

THE  
**PARTNER**  
MASTERS



# Microsoft 365 Copilot

Readiness Assessment



# Copilot for Microsoft Readiness Assessment Goals

## Assess your business readiness

Identify your organization's ability to drive adoption of Copilot for Microsoft 365 through effective organizational sponsorship, strategy, and execution of capabilities of generative AI solutions.

## Technical Readiness

Identify any gaps and opportunities where technical changes must be implemented for your organization to successfully support enablement of Copilot for Microsoft 365.

## Cyber & Security Readiness

Identify where cyber and data security enhancements need to be made within your organization to support the safe and compliant adoption of Copilot for Microsoft 365 by your business users.



# Readiness Assessment Agenda



## Discovery

- Copilot for Microsoft 365 Optimization Assessment Workshop with sponsors and stakeholders 2 Hours
- AI readiness 1:1 interviews with 3 executive sponsors and stakeholders 30 mins each



## Technical Review (Workshops)

- Review SharePoint and Teams Configuration 3 Hours
- Review Data Security, Governance and Controls 2 Hours
- [Optional] Enable trial license of SharePoint Advanced Management and review findings 2 Hours
- Review Identity & Access Management 1 Hour
- Review Device Management 2 Hour
- Review Data Lifecycle controls 2 Hour
- Review App Management 2 Hour
- Review data sources outside Microsoft 365 1 Hour



## Next Steps

- Assessment Report and Recommendations 1 Hour
- Guidance on Next Steps 30 Mins



# Out of scope

## Copilot for Microsoft 365 Deployment

Deployment of Copilot for Microsoft 365 is out of scope for this engagement but available as an add-on or separate SOW.

## Copilot for Microsoft 365 Adoption

Adoption and Change Management services including training for end-users for Copilot for Microsoft 365 is out of scope for this engagement but available as an add-on or separate SOW.

## Copilot for Microsoft 365 Customization

Customization of Copilot for Microsoft 365 and integration with any data source or application external to Microsoft 365 is out of scope for this engagement but available as an add-on or separate SOW.

# Discover – Know your data and understand the risks

Uncover the potential data and security risks Microsoft 365 Copilot could introduce into your organization.

What is sensitive?

- Define what is sensitive to the organization
- Generic & customer specific
  - Company secrets
  - Highly confidential
  - Personal Identifiable Information

Where does data live?

- Created inventory of all data repositories
- Considered as copilot source
  - Microsoft 365
  - 3rd party sources
  - Structured and unstructured

Who has access?

- What content can employee access
- Internal & external to the organization
- Access control and access management
- Oversharing

How is it used?

- Sensitive data overexposure
- Unprotected data
- Is the use of sensitive data managed

What is the risk?

- What if data is exposed
- Which data could harm the organization
- What would be the impact & cost
- Are we at risk
- Are we compliant

## Protect

Implement controls to mitigate and reduce risk.

Data Lifecycle controls

- Minimize obsolete data
- Retention policies and automatic deletion
- Records management for business, legal or regulatory record keeping requirements

Data Protection controls

- Protect sensitive information
  - Data encryption
  - Watermarking
- Prevent Data loss
- Protect against Oversharing and external sharing

Data access controls

- Optimize access permissions, remove, block
- Correct oversharing
- Exclude data sources

Data labeling

- Apply sensitivity labels to data
- Manual, user initiated
- Automatic, based on content, location, purpose, etc.

Data classification

- Select and define sensitive info types
  - Generic, out of the box
  - Customer specific, custom defined to specification



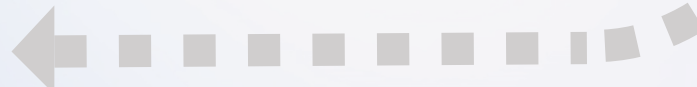
Organizational risk tolerance define next steps.

**Low risk**  
Enable copilot

**Medium risk**  
Implement (additional) data security and in parallel enable coplot.

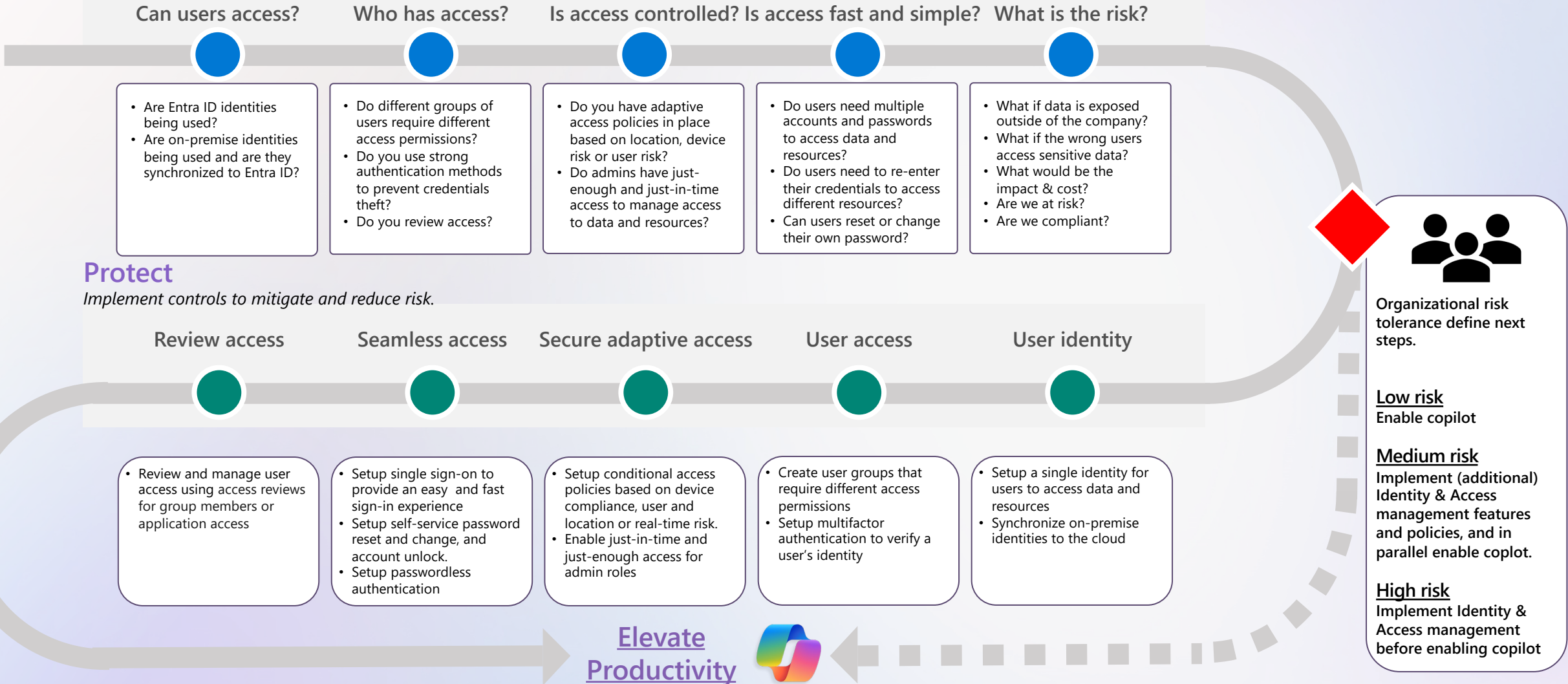
**High risk**  
Implement data security before enabling copilot

Elevate Productivity



# Discover – Protect user access to Microsoft Copilot for Microsoft 365

Use strong authentication and real-time, risk-based adaptive access policies without compromising user experience



# Discover – Secure access to Microsoft Copilot for Microsoft 365 from any device

Ensure that only secure, up-to-date and compliant Windows physical or virtual devices and mobile devices have access

Which devices?

- Windows physical devices
- Windows virtual devices (Windows 365 or AVD)
- Android Devices
- iOS/iPadOS devices
- macOS devices

Are devices managed?

- Are users accessing Microsoft 365 from unmanaged devices?
- Are users accessing Microsoft 365 from an MDM managed device?
- Are devices company-owned or personal?

Are apps up to date?

- Are the Microsoft 365 apps deployed remotely to all types of managed devices?
- Are the Microsoft 365 apps up to date for Copilot?

Are devices secure?

- Are security policies in place to protect devices from vulnerabilities and threats and improve compliance?
- Are devices up to date with the latest OS version?

What is the risk?

- What if compromised devices are used to access company data?
- What if corporate data is exposed?
- What would be the impact & cost?
- Are we at risk?
- Are we compliant?

## Protect

Implement controls to mitigate and reduce risk.

Wipe devices

- Fully wipe lost or stolen devices
- Wipe all work content on unmanaged devices including content generated by copilot when an employee leaves the company

Revoke access

- Revoke access to non-compliant devices
- Remediate non-compliant devices

Set compliance

- Deploy device compliance policies
- Create conditional access policies based on device compliance for accessing Microsoft 365

Manage apps

- Deploy Microsoft 365 apps
- Deploy app configuration policies
- Deploy app update policies

Manage devices

- Enroll devices into device management
- Deploy device configuration policies
- Deploy device protection policies
- Deploy OS update policies

Elevate  
Productivity



Organizational risk tolerance define next steps.

**Low risk**  
Enable copilot

**Medium risk**  
Implement (additional) endpoint management features and policies, and in parallel enable copilot.

**High risk**  
Implement endpoint management before enabling copilot

# Discover – Secure apps used to access to Microsoft Copilot for Microsoft 365

Control how data is accessed and shared by apps on mobile devices

On which devices?

- Do users access Microsoft 365 apps from personal devices?
- Do users access Microsoft 365 apps from third-party MDM managed devices?
- Do users access Microsoft 365 apps from unmanaged devices?

Which apps?

- From which Microsoft 365 apps do users need access to Microsoft 365 and Microsoft Copilot?
- Do users need access to Microsoft 365 from third-party apps?
- Are users allowed to use personal apps?

Are apps protected?

- Is a PIN, fingerprint or face ID required to access corporate apps?
- Can certain actions to move or access corporate data be prohibited or monitored within the apps?

How is data shared?

- Can you control how corporate data is shared between corporate and personal apps or storage locations?

What is the risk?

- What if shadow IT is used to access company data?
- What if corporate data is exposed to personal apps or public locations?
- What would be the impact & cost?
- Are we at risk?
- Are we compliant?

## Protect

Implement controls to mitigate and reduce risk.

Wipe app data

- Selectively wipe corporate data from the managed apps when a user leaves the company or when an unmanaged device is lost or stolen.

Define managed locations

- Setup OneDrive for Business
- Prevent the saving of company app data to a personal storage location

Set approved apps

- Restrict access to Microsoft 365 to only approved apps

Restrict app data usage

- Require a PIN, fingerprint or face ID to access an app in work context
- Control the sharing of data between corporate and personal apps (Restrict cut, copy, and paste)

Protect apps

- Setup app protection policies to protect the core Microsoft apps
- Setup app protection policies to protect supported third-party apps
- Protect in-house built apps

Elevate  
Productivity



Organizational risk tolerance define next steps.

Low risk  
Enable copilot

Medium risk  
Implement (additional) mobile application management features and policies, and in parallel enable copilot.

High risk  
Implement mobile application management before enabling copilot



# Next Steps

Schedule your assessment today!

[sales@thepartnermasters.com](mailto:sales@thepartnermasters.com)



Modern Work

Specialist  
Adoption and Change  
Management