features.

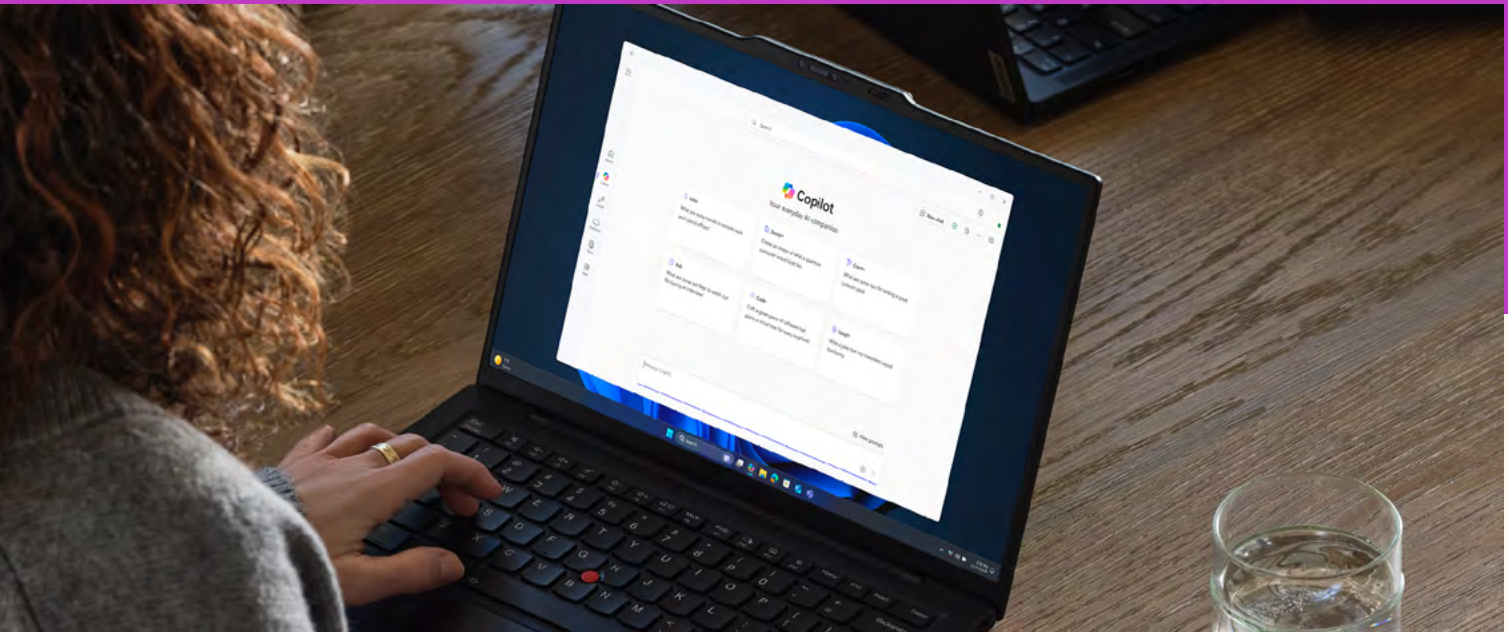
1. Policy tuning through DLP trigger analysis

Data Loss Prevention (DLP) policies are a cornerstone of Copilot governance, but their effectiveness depends on regular review and adjustment. Using Microsoft Purview DLP alert and incident logs, security teams should analyze:

- Which rules are triggering most frequently
- The context of blocked or audited actions (e.g., prompts referencing sensitive files, attempts to share protected content)
- False positives that may be impeding productivity
- Emerging patterns of risky behavior that existing rules do not yet address

This analysis should inform policy tuning cycles—adjusting conditions, refining sensitive information types, and updating rule severity to strike the right balance between protection and usability. Over time, this iterative approach reduces noise, strengthens enforcement, and helps ensure DLP remains aligned to evolving business and regulatory requirements.





2. Quarterly access reviews for licenses and sensitive data

To prevent “permission creep” and reduce the risk of oversharing, organizations should automate quarterly access reviews for both:

- **Copilot and agent licenses**
Validate that assigned licenses are still required for each user, and reclaim unused or underutilized seats.
- **Sensitive data sources used by Copilot and agents**
If you followed the Microsoft Purview guidance earlier to set up automated guardrails for how Copilot and agents can interact with sensitive data, then you do not need to do quarterly maintenance. SharePoint Advanced Management (SAM) provides point-in-time oversharing analysis, so the steps outlined in the oversharing remediation section should be done regularly.

These reviews should be workflow-driven, with site owners or data stewards confirming continued need for access. Where possible, integrate with Microsoft Entra access reviews to streamline approvals and automatically remove entitlements when no longer justified. This process enforces least-privilege principles and keeps Copilot and agent reasoning confined to approved, low-risk content.

3. Stay current with new governance features

Microsoft is continuously releasing new security, compliance, and governance capabilities for Copilot and Copilot Studio. To take advantage of these advancements, establish a formal review process that:

- Monitors Microsoft 365 Roadmap updates and Message Center posts
- Assigns responsibility to a governance lead to evaluate new features for relevance and readiness
- Tests new controls (e.g., expanded DLP for Copilot, advanced audit events, sensitivity label inheritance for agents) in a non-production environment before rollout
- Updates governance documentation, admin training, and user communications to reflect changes

By operationalizing this review cycle—ideally on a monthly or quarterly cadence—organizations can quickly adopt capabilities that enhance oversight, close security gaps, and maintain compliance with emerging regulations.

Security and governance are not static—they are living disciplines. Regular DLP policy tuning, automated quarterly access reviews, and proactive adoption of new Microsoft governance features help ensure that Copilot and agents remain secure, compliant, and aligned with business value goals as usage scales.

An abstract graphic at the bottom of the page features flowing, curved lines in shades of purple, pink, and blue. A small, glowing blue cube is positioned in the center, with a dashed line trailing behind it. In the bottom right corner, there is a partial view of a keyboard and a small interface element with the text "Ask a question".

Promote high-value use cases that drive strategic outcomes

Management controls focus on maximizing value from existing Copilot and agent investments, so usage aligns with business priorities and scaling capabilities in a controlled, secure manner. This requires disciplined license and cost management, targeted expansion of features and connectors, and a governance structure that promotes high-value use cases while maintaining compliance.

1. Developing a Copilot Center of Excellence

To sustain optimization and value realization, organizations should establish a Copilot Center of Excellence (CoE) as a cross-functional governance and enablement body. This team should include representatives from IT administration, security and compliance, and business units to ensure balanced decision-making and alignment with enterprise priorities.

The CoE should take ownership of agent governance, including reviewing, approving, and cataloging agents; setting development standards; and managing lifecycle processes. It should also act as a knowledge hub for sharing best practices, publishing success stories, and promoting high-value use cases across the organization.

Close collaboration with departmental “agent makers” will help the CoE identify new opportunities, ensure proper training, and align agent development with strategic objectives. Quarterly reviews led by the CoE should assess license utilization, the health of the agent portfolio, and the effectiveness of governance policies, making recommendations for adjustments where necessary.

By combining governance oversight with enablement and advocacy, the CoE can enforce compliance while accelerating innovation and adoption.

2. Optimizing license utilization

Microsoft 365 usage and adoption reports in the Microsoft 365 admin center provide the foundation for ongoing license optimization.

There, administrators should regularly review Copilot usage reports to identify licensed users who have little or no activity over a defined period, such as 30 to 90 days. These reports should be a key input for the Copilot Center of Excellence (CoE), which can then make recommendations on reclaiming and reassigning inactive licenses to high-demand users or new business units. This process avoids unnecessary spend and helps ensure that the most valuable seats are always in use.

In parallel, agent usage patterns should be analyzed using the Agent Usage and Message Consumption reports to determine which departments or teams are driving the most consumption. This data can be used to set departmental budgets for pay-as-you-go Copilot or agent consumption, and to configure alerts in the Power Platform admin center and Microsoft 365 admin center that notify administrators when spending approaches predefined thresholds.

Where appropriate, enforcement controls—such as soft limits that trigger admin notifications or hard limits that suspend usage—should be applied to prevent cost overruns. By continuously monitoring usage and reallocating resources, organizations can ensure that licenses and consumption budgets remain aligned with actual usage and business value.

3. Extending and enhancing capabilities

Once governance is stable, organizations can begin to safely expand Copilot and agent capabilities to unlock new high-value use cases. This expansion should be controlled and deliberate, using the right admin center for the right task to maintain security and compliance.

Use the Microsoft 365 admin center as your primary control plane for governing the availability of all agent types in your tenant. From the Integrated Apps page, you can manage the lifecycle for:

- First-party agents from Microsoft
- External agents from third-party vendors
- Custom, Shared, and Frontier agents—experimental or advanced agents that use new capabilities or integrations, which might be in the early stages of testing—developed within your organization

[Read more here](#) on the several types of agents you can manage in Copilot.

Within Microsoft 365 admin center's Agent Inventory and usage reports, you can approve, deploy, or block these agents, controlling which users or groups can access them. This process should be guided by the review and approval workflows established by the CoE to help ensure that only vetted solutions are made available.

For agents built in-house using Copilot Studio, Power Platform admin center provides granular control over their components and data access. This is where you enforce technical governance by using ACP to classify connectors as "Business," "Non-business," or "Blocked," helping ensure that agents only interact with approved data sources. These crucial DLP policies should be defined and managed by the CoE to instill a consistent management posture across all agents.

This combination of controlled expansion—using Microsoft 365 admin center for broad availability and Power Platform admin center for deep technical governance—is important for creating an agent portfolio that remains more relevant, secure, and impactful.

In the optimization phase, management controls shift from initial enablement to continuous value engineering. This helps to ensure that licenses and budgets are used efficiently, capabilities are expanded with discipline, and a governance body drives both compliance and innovation.

Turning data into decisions: Configure an analytics environment that drives lasting value

Because the optimization phase is about shifting from adoption to sustained business value, it's important to maintain momentum by moving beyond anecdotal success stories to a data-driven impact narrative. Copilot Control System (CCS) and Agent 365 provide a comprehensive reporting stack that operationalizes measurement so that analytics can be used to create a continuous feedback loop that optimizes enablement, refines governance, and maximizes the strategic value of Copilot and agents over the long term.

1. Operationalizing measurement and reporting

The following implementation steps outline how to set clear success criteria, configure the right analytics environment, and establish a repeatable reporting cadence—helping to ensure that measurement becomes a strategic lever for both demonstrating value and driving ongoing optimization.

- **Define success up front**
Agree on target KPIs and adoption goals before rollout (e.g., "75% active usage within 90 days," "20% reduction in report preparation time"), and capture baseline metrics for productivity, quality, and engagement.
- **Set up the analytics environment**
Assign Reports Reader or Global Reader roles in Microsoft 365 admin center. In Viva Insights, assign Analyst or Insights Administrator roles and upload organizational attributes (department, role, region, tenure). Then, integrate relevant business outcome data from CRM, ERP, HRIS, or service platforms.

- **Establish a reporting cadence**
Start with weekly reporting during pilot phase, then shift to monthly reporting once Copilot has been deployed at scale. Use dashboards to share adoption and impact data with executives, functional leaders, and change management teams.
- **Close the loop**
Treat measurement as a continuous improvement cycle, from data to insights to intervention to re-measurement. With this approach, organizations are better positioned to use insights to refine governance, adjust training, and optimize license allocation.

2. Demonstrating business value and ROI

Copilot and Agent Analytics offers both out-of-the-box and customizable tools to measure how Copilot and agents are impacting your organization. This includes surfaces explored previously in this playbook, specifically:

- **Copilot Dashboard**
Here, you'll be able to continue surfacing trends in licensing, activation, and usage, and correlating them with collaboration and productivity metrics.
- **Copilot business impact report**
It's important to continue validating your metrics and KPIs (e.g., revenue per seller, case resolution time, forecast accuracy, employee engagement), and compare them against metrics from CRM, ERP, HRIS, or other systems to create a unified view of AI's contribution to business performance.
- **Advanced adoption and impact reports**
Conduct deeper analysis with Power BI templates, including before/after comparisons, segmentation by department or geography, and AI-assisted hours/value calculations.

By integrating business outcome data with Copilot usage metrics on adoption, business impact, and sentiment, leaders can move beyond anecdotal success stories to more quantifiable ROI. And with regular, transparent reporting, leaders can build and maintain confidence throughout the organization, and keep AI investments aligned with strategic priorities.

3. Using analytics to optimize enablement and deployment

Measurement is not just about proving value—it's about finding and acting on opportunities to improve continuously. Copilot and Agent Analytics enables organizations to pinpoint where to focus enablement resources for maximum impact.

Remember, it's important to identify high- and low-adoption areas using segmentation in Viva Insights. Comparing adoption across roles, departments, or geographies can help identify high-adoption cohorts that can serve as internal case studies to replicate success, as well as low-adoption groups that could benefit from targeted training or governance adjustments. From there, IT leaders can:

- **Correlate usage patterns with outcomes**
The Copilot business impact report can reveal which specific Copilot actions (e.g., summarizing meetings, drafting emails, generating presentations) are most strongly associated with positive KPI shifts. This insight helps refine training and promotes high-value behaviors.
- **Spot underutilized features and surfaces**
Usage breakdowns by app (Word, Excel, Teams, Outlook, PowerPoint) can highlight where Copilot capabilities are being overlooked. For example, if summarization in Teams is widely used but Excel analysis is not, targeted enablement can unlock additional productivity gains.
- **Sequence interventions based on data**
Combine usage telemetry with sentiment surveys to determine why adoption is lagging in certain areas—then deploy the right intervention. It could be a training program to address skill gaps, a process redesign to embed Copilot into workflows, license reallocation to high-demand areas, or feature enablement for high-value scenarios.

In CCS and Agent 365, measurement is both a proof point and a steering mechanism. By combining Copilot usage telemetry, business outcome data, and employee sentiment, leaders have the tools to help them demonstrate ROI with confidence, secure ongoing investment, and continuously optimize deployment for maximum enterprise value.



CHAPTER 5

Conclusion and additional resources

Microsoft 365 Copilot and agents are quickly reshaping how organizations work, compete, and deliver value

Yet realizing this transformative technology's promise at enterprise scale requires more than deploying powerful tools. It demands a governance and management framework that gives leaders full visibility into how agents are accessed, used, and governed, and the ability to securely steer adoption with confidence, accountability, and measurable impact.

Copilot Control System (CCS) and Agent 365 deliver exactly that. Built into the Microsoft 365 ecosystem, CCS and Agent 365 provide integrated, enterprise-grade controls. This helps reduce the fragmentation and blind spots that can undermine AI initiatives, replacing them with a cohesive, enterprise-grade approach that is more secure by design, operationally efficient, and aligned to business priorities so that your deployments are secure, scalable, and measurable.

In following this playbook, your organization will be empowered to:

**Secure and govern Copilot and agents responsibly**

Apply consistent, policy-driven controls across all Copilot and agent interactions, protecting sensitive data and driving compliance with internal standards and global regulations.

**Manage AI at scale**

Centrally configure permissions, licenses, and lifecycle policies; mitigate uncontrolled growth; and integrate seamlessly with existing Microsoft 365 security, compliance, and analytics capabilities.

**Measure and optimize ROI**

Use Copilot and Agent Analytics, Viva Insights, and advanced reporting to link AI adoption directly to productivity gains, KPI improvements, and strategic business outcomes.

The result is an AI operating model that is transparent, governed, and measurable.

Take the first step: Review your governance baselines and data estate readiness. Set up measurement frameworks to track adoption and impact. Engage stakeholders across your business to align priorities and drive change. Then, use the tools and guidance in this playbook to maximize the value of Copilot and agents for your organization. This will help you unlock greater trust, strategic impact, and alignment to business value.

Success with Copilot and agents is a continuous journey of optimization and innovation. With CCS and Agent 365, your organization will have the tools to adapt, scale, and demonstrate clear ROI as your work and goals evolve. By embedding strong governance, management, and measurement practices, you establish a strong foundation from which your organization can strive to deliver lasting value, contain costs, and drive toward business outcomes.



**Dive deeper into the
Copilot Control System**

Copilot Control System tools

- [Microsoft Defender for Cloud Apps](#)
- [Microsoft Entra](#)
- [Microsoft Entra Agent ID](#)
- [Microsoft Purview](#)
- [SharePoint Advanced Management \(SAM\)](#)
- [Microsoft 365 admin center](#)
- [Power Platform admin center](#)
- [Copilot Analytics](#)
- [Microsoft Copilot Dashboard](#)
- [Microsoft 365 admin center reports](#)
- [Viva Insights \(advanced analysis\)](#)

Resources

- [Copilot Control System](#)
- [The strategic CIO's generative AI playbook](#)
- [Microsoft Purview: Learn about sensitivity labels](#)
- [Microsoft Purview: Learn about data loss prevention \(DLP\)](#)
- [Microsoft Purview: Learn about Adaptive Protection in data loss prevention](#)
- [Microsoft Purview: Learn about Data Secure Posture Management \(DSPM\) for AI](#)
- [Microsoft Purview: Default sensitivity labels and policies to protect your data](#)
- [Microsoft Purview: Learn about Insider Risk Management](#)
- [Microsoft Purview: Learn about data lifecycle management](#)
- [Microsoft Purview: Learn about Communication Compliance](#)

- [Microsoft SharePoint: Initiate site access reviews for data access governance reports](#)
- [Microsoft SharePoint: Restrict discovery of SharePoint sites and content](#)
- [Microsoft SharePoint: Manage inactive sites using Site lifecycle management](#)
- [How it works: Microsoft Entra multifactor authentication](#)
- [Microsoft Entra ID: Building a Conditional Access policy](#)
- [Microsoft Entra ID governance: What are access reviews?](#)
- [Microsoft Entra ID: Assign licenses to users by group membership using the Microsoft 365 admin center](#)
- [Microsoft 365: About administrator roles in the Microsoft 365 admin center](#)
- [Microsoft 365: Manage Microsoft 365 Copilot agents in the Microsoft 365 admin center](#)
- [Microsoft 365: AI adoption category in Adoption Score](#)
- [Power Platform: Designate the Microsoft Power Platform admin role](#)
- [Personal Developer Environments: Secure, governed innovation in Power Platform](#)
- [Power Platform: Advanced connector policies](#)
- [Microsoft Copilot Studio: Work with Power Platform environments in Copilot Studio](#)
- [Microsoft Viva Insights: Copilot Analytics introduction](#)
- [Microsoft Viva Insights: Copilot business impact report](#)
- [Microsoft Azure Cloud Adoption Framework: Establish an AI Center of Excellence](#)

Sources

¹"The CIO Report," a commissioned study conducted by Gartner, Inc., Q1 2025. This claim is based off the aggregated self-reported experiences as gathered through anonymous polling and 1:1 advisory sessions. The specific impacts of AI are projections based on the survey and study. They do not constitute guarantees nor promises, and individual productivity and beneficial outcomes are dependent on the organization and will vary.

²"Gartner Predicts 30% of Generative AI Projects Will Be Abandoned After Proof of Concept By End of 2025," July 29, 2024. This claim is based off the aggregated self-reported experiences as gathered through a survey of 822 business leaders conducted between September and November 2023. The specific impacts of AI, including revenue increases, cost savings, and productivity improvement are projections based on the survey. They do not constitute guarantees nor promises, and individual benefits or negative outcomes are dependent on the organization and will vary.

³"State of Cybersecurity Resilience 2025: Elevate your cybersecurity to fit an AI-driven world," June 25, 2025. This claim is based off the aggregated self-reported experiences as gathered through a survey of 2,286 respondents (1,828 CISOs and 458 CIOs) from companies with global revenues of >\$1 billion, spanning 17 countries—US (458), Canada (79), Brazil (102), UK (236), Ireland (68), France (182), Germany (190), Italy (180), Spain (100), UAE (66), KSA (66), South Africa (50), Australia (128), Japan (166), India (89), Singapore (77), Thailand (49)—and 24 industries: Banking (125), Insurance (130), Capital Markets (113), Automotive (50), Chemicals (100), Consumer Goods and Services (100), Retail (125), Telecommunications (125), Media (100), Oil & Gas (150), Healthcare Payers (50), Healthcare Providers (100), High Tech (100), Industrial (50), Life Sciences – BioPharma (142), Life Sciences – MedTech (76), Public Services (150), US Federal Services (50), Utilities (150), Software & Platforms (100), Transport (50), Aerospace & Defense (50), Travel & Hospitality (50), Natural resources (50). The potential deficiencies of organizations and their effects are pre projections based on the survey. They do not constitute guarantees or promises, and individual outcomes are dependent on the organization and will vary.

⁴"Gartner Survey Finds 45% of Organizations With High AI Maturity Keep AI Projects Operational for at Least Three Years," June 2025. This claim is based off the aggregated self-reported experiences as gathered through a survey of 432 respondents from organizations in the US, the UK, France, Germany, India, and Japan in Q4 of 2024. The security risks associated with AI are projections based on the survey. They do not constitute guarantees nor promises, and individual risks and outcomes are dependent on the organizations and will vary.

© 2025 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.