



# Microsoft 365 Copilot Technical Readiness Workshop



# Our Discussion Today

1 Art of the Possible

---

2 Discovery

---

3 Design

---

4 Closing



## Executive Summary

e360's Microsoft 365 Copilot Technical Readiness Workshop is a structured program designed to enable an organization and its employees for the AI transformation journey. It includes a comprehensive agenda covering:

- Art of the Possible
- Licensing
- Data Governance
- Technical Readiness
- User Enablement

## Why e360?

We are an award-winning IT consultancy specializing in cybersecurity, cloud, automation, end-user computing, software defined infrastructure, and core infrastructure.

Our organization proudly boast **30+ years** of Microsoft consulting experience, with Microsoft Advanced Specializations in Adoption and Change Management, Azure Infrastructure and Database Migrations, and Azure Virtual Desktops.



The age of Copilots  
has arrived.



# Copilot for Microsoft 365

Unlock productivity and unleash creativity

Natural Language



+



+



+



Large Language  
Models

Microsoft Graph  
- Your Data -

Microsoft 365  
Apps

The  
Internet

# Copilot for Microsoft 365 is transforming work

60%

of leaders say a lack of innovation or breakthrough ideas is a concern

64%

of people have struggled with finding time and energy to get their work done

70%

of people indicated they would delegate as much as possible to AI to lessen their workloads



68%

said Copilot improved the quality of their work

70%

said Copilot made them more productive

77%

said they didn't want to give Copilot up

# Copilot for Microsoft 365

1



Security  
foundation

2



AI at  
work

3



Culture  
shift







# **Microsoft 365 Copilot Technical Readiness Workshop - Discovery**

# Licensing Landscape



- Review current licensing model
- Identify areas to optimize licensing for Copilot
- Discuss current entitlements and how licenses are procured
- Determine best licensing model to align with desired objectives



# eDiscovery Premium for Monitoring



- Review eDiscovery capabilities for monitoring compliance and risk management
- Learn how to use eDiscovery to search for content across Microsoft 365
- Discover the benefits of eDiscovery for legal and compliance teams



# Data Loss Prevention Review



- Explore how Data Loss Prevention (DLP) can protect sensitive information
- Learn how to create and manage DLP policies
- Understand how DLP integrates with Microsoft 365 apps and services

# Retention Policies Overview



- Learn about retention policies and how they can help manage your information lifecycle
- Understand how to create and manage retention policies
- Explore the benefits of retention policies for compliance and risk management



# Purview Audit



- Learn about Purview and how it can help you discover and manage sensitive data
- Understand how Purview integrates with Microsoft 365 and other data sources
- Explore the benefits of using Purview for data governance and compliance





# Restricted SharePoint Search



This is intended as a temporary solution to give you time to review and audit site permissions, while implementing robust data security solutions from Microsoft Purview and content management with SharePoint Advanced Management.

- Restricted SharePoint Search is designed for organizations particularly concerned about unintentional oversharing of content
- When enabled, Copilot experiences and organization-wide search are limited to a select set of SharePoint sites, as well as the individual user's files and content

## IMPACT

Restricted SharePoint Search disables organization-wide search, while allowing you to select sites that you trust. This means users in your organization can use Copilot to reason over:

- An allowed list of curated SharePoint sites set up by admins (up to 100 SharePoint sites), honoring existing permissions on a site
- Users' OneDrive for Business, chats they are part of, emails they send and receive, calendars to which they have access, etc.
- Files that are shared with, and accessed by users
- Content from users' frequently visited sites

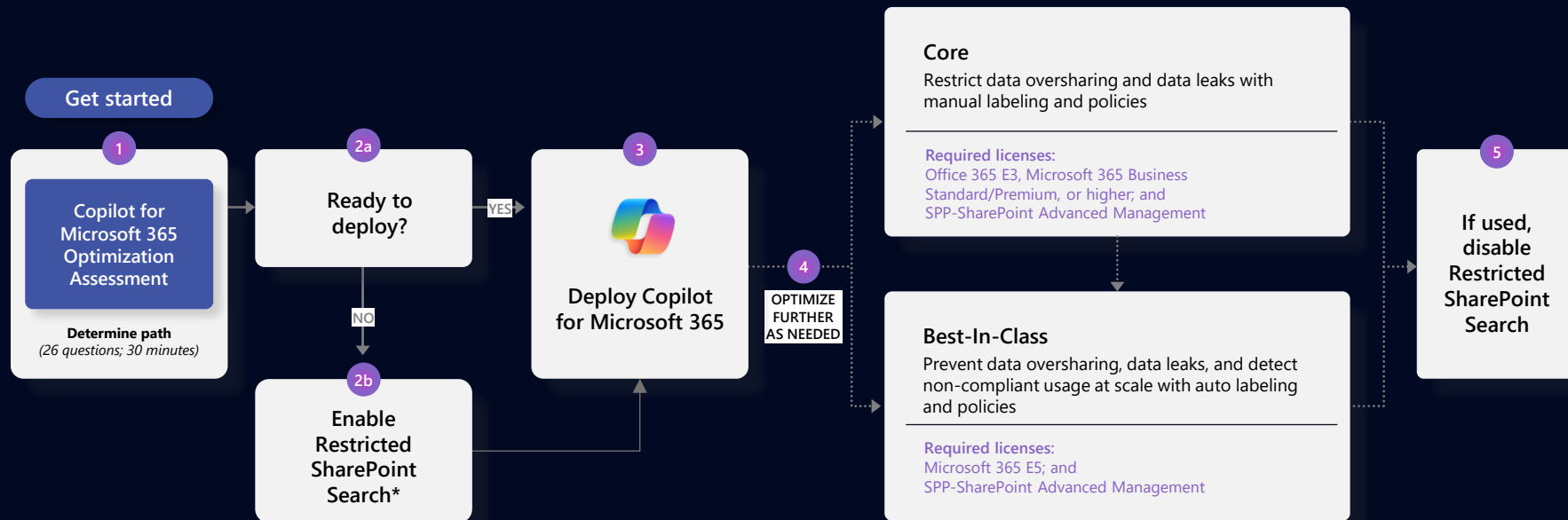
Access this [blog](#) for more info.

## PREREQUISITES

- Available to tenants with Copilot for Microsoft 365 subscriptions
- Activation requires Global/Tenant/SharePoint admin rights



# Apply appropriate Data Security controls



\*Restricted SharePoint Search will limit Copilot for Microsoft 365 experiences and organization-wide search. It is a temporary option which gives you time to address oversharing concerns while getting started on your Copilot journey





# Microsoft 365 Copilot Technical Readiness Workshop - Design


# Copilot for Microsoft 365 implementation



## Copilot implementation

### Copilot essentials checklist

- ✓ Sponsor
- ✓ Scenarios
- ✓ Security

  
You are here

### User enablement

Prepare organization and employees for AI transformation journey

Workstreams support each other for maximum value and ROI

### Technical readiness

Address technical deployment and optimization, including governance, security, compliance, and management

Leadership journey 



# Copilot for Microsoft 365



## Implementation overview

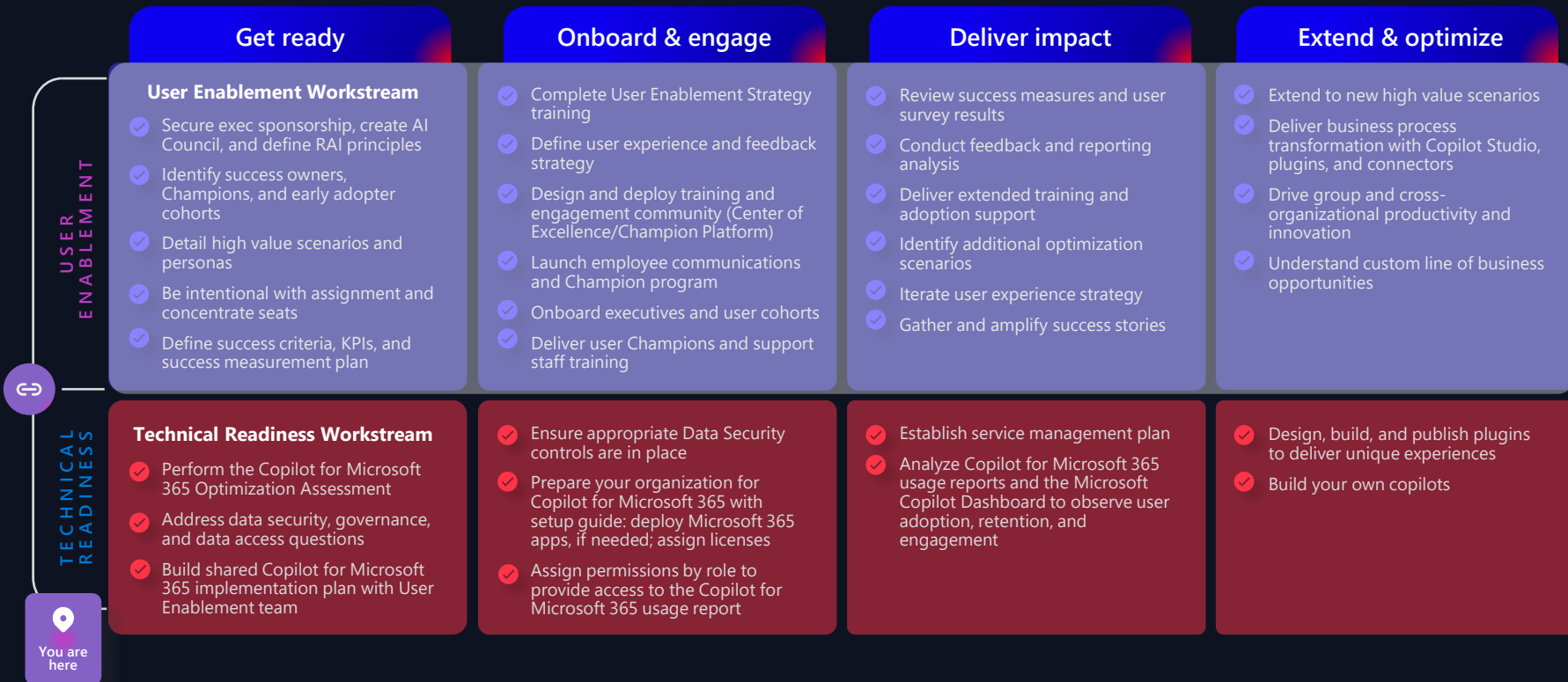




# Copilot for Microsoft 365



## Implementation overview





# Sample Implementation Project Summary

- First 30 days
- 30-60 days
- Recurring tasks

## Shared milestone view





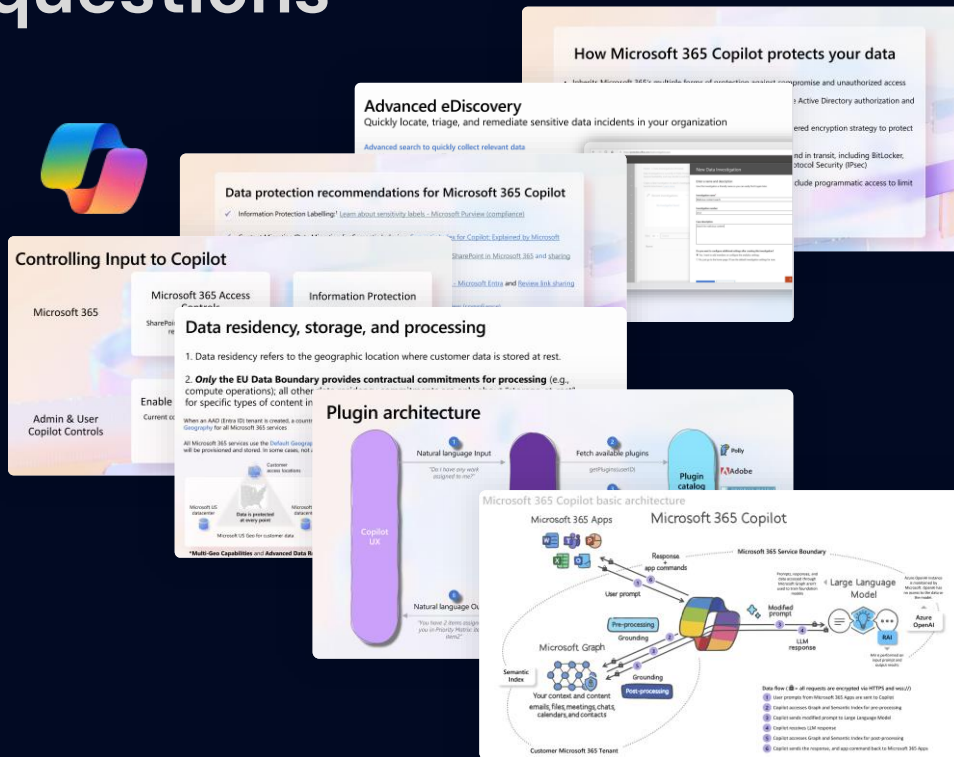
# Address security, governance, and data access questions



Shared activity

Access the [IT Professional admin resources](#) for additional documentation and to help address deeper questions you may have about Copilot for Microsoft 365, such as:

- How does [Copilot with commercial data protection](#) AI-powered chat for the web, work? How is it different from Copilot for Microsoft 365?
- Is this AI-powered chat available for [eligible Entra ID users](#) at no additional charge?
- How does Copilot for Microsoft 365 work?
- How does the Semantic Index work?
- Where does my data go?
- How do Copilot plugins and connectors work?
- What permissions and policies should I think about to prepare?
- What is Microsoft's responsible AI commitment?
- AND MORE....



# Defender XDR



Microsoft Defender XDR (Extended Detection and Response) is a comprehensive security solution designed to protect various aspects of an organization's digital environment. It integrates detection, prevention, investigation, and response capabilities across multiple domains, including endpoints, identities, email, and cloud applications.

Key features of Microsoft Defender XDR include:

- **Unified Threat Protection:** It coordinates threat detection and response across different security layers, providing a holistic view of potential threats.
- **Automation and AI:** Leveraging artificial intelligence and automation, it can automatically stop certain types of attacks and remediate affected assets.
- **Integration with Microsoft Security Products:** It uses information from other Microsoft security tools to enhance its effectiveness<sup>1</sup>.
- **Role-Based Access Control (RBAC):** It includes a unified RBAC model to ensure that users have the least privilege necessary for their roles.

Helps organizations streamline their security operations and improve their overall security posture.





## Licensing for Securing and governing Copilot for Microsoft 365

### Baseline



Copilot for Microsoft 365  
+ Office 365 E3

Multi-factor Authentication

Audit logging

### Core



Copilot for Microsoft 365  
+ Microsoft 365 E3  
+ SharePoint Advanced Management

Conditional Access

Manual sensitivity labels

Data loss prevention policies

Advanced SharePoint sitewide access  
controls and reporting

Unified endpoint management

### Best-in-class



Copilot for Microsoft 365  
+ Microsoft 365 E5\*

Conditional Access based on identity risk

Automatically apply sensitivity labels

Automatically remove inactive content

Prevent data leak on endpoint devices

Detect non-compliant usage

\*Microsoft 365 E5 does not include SharePoint Advanced Management





# Get started with Copilot for Microsoft 365

Required licenses:  
Office 365 E3 or higher

Follow the recommended activities to proceed with Copilot for Microsoft 365 deployment

Product	Deployment outcomes	Get started activities
<b>Copilot for Microsoft 365</b>	Evaluate data governance maturity and data security controls	<ul style="list-style-type: none"><li>Complete Copilot for Microsoft 365 <a href="#">Optimization Assessment</a></li><li>Based on the outcomes of the assessment determine your path forward</li></ul>
	Deploy Copilot for Microsoft 365	<ul style="list-style-type: none"><li>Follow the Microsoft Copilot for Microsoft 365 setup guide to proceed with the deployment steps</li><li>If there are any concerns about your data security, enable Restricted SharePoint Search</li><li>If enabled, update Restricted SharePoint Search allow list: configure up to 100 sites to be on the allow list of sites. Start with sites containing highly used unrestricted content.</li><li>FastTrack for Microsoft 365 can help you get started*</li></ul>
<b>Copilot with commercial data protection</b>	Enable commercial data protection in Copilot for all users in your organization	<ul style="list-style-type: none"><li>Log into Copilot on <a href="https://copilot.microsoft.com">copilot.microsoft.com</a> and flip the Work/Web toggle to Web. See if commercial data protection is enabled (look for green Protected pill by the user profile)</li><li>Review the <a href="#">Copilot with commercial data protection documentation</a> to ensure that commercial data protection is available for your users</li></ul>



# Continue to the Best-in-Class path as needed

Required licenses:  
Microsoft 365 E5; and SPP-SharePoint  
Advanced Management

Follow the recommended activities for the Best-in-Class path to achieve top-tier security posture

Product	Deployment outcomes	Best-in-Class activities
Copilot for Microsoft 365	If enabled, update Restricted SharePoint Search allow list	<ul style="list-style-type: none"><li>Configure up to 100 sites to be on the allow list of sites. Extend to sites containing restricted content, after validating permissions are set correctly</li></ul>
Microsoft SharePoint	Perform periodic reviews of oversharing reports, restrict access as appropriate	Run <a href="#">DAG reports</a> on a periodic basis and apply RAC to sites that appear to be overshared
	Perform periodic reviews of inactive sites, and take action	Apply <a href="#">inactive sites policy</a> and review resulting report
	Perform periodic reviews of Change History reports to discover when oversharing occurs	Run <a href="#">the change history report</a> and investigate changes to sharing in sites
Microsoft Purview	Apply a baseline protection to documents and containers (Microsoft 365 Groups, Microsoft Teams Sites) without the need for content inspection or manual labeling	<ul style="list-style-type: none"><li>Set a <a href="#">default sensitivity label</a> on SharePoint Online document libraries to protect documents without content inspection</li><li>Use <a href="#">Sensitivity labels to protect content</a> in Teams, Groups and SharePoint sites</li></ul>
	Dynamically protect sensitive information from being shared beyond its intended audience and reduce the risk of oversharing on across instant messages and user endpoints.	<ul style="list-style-type: none"><li>Create, deploy, and regularly evaluate <a href="#">Teams DLP Policies</a></li><li>Create, deploy, and regularly evaluate <a href="#">Endpoint DLP Policies</a></li><li>Create <a href="#">Adaptive Protection policies</a> to automatically <a href="#">assign DLP policies</a> based on the users identified risk level</li></ul>
	Automatically protect sensitive data access by Copilot for Microsoft 365 based on recommended conditions.	<ul style="list-style-type: none"><li><a href="#">Automatically apply sensitivity labels</a> to content in <a href="#">SharePoint, OneDrive, and Exchange</a></li><li>Automatically apply sensitivity labels to content within <a href="#">Office apps</a></li></ul>
	Automatically retain or dispose of documents based on their content	<a href="#">Automatically apply retention labels to content</a> that match specific conditions
	Detect sensitive data and non-compliant content in Copilot interactions	<a href="#">Create Communication Compliance</a> policies to regularly evaluate interactions with Copilot for Microsoft 365
	Preserve, collect, review, analyze, and export Copilot interactions	Use <a href="#">eDiscovery Premium</a> to <a href="#">search for and optionally delete Copilot interactions</a>





**Thank You!**