

Microsoft 365 Copilot Readiness Planning and Roadmap

December 17, 2024

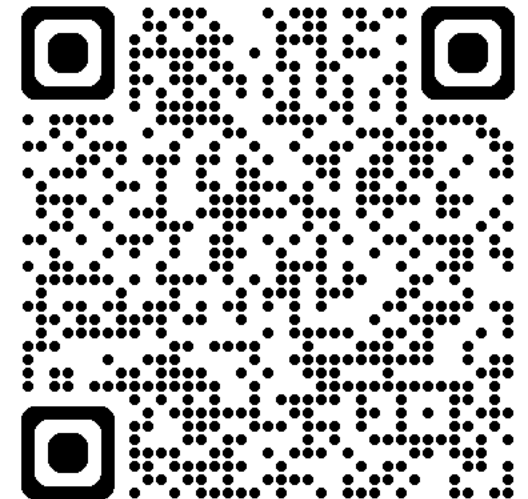
11-11:45 AM EST



Peter Carson



- President, Envision IT
- 14X Microsoft M365 MVP
- Regular industry speaker
- pcarson@envisionit.com
- envisionit.com
- [linkedin.com/in/petercarson](https://www.linkedin.com/in/petercarson)
- President Toronto M365 User Group



Agenda

Introductions

Microsoft 365 Copilot at Ignite

Readiness Roadmap

Summary, Q&A and Closing

3 Key Takeaways

1

AI Is Coming – Either Under Your Control or Not

2

Data Needs to Be Prepared Before You Turn on Copilot

3

Start with Tenant Reporting and Analysis

Microsoft 365 Copilot at Ignite

Tuesday, Nov 19

Microsoft 365 Copilot Advantages: How does it compare with other AI solutions
(Decision-maker)

Speakers: Seth Patton, Rob Howard

Time: 2:45 – 3:30 PM CST

Where's the ROI? We've got you.
(Technical)

Speaker: Matthew Duncan

Date & Time: 3:45 – 4:00 PM CST

Explore technical details and applications of Microsoft 365 Copilot Business Chat and Copilot Pages
(Technical)

Speakers: Ned Friend, Maya Rodrig

Time: 4:00 – 4:45 PM CST

Explore top Copilot functional and industry use cases, prompts, and tools
(IT/Pro TDM)

Speakers: Alyson Ginesta, Cynthia Johnson

Time: 4:30 – 5:00 PM CST

Wednesday, Nov 20

How M365 Copilot Works
(Decision-maker)

Speaker: Ned Friend

Time: 11:15 – 11:45 AM CST

Ground Microsoft 365 Copilot in your business knowledge
(Decision-maker)

Speakers: Jenn Cockrell, Mike Bassani

Time: 1:15 – 2:00 PM CST

How to drive user engagement and business value with Microsoft 365 Copilot
(Decision-maker)

Speakers: Cynthia Johnson, Alyson Ginesta

Time: 5:00 PM – 5:45 PM CST

Thursday, Nov 21

Follow the prompt! Tracking and managing Copilot prompts at hyperscale
(Technical)

Speakers: Ben Summers, Erica Toelle

Time: 9:45 – 10:30 AM CST

Discover a new way of working with M365 Copilot + Pages at the center
(Decision-maker)

Speaker: Manon Knoertzer

Time: 1:30 – 2:00 PM CST

Friday, Nov 22

The spectrum of agents with Copilot Studio
(Decision-maker)

Speakers: Jack Rowbotham

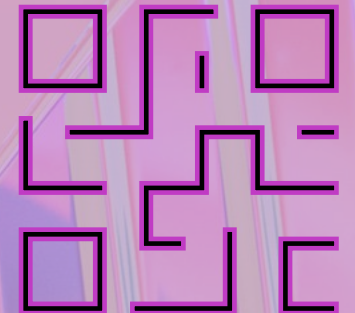
Time: 9:00 – 9:45 AM CST

Prepare your data for Microsoft Copilot with new tools
(Technical)

Speakers: Alex Pozin, Erica Toelle, Dave Minasyan

Time: 9:00 AM – 9:45 AM CST

Optional QR Code



Is Deploying Copilot like opening Pandora's Box?

- Copilot for Microsoft 365 has great potential
- It combines large language models (LLMs) with your organization's data making it one of the most powerful productivity tools on the planet
- But with great power comes great responsibility, especially when it comes to keeping your data safe





Search



Work

Web



Copilot

To get started, try one of the suggested prompts, type your own, or just select the content you want to work with.

- All
- People
- Files
- Meetings
- Emails
- Prompts



Help me learn about
topic

Draft email notes for
meeting

Help me improve my
writing based on **file**

Are there any
org changes
happening
next month?

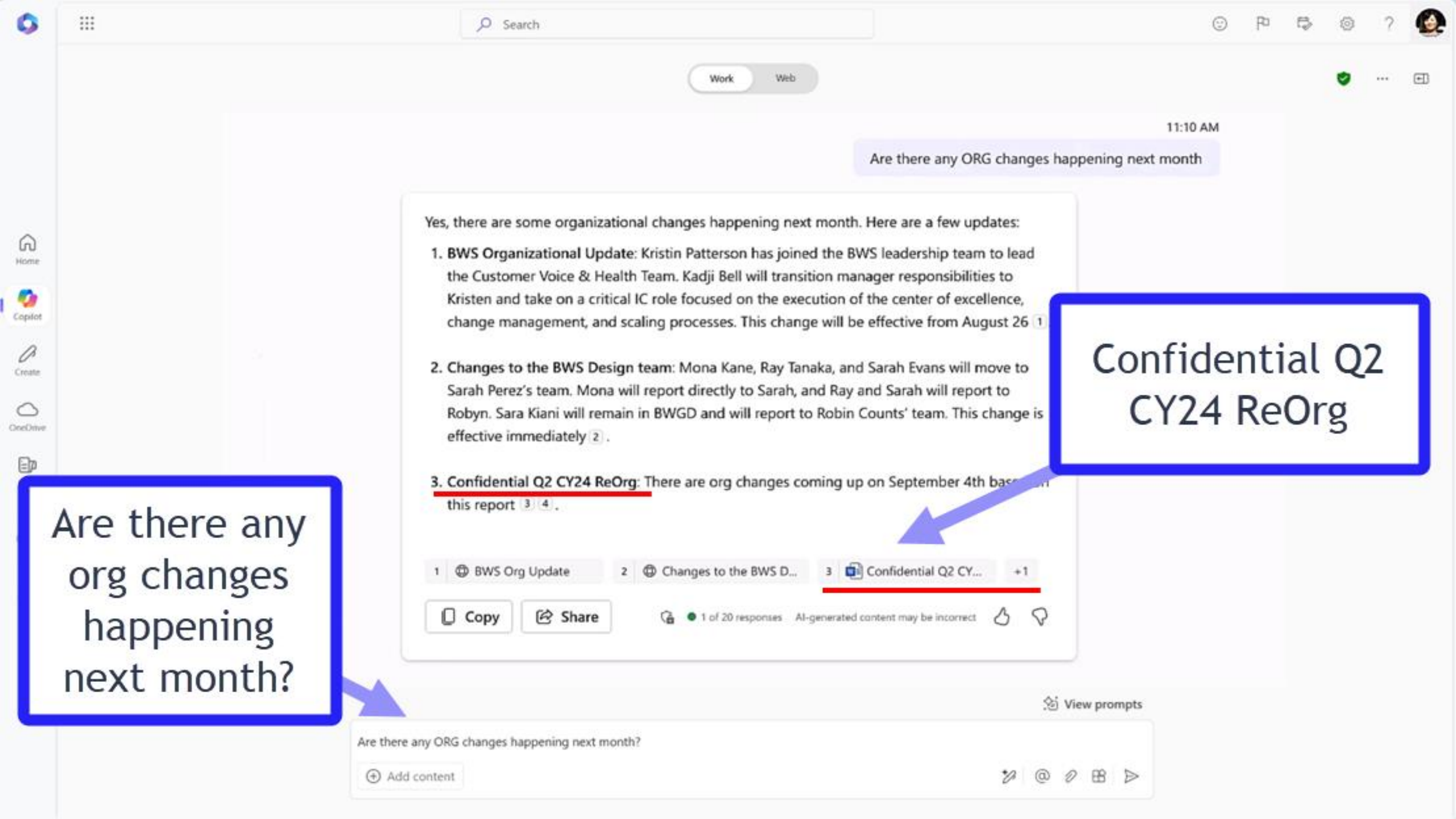
Are there any ORG changes happening next month?

+ Add content

View prompts



- Home
- Copilot
- Create
- OneDrive
- Feed
- Pages
- Apps



Search

Work Web

11:10 AM

Are there any ORG changes happening next month

Yes, there are some organizational changes happening next month. Here are a few updates:

- 1. BWS Organizational Update:** Kristin Patterson has joined the BWS leadership team to lead the Customer Voice & Health Team. Kadji Bell will transition manager responsibilities to Kristen and take on a critical IC role focused on the execution of the center of excellence, change management, and scaling processes. This change will be effective from August 26 ¹
- 2. Changes to the BWS Design team:** Mona Kane, Ray Tanaka, and Sarah Evans will move to Sarah Perez's team. Mona will report directly to Sarah, and Ray and Sarah will report to Robyn. Sara Kiani will remain in BWGD and will report to Robin Counts' team. This change is effective immediately ².
- 3. Confidential Q2 CY24 ReOrg:** There are org changes coming up on September 4th based on this report ³ ⁴.

Confidential Q2
CY24 ReOrg

Are there any
org changes
happening
next month?

1 BWS Org Update 2 Changes to the BWS D... 3 Confidential Q2 CY... +1

Copy Share 1 of 20 responses AI-generated content may be incorrect

Are there any ORG changes happening next month?

Add content

View prompts

@

How Copilot gets access to content

Copilot retrieves only the information you have access to

The process is called “retrieval augmented generation”

1

You submit a prompt

2

Orchestrator determines what it needs to answer the prompt

3

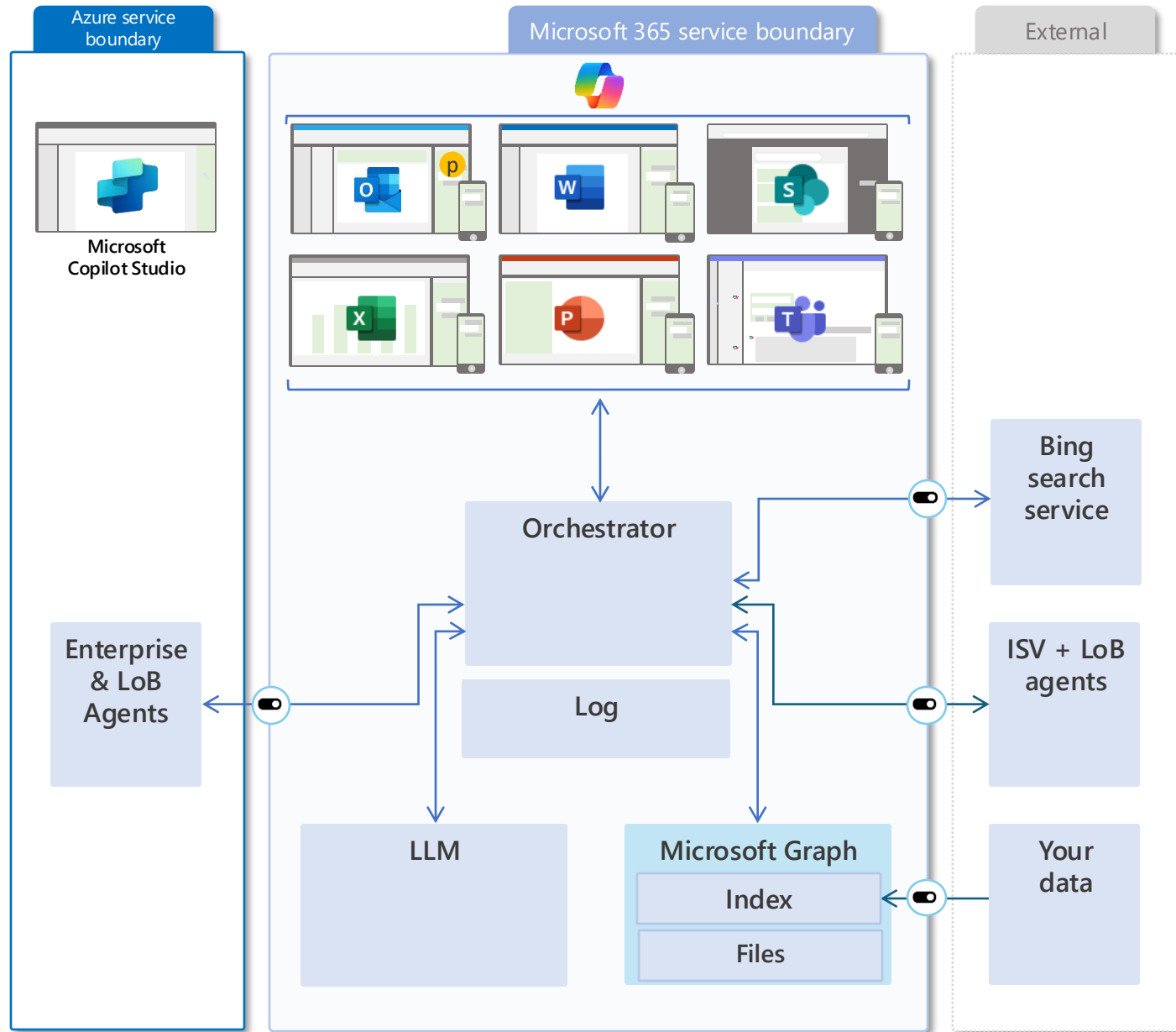
Orchestrator uses Graph to find relevant info you **are allowed to access**

4

Orchestrator appends info to your prompt to enhance it

5

LLM uses additional that information to generate a response



[Microsoft Ignite 2024 - Follow the Prompt! Tracking and Managing Copilot prompts at hyperscale](#)

Internal oversharing: Too much access and too few controls

1

Over-permissioning too much internal access

Bias towards overly broad access
for permissions and links

2

Under-enforcement too few internal controls

Content looks the same without
labeling and content-aware policies
to follow its use

Implications

Risk of exposure in search and AI tools

Hard to get started with AI and solve without the right tools

Oversharing is a byproduct of collaboration

Individual user permissions



Exchange mailbox



Teams chats



OneDrive for Business

Group based permissions



Teams channels

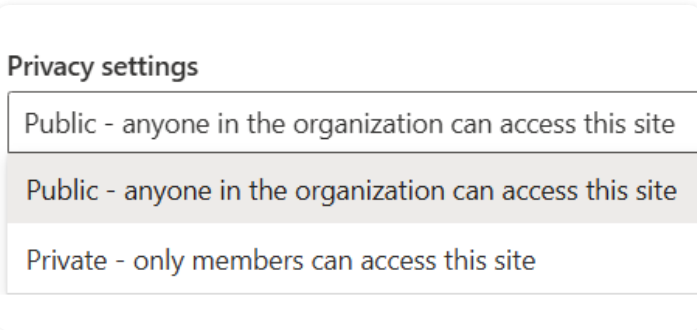


SharePoint sites

Option to share more broadly via link

Highest risk of oversharing in Microsoft 365 Copilot

Common causes of Copilot oversharing in SharePoint



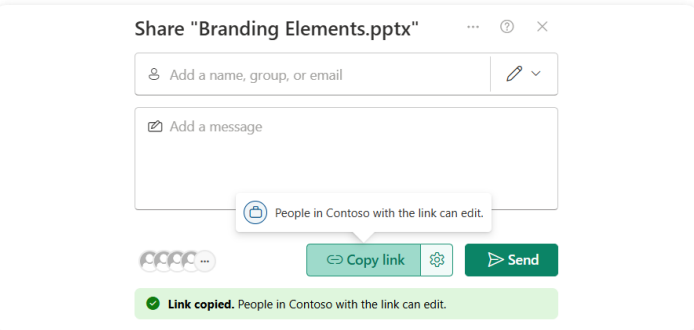
Privacy settings

Public - anyone in the organization can access this site

Public - anyone in the organization can access this site

Private - only members can access this site

Site privacy set to public



Share "Branding Elements.pptx"

Add a name, group, or email

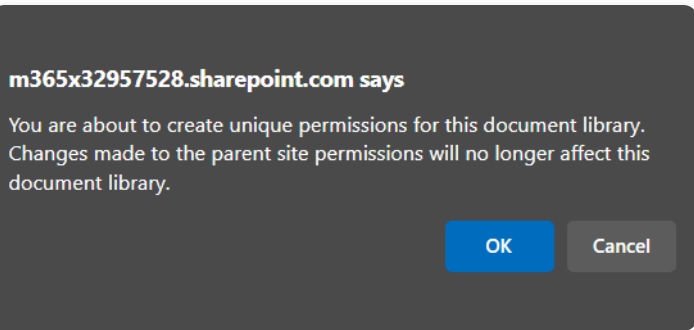
Add a message

People in Contoso with the link can edit.

Copy link Send

Link copied. People in Contoso with the link can edit.

Default sharing option is everyone

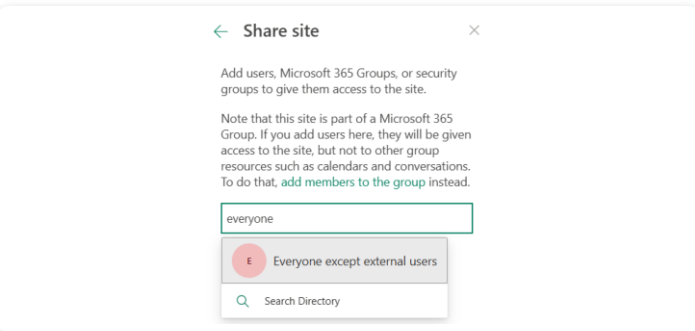


m365x32957528.sharepoint.com says

You are about to create unique permissions for this document library. Changes made to the parent site permissions will no longer affect this document library.

OK Cancel

Broken permission inheritance



Share site

Add users, Microsoft 365 Groups, or security groups to give them access to the site.

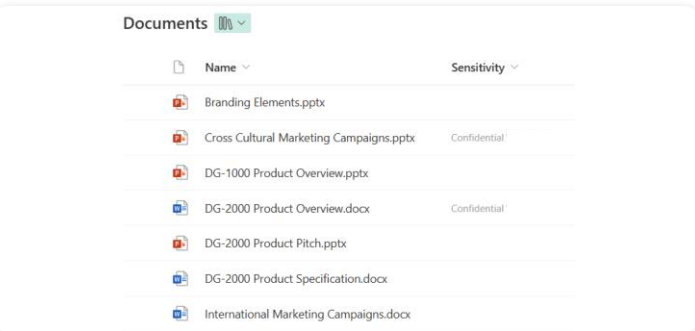
Note that this site is part of a Microsoft 365 Group. If you add users here, they will be given access to the site, but not to other group resources such as calendars and conversations. To do that, add members to the group instead.

everyone

Everyone except external users

Search Directory

Use of "everyone except external users" domain group



Documents

Name	Sensitivity
Branding Elements.pptx	
Cross Cultural Marketing Campaigns.pptx	Confidential
DG-1000 Product Overview.pptx	
DG-2000 Product Overview.docx	Confidential
DG-2000 Product Pitch.pptx	
DG-2000 Product Specification.docx	
International Marketing Campaigns.docx	

Sites and files without sensitivity labels

Two powerful tools to address oversharing



Microsoft 365 Copilot

Now powered by SharePoint Advanced Management

Provides SharePoint site management and content governance capabilities



Microsoft Purview

Provides security, compliance, and governance across data and files

Govern Copilot content access and quality with SAM

SharePoint Advanced Management enhances content governance for SharePoint and OneDrive, streamlining content management and preventing content sprawl and oversharing



Content Sprawl



Content Oversharing
prevention



Site Lifecycle

Secure and govern Copilot data with Microsoft Purview



with



Security



Compliance



Privacy



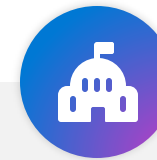
Responsible AI



Discover
AI risks












Protect
sensitive data



Govern
Copilot usage

Prevent Data Oversharing | Data Leaks | Non-Compliant Usage

Address internal user oversharing concerns for M365 Copilot deployment

	Pilot (optional) 	Deploy (at scale) 	Operate 
Activities	<ul style="list-style-type: none"> Identify most popular sites & assess oversharing Grant Copilot access to popular, low risk sites Turn on proactive audit and protection 	<ul style="list-style-type: none"> Discover oversharing risks Restrict sensitive info from Copilot access and/or processing Increase site privacy 	<ul style="list-style-type: none"> Further reduce risk and simplify oversight Further secure sensitive data Improve Copilot responses
Outcomes	 Deploy copilot to sub-set of users with up to 100 sites	 Copilot fully deployed in your organization	 Continuous improvement of data security practices
Effort*	 2-4 days	 2-4 weeks	 More than one month

*Suggested efforts should be reviewed into timelines based on your tenant size and organizational complexity

Microsoft deployment blueprint to address internal oversharing in Microsoft 365 Copilot

Customers with E3 **Foundational**

LEGEND 1 - Copilot and SharePoint Adv. Mgt. 2 - OEI/MEI

Address internal user oversharing concerns in Microsoft 365 Copilot

Realize value quickly with Copilot by reviewing potential content sharing risks and optionally enabling Restricted SharePoint Search to address risk to enable full Copilot deployment

Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot	Deploy	Operate
Effort	2-4 days	2-4 weeks	1+ months
Deployment steps	<ol style="list-style-type: none"> 1. Identify the most popular sites & assess oversharing <ul style="list-style-type: none"> Export the top 100 most used sites from SPO admin center Run SAM permission state report¹ Use Purview Content Explorer to view which sites contain sensitive information types (SITs)² 2. Grant Copilot access to popular, low risk sites <ul style="list-style-type: none"> Cross reference the report results from SAM and Content Explorer with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery^{1,3} Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identified¹ 3. Turn on proactive audit and protection <ul style="list-style-type: none"> Turn Off EEEU (everyone except external users) at the tenant level² Turn on Audit and view Copilot interaction activity reports and charts^{1,2} Turn on audit-mode oversharing SPO DLP policy to detect anyone sharing links for labeled and unlabeled data² 	<ol style="list-style-type: none"> 1. Discover oversharing risks <ul style="list-style-type: none"> Use permission state report with SITs to flag sites and files that are potentially overshared (Includes: EEEU, company shared links)¹ Identify Copilot agent insights & take actions¹ 2. Restrict sensitive info from Copilot access and/or processing <ul style="list-style-type: none"> Initiate Access Review for all sites that are overshared¹ Apply restricted access control (RAC) on business-critical sites¹ Exclude critical sites from Copilot reasoning over them¹ 3. Increase site privacy <ul style="list-style-type: none"> Publish labels to Office apps, Container/Sites, Outlook for manual data protection by user² Use site labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members² Turn on enforce-mode oversharing SPO DLP policy to restrict access to sensitive data exposure & starting remediating them² Disable RSS (if enabled) to allow full Copilot experience¹ 	<ol style="list-style-type: none"> 1. Further reduce risk and simplify oversight <ul style="list-style-type: none"> Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners¹ Automate SAM permission state report to maintain permissions hygiene¹ <ul style="list-style-type: none"> Automate permission reports and actions to maintain permission hygiene¹ Regularly review oversharing reports and restrict access as needed¹ Proactively avoid oversharing by applying RAC at site provisioning¹ Periodically review inactive sites and take necessary action¹ Control site provisioning by allowing creation for users that complete training¹ <ul style="list-style-type: none"> Use change history to identify site changes that may cause oversharing¹ Continuously manage all your oversharing DLP alerts via the Microsoft Purview Portal² 2. Secure Copilot responses <ul style="list-style-type: none"> Reduce risk by remediating alerts for overshared documents from the SPO DLP policy and applying sensitive labels² 3. Improve Copilot responses <ul style="list-style-type: none"> Setup retention/deletion policies for SharePoint to reduce data surface² Identify inactive sites, then restrict access or delete¹

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel

Customers with E5 **Optimized**

LEGEND 1 - Copilot and SharePoint Adv. Mgt. 2 - OEI/MEI 3 - MES/ES Compliance

Address internal oversharing concerns in Microsoft 365 Copilot

Realize value quickly with Copilot by reviewing potential content sharing risks and optionally enabling Restricted SharePoint Search to address risk to enable full Copilot deployment

Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot	Deploy	Operate
Effort	2-4 days	2-4 weeks	1+ months
Deployment steps	<ol style="list-style-type: none"> 1. Identify the most popular sites & assess oversharing <ul style="list-style-type: none"> Export the top 100 most used sites from SPO admin center Run SAM permission state report¹ Run the Purview DSPM Oversharing posture assessment to gain visibility into all data at risk of Copilot access, pivoted on labels and sensitive information types² 2. Grant Copilot access to popular, low risk sites <ul style="list-style-type: none"> Cross reference the report results from SAM and Purview DSPM for AI with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery^{1,3} Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identified¹ 3. Turn on proactive audit and protection <ul style="list-style-type: none"> Turn Off EEEU (everyone except external users) at the tenant level² Turn on Purview Audit and view Copilot interaction activity reports and charts^{1,2} Turn on proactive analysis for sensitive data handling with prompts and responses with Purview Communications Compliance³ Turn on audit-mode oversharing SPO Purview DLP policy to detect anyone sharing links for labeled and unlabeled data² 	<ol style="list-style-type: none"> 1. Discover oversharing risks <ul style="list-style-type: none"> Use DAG permission state report with SITs to flag sites and files that are potentially overshared (Includes: EEEU, company shared links)¹ Identify Copilot agent insights & take actions¹ Create customized Purview DSPM Oversharing posture assessments to scale out data security actions, pivoted on labels and sensitive information types² 2. Restrict sensitive info from Copilot access and/or processing <ul style="list-style-type: none"> Initiate SAM Access Review for all sites that are overshared¹ Apply SAM restricted access control (RAC) on business-critical sites¹ Exclude critical sites from Copilot reasoning over them with SAM Restricted Content Discovery (RCD)¹ Publish sensitivity labels with Purview Information Protection to Office apps, Container/Sites, Outlook for manual data protection by user² Exclude Copilot from summarizing sensitive content via sensitivity labels² 3. Increase site privacy <ul style="list-style-type: none"> Use site sensitivity labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members² Apply default site library sensitivity labels to protect new and modified unlabeled documents² Turn on enforce-mode oversharing SPO Purview DLP policy to restrict access to sensitive data exposure & starting remediating them² Disable RSS (if enabled) to allow full Copilot experience¹ 	<ol style="list-style-type: none"> 1. Further reduce risk and simplify oversight <ul style="list-style-type: none"> Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners¹ Automate SAM permission state report to maintain permissions hygiene¹ <ul style="list-style-type: none"> Automate permission reports and actions to maintain permission hygiene¹ Regularly review oversharing reports and restrict access as needed¹ Proactively avoid oversharing by applying RAC at site provisioning¹ Periodically review ownerless sites and take necessary action¹ Control site provisioning by allowing creation for users that complete training¹ <ul style="list-style-type: none"> Use change history to identify site changes that may cause oversharing¹ Routinely run Purview DSPM Oversharing posture assessments to scale out data security actions, pivoted on labels and sensitive information types² Continuously manage all your oversharing Purview DLP alerts via incidents with Microsoft Defender XDR incident queue³ View risky user activity in context of oversharing Purview DLP incidents³ 2. Further secure sensitive data <ul style="list-style-type: none"> Automatically label new documents and prevent them from oversharing with run time auto-labeling policy, starting with client-side policies and extend to service-side policies³ Reduce risk by remediating alerts for overshared documents from the SPO Purview DLP policy by applying sensitive labels and disabling anyone access² 3. Improve Copilot responses <ul style="list-style-type: none"> Setup Purview retention/deletion policies for SharePoint to reduce data surface² Identify inactive sites with SAM, then restrict access or delete¹

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel

Get the blueprint:
<https://aka.ms/Copilot/OversharingBlueprintLearn>

Envision IT Copilot Readiness Roadmap



Consolidate

- Unified Data Platform
 - Migrating from file shares and on-premises SharePoint
 - Ensures all data is accessible and manageable
- Enhanced Data Visibility
 - Leverages advanced features of Microsoft 365
 - Includes enhanced security and collaboration tools
- Informed Decision Making
 - All data in one place aids in making better decisions

Inventory

Third-Party Tools

ShareGate
by **workleap**

 **AvePoint**
Insights
For Microsoft 365

 **Orchestra**


Rencore
governance

Lightning**Tools**

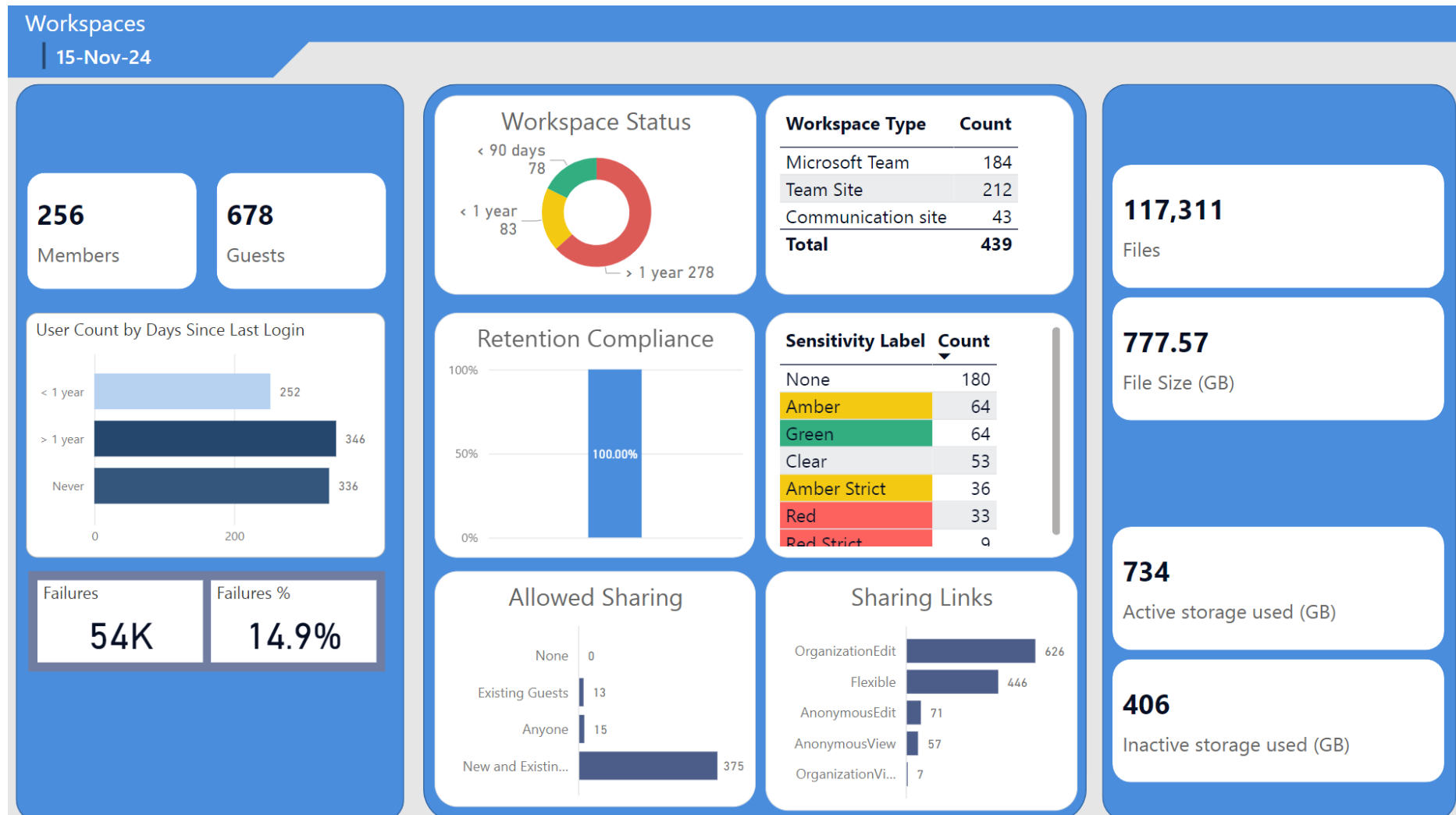
 **bindtuning**

 **envision IT**

 **Syskit**

 **BCC**

Envision IT M365 Tenant Dashboard



M365 Tenant Dashboard | Envision IT

Clean, Secure, and Label

Clean

- Delete or archive stale content
- Retention policies

Secure

- Default sharing
- Private versus public
- Broken permissions
- Everyone

Label

- Workspace and container labels
- Document labels



**Microsoft
Purview**



Data Security



For information and cybersecurity teams



**Data
Governance**



For data consumers, data engineers, data officers



**Risk &
Compliance**



For risk, compliance, and legal teams

Purview Labels

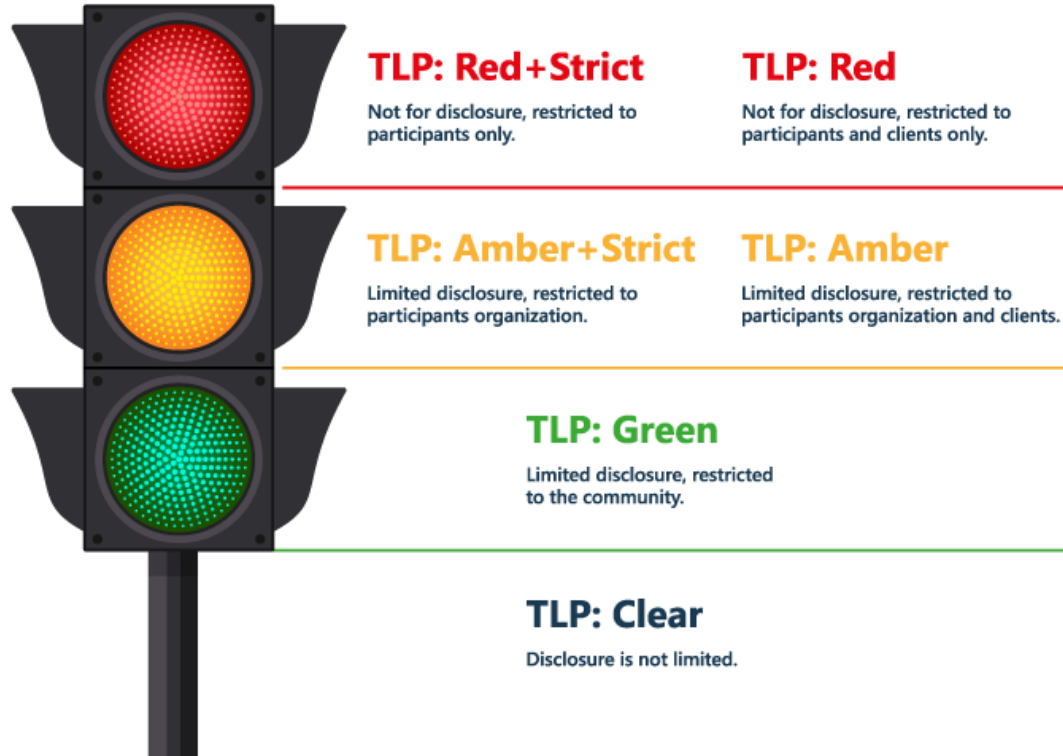
Retention

- Manage lifecycle of data
- Specify how long content should be kept and then what actions should be taken
- Ensure compliance with regulations and internal policies
- Typically many (could be hundreds) of labels

Sensitivity

- Designed to protect sensitive information
- Classifying and secure
- Control how content is handled and shared
- Small number of labels

Sensitivity Labels



- Apply labels to data to enforce protection policies
- Control how content is handled and shared
- Designed to protect sensitive information

AI-Powered Classifiers



- Utilize AI to accurately classify data based on content and context
- Enhance the precision of data protection measures
- An emerging technology

Default Labels for Document Libraries

Library settings

Name *

Documents

Description

Default sensitivity labels ⓘ

Choose a default sensitivity label that will be applied to all the Office or PDF files within your library. This will only be applied to newly created or edited files. [Learn more](#)

General

[More library settings](#)

Save Cancel

- Traditionally required E5 or E5 Compliance licenses
- Now also part of SharePoint Advanced Management
- Auto-labelling is still E5
- Only applies to new or edited documents
- Can also be applied to existing documents with PowerShell

SharePoint Advanced Management



**Manage
content sprawl**



**Prevent
oversharing**



**Control Copilot
access to content**



**Manage
content lifecycle**

- \$3 USD / user / month
- Need to license 100% of users, including F1/F3

- Free for the tenant if at least 1 Copilot license purchased
- Rolling out Jan – Mar 2025
- Trial available now

[Microsoft SharePoint Premium - SharePoint Advanced Management overview - SharePoint in Microsoft 365 | Microsoft Learn](#)



Up Next:
Addressing
oversharing at
site level

1

Identify overshared sites with **Permission State Report**

2

Enlist site owners to address permissions and access with **Site Access Review**

3

Temporarily lock down site access to clean up permissions with **Restricted Access Control**

4

Prevent Copilot from accessing sensitive sites with **Restricted Content Discovery**

- Home
- Sites
 - Active sites
 - Deleted sites
- Containers
- Policies
- Settings
- Content services
- Migration
- Reports
 - Change history
 - Data access governance
 - OneDrive accounts
- Advanced
 - More features
- Advanced management PRO
- Customize navigation
- Show all



Welcome to data access governance

These new reports help you maintain the security and compliance of your data in SharePoint.



Next

Reports My review requests

Sharing links

Identify potential oversharing by monitoring sites where users created new sharing links in SharePoint.

View reports

Sensitivity labels applied to files

Monitor sensitive content by reviewing the sites where sensitive files are stored and the policies applied to these sites.

View reports

Content shared with 'Everyone except external users'

Discover potential oversharing by reviewing content shared with 'Everyone except external users'. Send site owners requests to review access permissions of their content based on the report.

View reports



- Home
- Sites
 - Active sites
 - Deleted sites
- Containers
- Policies
- Settings
- Content services
- Migration
- Reports
 - Change history
 - Data access governance
 - OneDrive accounts
- Advanced
- More features

Data access governance > Sharing links

Sharing links

Use these reports to review SharePoint sites where users created the most sharing links for files and folders in the last 28 days. To get the latest data for a report, you must run it, which can take a few hours.
[Learn more about these reports](#)

▶ Run all ↻ Refresh status

<input type="checkbox"/>	Report name	Status	Sites found
<input type="checkbox"/>	"Anyone" links	Updated 2 days ago	-
<input type="checkbox"/>	"People in your organization" links	Updated 2 days ago	-
<input type="checkbox"/>	"Specific people" links shared externally	Updated 2 days ago	-

Refresh status
Help

- Home
- Sites
 - Active sites
 - Deleted sites
- Containers
- Policies
- Settings
- Content services
- Migration
- Reports
 - Change history
 - Data access governance
 - OneDrive accounts
- Advanced
- More features
- Advanced management PRO
- Customize navigation

Sensitivity labels applied to files

Use these .csv reports to review up to 10,000 SharePoint sites that have the most Office files with specific sensitivity labels applied. To get the latest data for a label, add a report for it or run the report if it already exists.

[Learn more about these reports](#)

+ Add a report ▶ Run all ↻ Refresh status

<input type="checkbox"/>	Report name	Status	Download report
<input type="checkbox"/>	Sites with files labeled "TLP Amber"	Updated 19 days ago	Download
<input type="checkbox"/>	Sites with files labeled "TLP Amber (Strict)"	Updated 19 days ago	Download
<input type="checkbox"/>	Sites with files labeled "TLP Clear"	Updated 19 days ago	Download
<input type="checkbox"/>	Sites with files labeled "TLP Green"	Updated 19 days ago	Download
<input type="checkbox"/>	Sites with files labeled "TLP Red"	Updated 19 days ago	Download
<input type="checkbox"/>	Sites with files labeled "TLP Red (Strict)"	Updated 19 days ago	Download

Refresh status

Help

- ☰
- 🏠 Home
- 📁 Sites ^
 - Active sites
 - Deleted sites
- 📦 Containers v
- ⚙️ Policies v
- ⚙️ Settings
- 📄 Content services v
- ☁ Migration
- 📈 Reports ^
 - Change history
 - Data access governance**
 - OneDrive accounts
- ⚙️ Advanced v
- ⋮ More features

Data access governance > Content shared with 'Everyone except external users'

Content shared with 'Everyone except external users'

Use these reports to view sites where 'Everyone except external users' was added as a site member, or view sites with specific content, like files, folders, and lists, shared with 'Everyone except external users'. Reports include data from the last 28 days. To get the latest data, run the report, which may take a few hours.

[Learn more about these reports](#)

+ Create report
 ▶ Run all
↻ Refresh status

<input type="checkbox"/>	Report name	Status	Report type (i)	Date rang
<input type="checkbox"/>	<u>All Sites</u>	Updated 2 days ago	Sites with specific content shared	Nov 4, 202

Restricted Access Control (RAC)



for SharePoint & OneDrive

RAC (Restricted access control) policy can be set at the site level. Even if individual files/folders have broken inheritance and over-shared, only RAC allowed users can access

Copilot honors RAC policy!

Microsoft 365 group-connected sites, Non-group SharePoint sites, Teams sites, Shared channel sites, OneDrive sites

Generally available

The screenshot shows the SharePoint admin center interface for 'Contoso Energy'. The main view is 'Snapshot till March', which displays a list of sites where the number of users across all permission scopes (inherited and broken) exceeds a threshold. The table below shows the following data:

Name	URL	Site access review status	Teams	Total permissioned users	Count of users
Contoso HR	./teams/contosohr	—	1	22334	312
Contoso Marketing	./teams/contosomar	Pending	1	15698	296
Contoso Finance	./sites/contosofin	Completed	-	11237	167
Contoso Giving	./sites/contosogiv	-	-	10245	145
Contoso team	./sites/contosoteam	-	-	8530	124
Contoso Vac	./sites/contosovac	-	-	6054	72
Contoso HRA	./teams/contosohra	-	1	3996	2416
Contoso Media	./sites/contosomedia	-	-	2804	38
Contoso in house	./sites/contosoinh	-	-	1890	32
Contoso infra	./sites/contosoinfra	-	-	1487	23
Contoso design	./sites/contosodesign	-	-	1329	21
Contoso leaders	./teams/contosolead	-	1	1127	647
Contoso data	./teams/contosodata	-	1	1038	721

The 'Restricted site access' modal window is open, showing the option to 'Restrict SharePoint site access to only users in specified groups' (checked). The 'Add group' search box is populated with the following groups:

- Contoso Financial Council
- Contoso Tech
- Contoso Marketing
- Contoso HR

[Restrict SharePoint site access with Microsoft 365 groups and Entra security groups - SharePoint in Microsoft 365](#)
[Microsoft Learn](#)

Restricted Content Discovery (RCD)

Advanced access control to exclude sites from Copilot

1

Use this [site-level setting Restricted Content Discoverability](#) to restrict content discoverability via Copilot and Org-wide search

2

SharePoint Admin sets this property to a site via PS cmdlet

3

There is no change to the site's permissions!
> Users continue to have physical access

4

Contents of the site gets reindexed** – as a result contents are security trimmed and [not discoverable via Copilot and tenant-wide search](#)

```
>Set-SPOSite -Identity <site-url> -RestrictContentOrgWideSearch $true
```

Public preview

[Restrict discovery of SharePoint sites and content - SharePoint in Microsoft 365 | Microsoft Learn](#)



Up Next: Addressing oversharing at file level

1

Identify overshared files and sites with new **Oversharing assessments** surfaced in **Data Security Posture Management for AI**

2

Keep Copilot from using labeled files in prompts responses with **Data Loss Prevention for M365 Copilot and Information Protection sensitivity labels**

Train

- Training your users, not the LLM
- Use cases
- Prompt engineering
 - [Microsoft Copilot for Microsoft 365 Tips, Tricks & Prompts - Microsoft UK](#)
 - [Craft effective prompts for Microsoft 365 Copilot - Training | Microsoft Learn](#)
 - [Copilot Prompt Gallery](#)
 - [10 Prompt Strategies in Copilot for Microsoft 365 | LinkedIn](#)

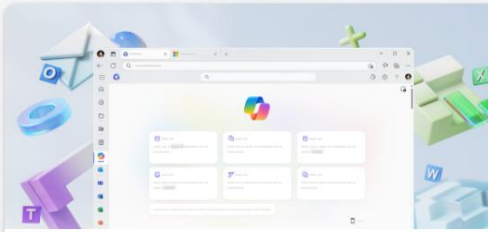
- Copilot
- Activity
- Chat
- Calendar
- Calls
- OneDrive
- Viva Conne...
- Orchestr...
- Approvals
- Power BI
- Viva Insights
- ...
- Apps

← Back to Viva Insights Home

Share

Microsoft Copilot Dashboard

- Readiness
- Adoption
- Impact
- Learning**




Microsoft

Get started with Microsoft Copilot

Find all the Microsoft 365 Copilot documentation.

[Read](#)

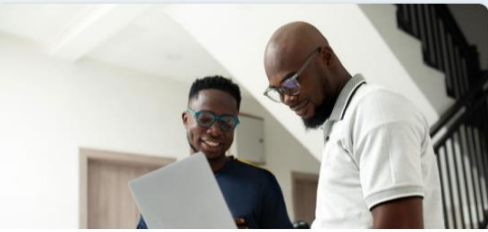


Microsoft

Learn how Microsoft integrates security and privacy into Copilot

Get an overview about how Copilot uses and protects organisational data.

[Read](#)



Microsoft

Explore how Copilot works with Microsoft Mechanics

Watch detailed explanations of Microsoft 365 Copilot and see it in action.


[Watch](#)



Microsoft

Learn how Copilot can improve workplace productivity

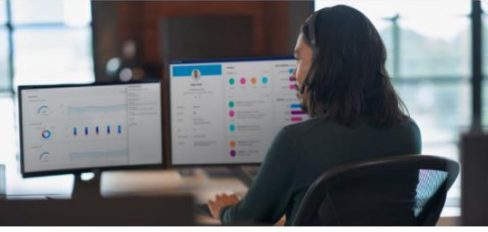
Read up on Microsoft's latest survey results that show Copilot users report higher productivity.



Github blog

Explore the impact of Copilot on code quality at GitHub

Learn more about how code quality can be improved when Github Copilot is enabled.



Microsoft

Dive into the art and science of working with AI

Learn what business leaders need to know to get their organisations and people ready.

Governance

- Viva Insights
- Microsoft Purview Compliance Manager - DPSM
 - Helps you automatically assess and manage compliance across a multcloud environment
 - Features
 - Assessments
 - Compliance score
 - Automatic and manual testing
 - Document evidence
 - Third party tools

← Back to Viva Insights Home

Share ▾

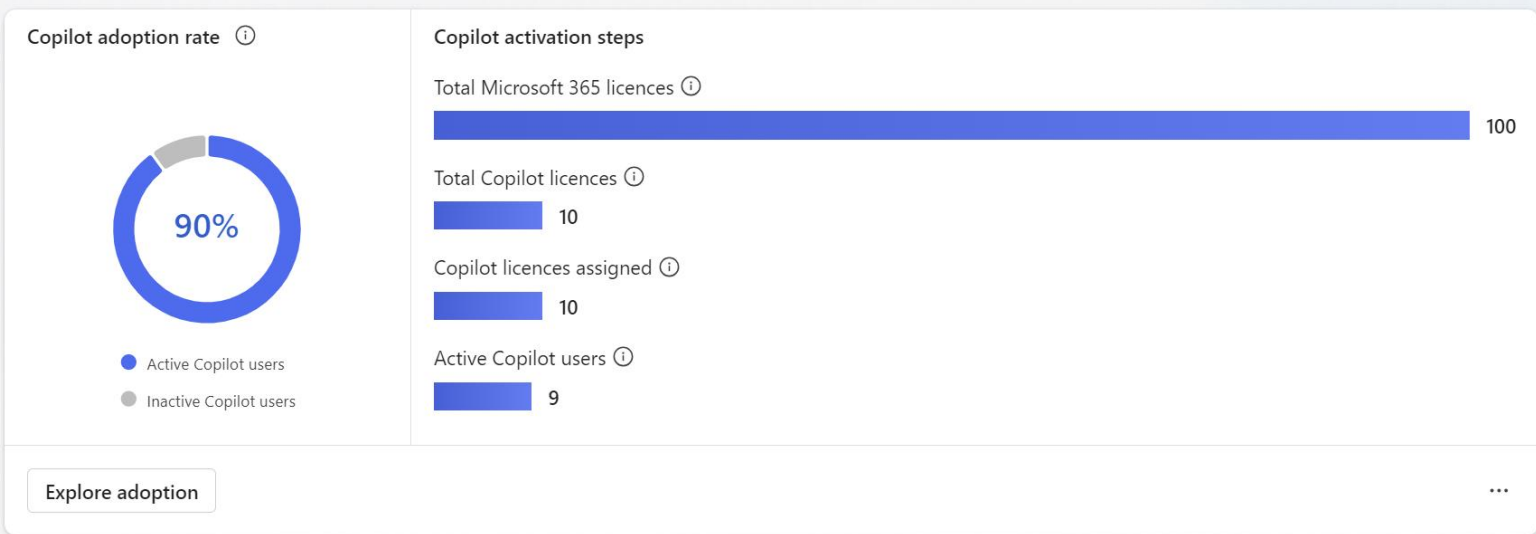
Microsoft Copilot Dashboard

Readiness Adoption Impact Learning

Activate Microsoft 365 Copilot for your organisation

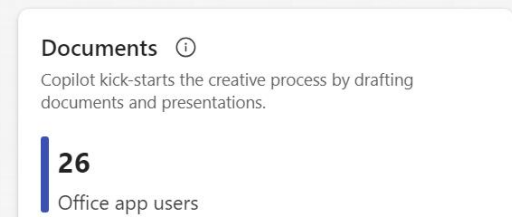
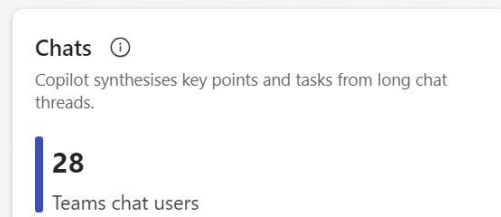
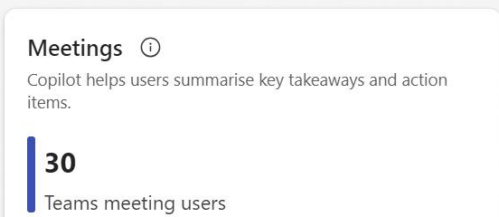
Any user with a prerequisite Office 365 or Microsoft 365 licence can be assigned a Copilot licence.

Time period: 4 weeks (2 Nov – 29 Nov)



How Copilot can transform your work

Assess how Copilot can bring value to Microsoft 365 app users in your organisation. [Read the research](#)



- Home
- Solutions
- Learn
- Settings
- DSPM for AI
 - Overview
 - Recommendations
 - Reports
 - Policies
 - Activity explorer**
 - Data assessments Preview
- Compliance Manager

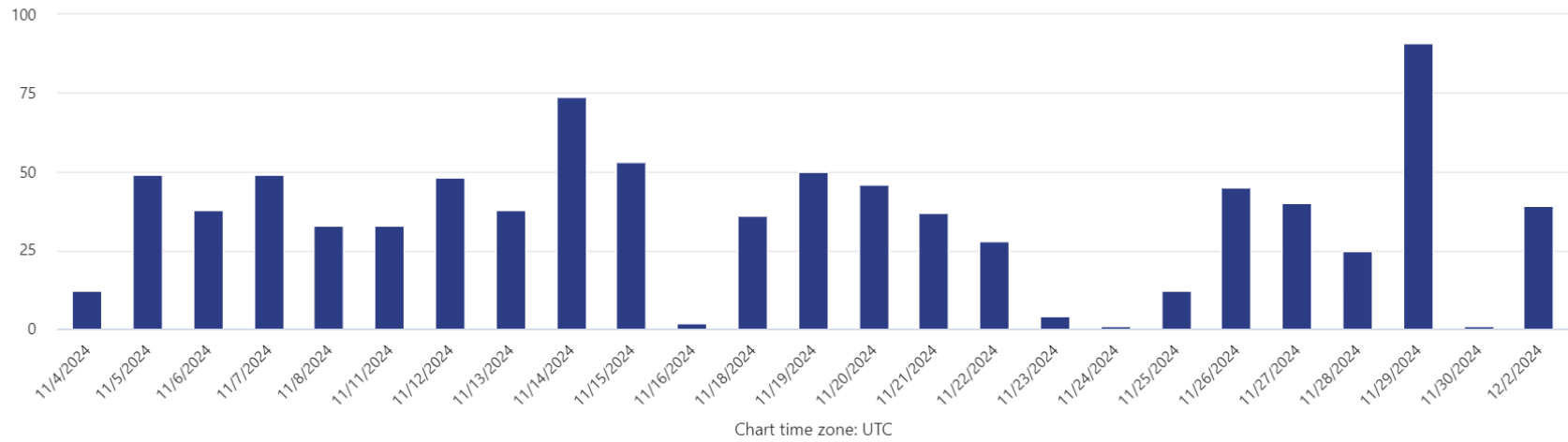
Additional permissions required. Your role can't view AI Visits or user risk levels. For permission, ask an administrator to change your role. [Learn more about roles](#)

Activity explorer

Review AI activity including AI interactions (prompts and response), activity with sensitive info types, and more.

Filters:

- Timestamp: 11/3/2024-12/2/2024
- Activity type: AI Interaction
- AI app category: Microsoft Copilot Experiences
- App: Any
- App accessed in: Any
- User: Any
- Sensitive info type: Any
- Resources accessed: Any
- Sensitive files referenced: Any
- Scope: Any
- Reset all



Export 884 items

<input type="checkbox"/>	Activity type	User	Timestamp (UTC)	AI app category	App	App accessed in	Sensitive info type	Resources access...
<input type="checkbox"/>	AI Interaction	pcarson@envisionit.com	Dec 2, 2024 10:25 PM	Microsoft Copilot...		Outlook		Yes
<input type="checkbox"/>	AI Interaction	rhawks@envisionit.com	Dec 2, 2024 9:51 PM	Microsoft Copilot...		Outlook		Yes
<input type="checkbox"/>	AI Interaction	rhawks@envisionit.com	Dec 2, 2024 9:43 PM	Microsoft Copilot...		Outlook		Yes

3 Key Takeaways

1

AI Is Coming – Either Under Your Control or Not

2

Data Needs to Be Prepared Before You Turn on Copilot

3

Start with Tenant Reporting and Analysis

Thank you!

Any Questions?