FREE GUIDE

RUA TECHNOLOGIES

The Microsoft 365 Copilot & AI Agent Readiness Checklist

Everything to put in place before you roll out Microsoft 365 Copilot or build your first AI agent: data, identity, governance, licensing and a pilot plan that proves value.

7 sections + glossary	20 minutes	Print-ready checklist
WHAT'S INSIDE	TIME TO READ	FORMAT

Use cases | Data & permissions | Identity | Governance | Pilot & adoption

ruatechnologies.com | sales@ruatechnologies.com | +91 91315 71358

Updated October 2026

INSIDE THIS GUIDE

What you'll find

01 Choose use cases worth doing

02 Fix your data and permissions

03 Secure identity and devices

04 Licensing and technical prerequisites

05 Governance and policy

06 Designing your first agent

07 Pilot, train and measure

AI assistants and agents are moving from experiments to everyday business tools. Microsoft 365 Copilot helps individuals draft, summarize and analyze inside the apps they already use. Agents, built with tools such as Copilot Studio, go further by following a process and taking actions in connected systems.

Both share one dependency that is easy to underestimate: they work with the data and permissions you already have. If files are over-shared, outdated or unlabeled, an AI tool will surface them faster than a person ever would. Readiness is mostly about getting those foundations right before you switch anything on.

HOW TO USE THIS GUIDE

Treat each section as a gate. Do not move to a wider rollout until the boxes in the earlier sections are ticked. A short, well-prepared pilot beats a large, rushed launch.

CHECK LICENSING AND AVAILABILITY

Product names, plan eligibility and features change often. Confirm current Copilot licensing requirements and feature availability with Microsoft or your partner before you budget.

SECTION 01

Choose use cases worth doing

The best first projects are narrow, repetitive and low-risk, with a result you can measure.

- [ ] List five to ten tasks that eat time: meeting summaries, drafting replies, report preparation, policy questions, ticket triage
- [ ] Score each by volume (how often), time saved per use and risk if the AI is wrong

- [ ] Pick one to three for the pilot; avoid anything involving payments, legal commitments or sensitive personal data at first
- [ ] Define a clear success measure for each (for example minutes saved, tickets resolved without escalation)
- [ ] Capture a baseline before the pilot so improvement is provable
- [ ] Decide who owns each use case and who will review the results

STARTER USE CASE	WHY IT WORKS
Internal HR / IT FAQ agent	High volume, answers come from approved documents, low risk
Meeting and email summarization	Immediate value for managers, easy to verify
Sales call follow-ups	Saves admin time, human sends the final message
Document and knowledge search	Reduces time spent hunting for the latest file

SECTION 02

Fix your data and permissions

This is the section most organizations skip, and the one that causes the most trouble. AI tools respect existing access rights, so anything a user can technically open can appear in their results.

- [ ] Review SharePoint, OneDrive and Teams sharing; find sites and files shared with ‘everyone’ or broad groups
- [ ] Remove access for people who have left or changed roles
- [ ] Archive or delete outdated, duplicate and draft content that would pollute answers
- [ ] Apply sensitivity labels to confidential and regulated content (HR, finance, legal, customer data)
- [ ] Check that labeled content is protected by policy, not just tagged
- [ ] Identify where personal data is stored and confirm it is handled lawfully
- [ ] Decide which sites and libraries agents are allowed to read, and which are off-limits
- [ ] Re-run a permissions review on a schedule, not once

> **WHY THIS COMES FIRST**
>
> If a confidential spreadsheet is accessible to the whole company today, Copilot may quote from it tomorrow. Fix the access, and the AI becomes safe to use.

SECTION 03

Secure identity and devices

AI tools sit behind the same sign-in as your email and files, so identity controls apply directly.

- [ ] Enforce multi-factor authentication for every user, with no unmanaged exceptions
- [ ] Use Conditional Access to require compliant devices and block legacy authentication
- [ ] Review administrator roles and apply least-privilege access
- [ ] Make sure devices are enrolled in management and patched
- [ ] Confirm endpoint protection is deployed and reporting
- [ ] Enable sign-in and audit logging so activity can be reviewed
- [ ] Have a process for lost devices and compromised accounts

LINK TO THE REST OF YOUR SECURITY

Readiness work overlaps with Zero Trust, data loss prevention and identity hardening. Doing it once benefits AI and everything else.

SECTION 04

Licensing and technical prerequisites

Confirm what you need before you promise anything to the business.

- [ ] Confirm which of your current Microsoft 365 plans are eligible for Copilot
- [ ] Decide who gets licenses in the pilot (a mix of roles, not just enthusiasts)
- [ ] Check that users are on supported, up-to-date Microsoft 365 apps
- [ ] Confirm the tenant, domains and identity configuration are healthy
- [ ] Review what extra licensing or capacity agents built in Copilot Studio may require
- [ ] Plan for how licenses will be reassigned if usage is low
- [ ] Ask for a current written quote; do not rely on list prices you saw months ago

COST NOTE

We have not quoted prices because they vary by plan, region and agreement. Compare a quote against the time-saving targets you set in Section 01.

SECTION 05

Governance and policy

Clear rules protect the business and make adoption easier, because people know what is allowed.

- [ ] Publish an acceptable-use policy for AI: what staff may and may not do
- [ ] Define which data must never be pasted into any AI tool
- [ ] Require a human review step for external communications, financial actions and decisions affecting people
- [ ] Assign an owner for each agent: who maintains its content, access and results
- [ ] Set up data loss prevention policies for sensitive information types
- [ ] Decide how outputs will be fact-checked before they are relied upon
- [ ] Document how personal data is processed, and review it against applicable Indian data-protection requirements
- [ ] Create a simple route for staff to report wrong or unsafe AI answers
- [ ] Agree how unapproved ‘shadow AI’ tools will be handled

> **AGENTS NEED EXTRA CARE**
>
> An agent can act, not just answer. Start with read-only or draft-only behavior, add approvals for anything that changes data, and log what it does.

SECTION 06

Designing your first agent

If you plan to build an agent, for example with Microsoft Copilot Studio, keep the first one small and well-bounded.

- [ ] Write the agent's purpose in one sentence and list what it must not do
- [ ] Give it only the knowledge sources it needs (specific sites or documents, not the whole tenant)
- [ ] Limit connected actions to the minimum, and require approval for sensitive steps
- [ ] Write clear instructions about tone, escalation and what to say when unsure
- [ ] Test with real questions, including trick and out-of-scope questions
- [ ] Review a sample of conversations every week during the pilot
- [ ] Define when it should hand over to a person
- [ ] Decide who is notified when it fails or behaves unexpectedly

CHATBOT	COPILOT	AGENT
Answers scripted questions	Helps one user inside an app	Pursues a goal across steps and systems
Cannot act in systems	User directs each step	Acts within set permissions
Low setup effort	Low to medium	Medium; needs design and governance

SECTION 07

Pilot, train and measure

Adoption is a people problem as much as a technical one. A structured pilot gives you evidence and champions.

- [ ] Run the pilot for four to eight weeks with a defined group
- [ ] Train users on what to ask, how to check answers and what not to share
- [ ] Name a champion in each team to share tips and collect feedback
- [ ] Track the measures you defined in Section 01 against your baseline
- [ ] Survey users on usefulness, trust and problems
- [ ] Review security and permissions findings with IT before expanding
- [ ] Decide on scale-up, adjust or stop, using the evidence
- [ ] Share results with leadership in plain language

A simple 90-day roadmap

DAYS	FOCUS
1 to 30	Pick use cases, fix permissions and labels, secure identity, confirm licensing
31 to 60	Pilot with a small group; train, measure and collect feedback
61 to 90	Review results, tighten governance, expand to the next team

> **COMMON PITFALLS**
>
> Switching Copilot on for everyone on day one; skipping the permissions review; no success measure; no owner for agents; treating AI output as always correct.

REFERENCE

Glossary of terms

Microsoft 365 Copilot
An AI assistant built into Microsoft 365 apps that helps users draft, summarize and analyze using their organization's data.

AI agent
Software powered by a language model that pursues a goal, decides the steps and can take actions in connected systems.

Copilot Studio
A Microsoft tool for building custom agents and connecting them to business knowledge and workflows.

Sensitivity label
A tag applied to files and emails that classifies them (for example Confidential) and can enforce protection.

DLP
Data loss prevention: policies that detect and block sensitive information from being shared inappropriately.

Conditional Access
Policies that decide whether a sign-in is allowed based on user, device, location and risk.

Shadow AI
AI tools used by staff without approval or oversight from IT.

NEXT STEP

Want a Copilot and AI readiness review?

We assess your permissions, identity and data, recommend the right first use cases, and help you run a governed pilot with Copilot or Copilot Studio, so you can scale with confidence.

Web ruatechnologies.com/contact/

Email sales@ruatechnologies.com

Phone / WhatsApp +91 91315 71358

Microsoft, Microsoft 365, Office, Copilot and related names are trademarks of Microsoft Corporation. This guide is general information, not legal or compliance advice; check product details and dates with Microsoft before acting. Rua Technologies © 2026.