

Copilot for Microsoft 365 is transforming work

68%

70%

77%

said they didn't

want to give Copilot up

said Copilot made

them more productive

said Copilot improved the quality of their work



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 Al to lessen their workloads



Copilot for Microsoft Readiness Assessment Goals

Assess your business readiness

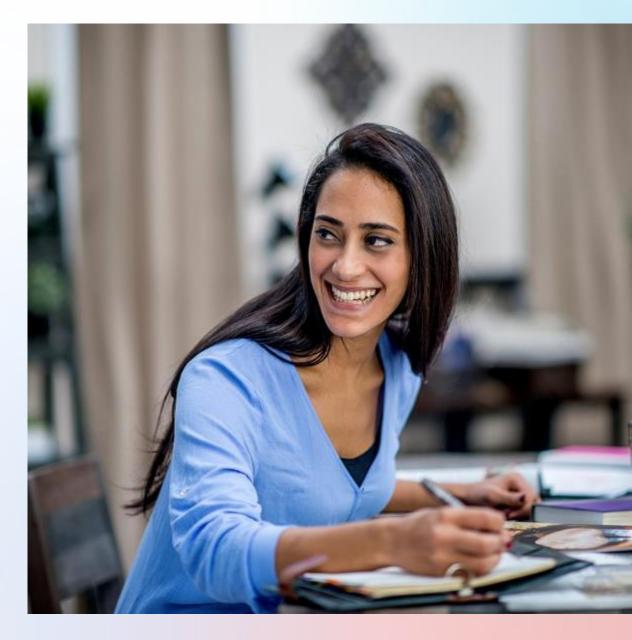
Identify your organization's ability to drive adoption of Copilot for Microsoft 365 through effective organizational sponsorship, strategy, and execution of capabilities of generative AI solutions.

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



Technical Review (Works	shops)
☐ 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



- ☐ 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 365is 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

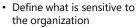
Uncover the potential data and security risks Microsoft 365 Copilot could introduce into your organization.

What is sensitive? Where does data live? Who has access?

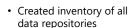
How is it used?

What is the risk?

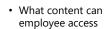




- Generic & customer specific
 - Company secrets
 - · Highly confidential
 - Personal Identifiable Information



- Considered as copilot source
 - Microsoft 365
 - 3rd party sources
 - Structured and unstructured



- · Internal & external to the organization
- · Access control and access management
- Oversharing



- Unprotected data
- Is the use of sensitive data managed



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



Implement controls to mitigate and reduce risk.

Data Lifecycle controls

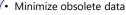
Data Protection controls

Data access controls

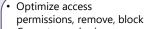
Data labeling

Data classification





- Retention policies and automatic deletion
- Records management for business, legal or regulatory record keeping requirements
- Protect sensitive information
 - Data encryption
- Watermarking
- Prevent Data loss
- Protect against Oversharing and external sharing



- Correct oversharing
- · Exclude data sources
- Apply sensitivity labels to data
- Manual, user initiated
- Automatic, based on content, location, purpose, etc.
- Select and define sensitive info types
- Generic, out of the box
- Customer specific. custom defined to specification



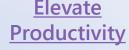


Organizational risk tolerance define next steps.

Low risk **Enable copilot**

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

High risk Implement data security before enabling copilot



Discover – Protect user access to Microsoft Copilot for Microsoft 365

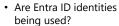
Use strong authentication and real-time, risk-based adaptive access policies without compromising user experience

Can users access?

Who has access?

Is access controlled? Is access fast and simple? What is the risk?

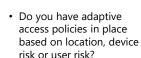




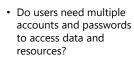
 Are on-premise identities being used and are they synchronized to Entra ID?



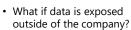
- · Do different groups of users require different access permissions?
- Do you use strong authentication methods to prevent credentials theft?
- Do you review access?



Do admins have justenough and just-in-time access to manage access to data and resources?



- · Do users need to re-enter their credentials to access different resources?
- Can users reset or change their own password?



- What if the wrong users access sensitive data?
- What would be the impact & cost?
- · Are we at risk?
- Are we compliant?



Implement controls to mitigate and reduce risk.

Review access

Seamless access

Secure adaptive access

User access

User identity



Review and manage user

for group members or

application access

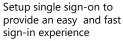
access using access reviews



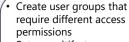




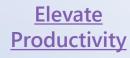




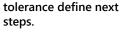
- Setup self-service password reset and change, and account unlock.
- Setup passwordless authentication
- Setup conditional access policies based on device compliance, user and location or real-time risk.
- Enable just-in-time and just-enough access for admin roles



- Setup multifactor authentication to verify a user's identity
- Setup a single identity for users to access data and resources
- Synchronize on-premise identities to the cloud







Organizational risk



Medium risk Implement (additional) **Identity & Access** management features and policies, and in parallel enable coplot.

High risk Implement Identity & Access management before enabling copilot

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

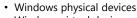
Ensure that only secure, up-to-date and compliant Windows physical or virtual devices and mobile devices have access

Which devices?

Are devices managed? Are apps up to date? Are devices secure?

What is the risk?

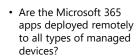




- · Windows virtual devices (Windows 365 or AVD)
- Android Devices
- iOS/iPadOS devices
- macOS devices



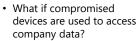
- Are users accessing Microsoft 365 from an MDM managed device?
- Are devices companyowned or personal?



• Are the Microsoft 365 apps up to date for Copilot?



 Are devices up to date with the latest OS version?



- What if corporate data is exposed?
- What would be the impact & cost?
- · Are we at risk?
- Are we compliant?



Implement controls to mitigate and reduce risk.

Wipe devices

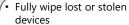
Revoke access

Set compliance

Manage apps

Manage devices





• Wipe all work content on unmanaged devices including content generated by copilot when an employee leaves the company

Revoke access to noncompliant devices

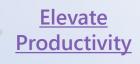
Remediate non-compliant devices

Deploy device compliance policies

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

Deploy Microsoft 365 apps

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







Organizational risk tolerance define next steps.

Low risk **Enable copilot**

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

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

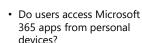
On which devices?

Which apps?

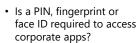
Are apps protected?

How is data shared?

What is the risk?



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



- Can certain actions to move or access corporate data be prohibited or monitored within the apps?
- Can you control how corporate data is shared between corporate and personal apps or storage locations?
- 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?



Implement controls to mitigate and reduce risk.

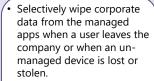
Wipe app data

Define managed locations

Set approved apps Restrict app data usage

Protect apps





Setup OneDrive for Business

 Prevent the saving of company app data to a personal storage location Restrict access to Microsoft 365 to only approved apps

- 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)
- 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







Organizational risk tolerance define next steps.

Low risk Enable copilot

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

High risk
Implement mobile
application management
before enabling copilot



Next Steps

Schedule your assessment today!

info@Moonshot-Solutions.com

