

## COPILOT READINESS GUIDE

# 5 ways to get your business AI ready

Interested in Microsoft Copilot, but unsure whether your environment is ready for AI?

This guide outlines five common security gaps that can slow or block AI projects – and how to address them to deploy AI securely and confidently.



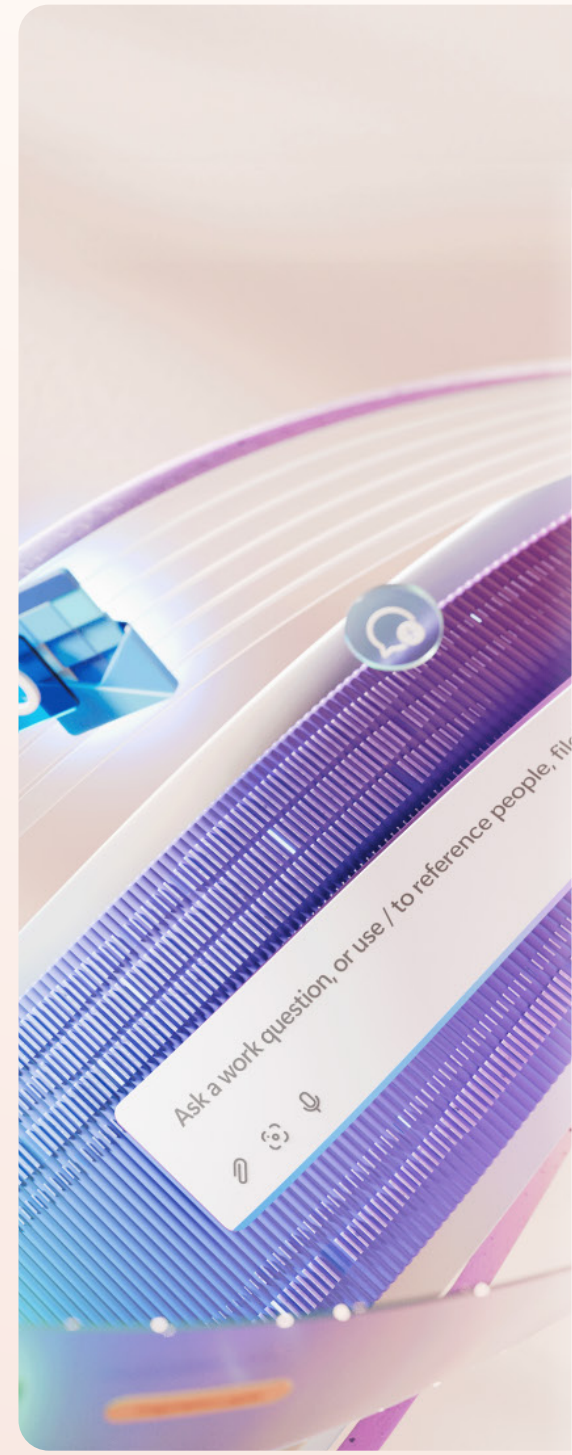
# 1

## Start by strengthening identity

Copilot relies on existing user permissions and access controls. If your identity hygiene is weak, AI can amplify the risks.

Strengthen your AI readiness by:

- Running Microsoft Entra ID assessments
- Strengthening multi-factor authentication (MFA) across users and admins
- Implementing Conditional Access policies
- Tightening privileged access controls and identity governance



# 2

## Understand and protect data

Copilot can only protect data it understands. Which means if your underlying data estates are unclassified or poorly protected, it increases the risk of oversharing sensitive information.

Protect your data by:

- Implementing Microsoft Purview data classification
- Applying sensitivity labels across information sets
- Deploying Data Loss Prevention policies
- Identifying sensitive content across Microsoft 365

# 3

## Modernise threat protection

As AI adoption grows, so does your need for coordinated visibility. Legacy security tools can create visibility gaps across identities, endpoints, email, and cloud applications, making it harder to detect and respond to threats.

Protect your business by:

- Standardising security management through Microsoft Defender XDR
- Replacing fragmented point solutions with unified protection
- Improving visibility across Microsoft 365
- Strengthening detection and response capabilities

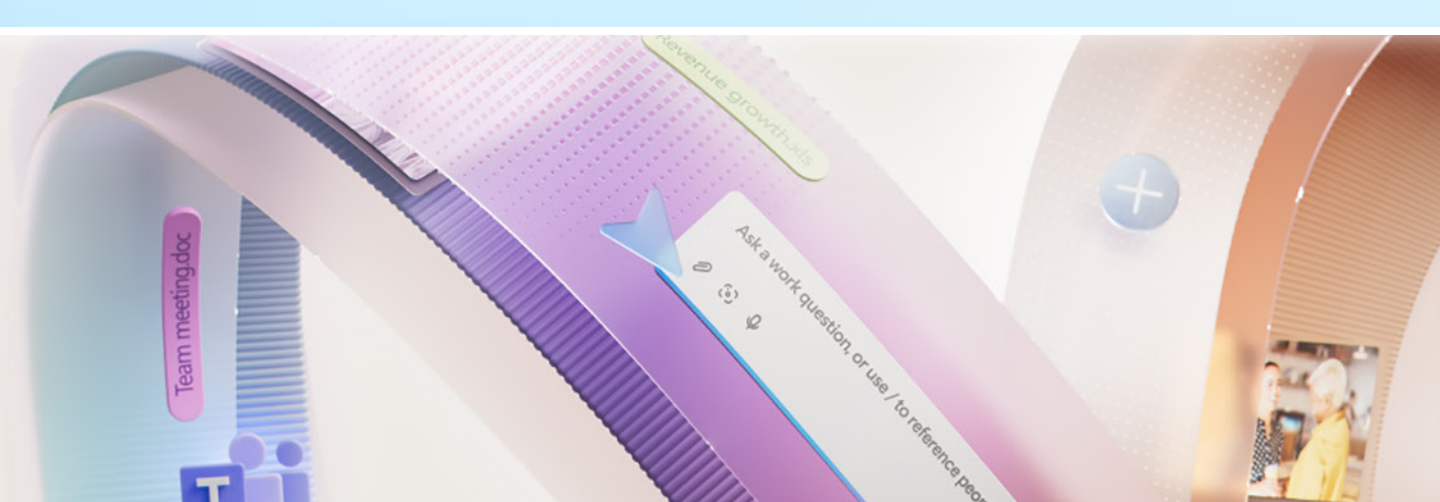
# 4

## Build governance and compliance controls

AI can introduce new compliance risks – and without the right governance processes in place, it can put the brakes on your Copilot adoption.

Put control in place by:

- Deploying Microsoft Purview compliance and governance features
- Introducing governance controls around Copilot use
- Supporting retention, audit policies, and information life cycles
- Aligning AI use with internal and regulatory requirements



# 5

## Create an AI-ready security strategy

Guide your journey with a roadmap that connects security and AI to make Copilot adoption achievable for the business.

Build your roadmap by:

- Undertaking an AI readiness assessment
- Putting security first
- Aligning adoption to business goals
- Connecting security foundations to productivity outcomes

## Lay the foundations to secure your AI ambitions

Whether you need help identifying where your security gaps are or building a roadmap to get your Copilot adoption programme firmly on track, we can help.

Get in touch to explore the support we offer.

[TALK TO US](#)