



BUILDING YOUR OWN AI AGENTS IN COPILOT



Copyright©2026 Virtual Training Co. All rights reserved. This publication or any part thereof, may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, storage in an information retrieval system, or otherwise without written permission of Virtual Training Co, W5813 Timber Trail, New Lisbon, WI 53950.



Build Your Own AI Agents in Copilot

This session shows how to plan, build, test, edit, and pilot Microsoft 365 Copilot agents for repeatable business work. You will learn how to choose a starting point, define a focused agent purpose, connect trusted knowledge sources and attachments, customize instructions and behavior, test realistic prompts, and share or pilot an agent with a small team.



What You Will Learn

- What Copilot Agents are and where they fit in everyday business work.
- How to create an agent using natural language in Agent Builder.
- How to connect trusted, current, permission-aware knowledge sources.
- How to customize instructions, response behavior, outputs, and boundaries.
- How to test realistic responses before launch.
- How to share or pilot an agent with team members.

What Is a Copilot Agent?

Copilot chat gives you one-time help in response to a prompt. A Copilot agent is a reusable assistant built for a specific job. It follows specific instructions, uses approved knowledge, and produces a consistent type of response for you or your team.

Agents are useful for repeatable questions, recurring updates, meeting preparation, project coordination, policy or process lookups, request intake, and follow-up tasks. A focused agent can reduce searching, improve consistency, and help your team move from information to a practical next step.

Newest Copilot Agent Feature Highlights

Microsoft continues to expand what Copilot agents can do. As you build and teach agents, call out these current changes so learners understand the newest terminology and default capabilities.

- **“Uploaded files” is now “Attachments.”** The section serves the same purpose, but the clearer name helps users understand that files can be attached as part of the agent setup or conversation context.
- **Agents can write code and create files.** New agents can use code-writing capability and create Word, Excel, and PowerPoint files when those features are available in the organization. These capabilities are on by default, though availability may still depend on license, admin settings, and tenant configuration.



- **Agents can generate graphics and illustrations.** Image generation is also on by default when available, so an agent may help create visuals such as graphics, illustrations, concept images, and supporting visuals for business content.
- **Teaching note:** Remind students that “on by default” does not mean “use without review.” Generated code, documents, spreadsheets, presentations, and visuals should still be checked for accuracy, appropriateness, permissions, and business fit before sharing.

The Core Parts of an Agent

- **Purpose:** the business outcome the agent supports.
- **Audience:** the business professionals or team members who will use it.
- **Instructions:** the role, tone, tasks, response style, and limits.
- **Knowledge:** the approved information the agent can use.
- **Outputs** and actions: what the agent returns or prepares for review.
- **Boundaries:** what it should not do and when it should direct you to a person or official process.

Student takeaway: Start with one narrow job. A well-defined agent is easier to explain, test, govern, and improve.

How You Create an Agent

Creating an agent follows a simple sequence. Start with the job the agent should perform, then build, test, and improve it before other people rely on it. Screens and options may vary by license, permissions, and organizational settings.

The Overall Build Path

- Name the agent and describe the specific job it should do.
- Add clear instructions for its audience, tasks, tone, output, and boundaries.
- Add approved knowledge sources that contain the information it should use.
- Test the agent with realistic prompts, then refine its instructions, sources, and scope.
- Share it or pilot it with a small team when the results are accurate, useful, and appropriately bounded.



Example description: “Create a Project Meeting Prep Agent for business professionals. Use approved project files and meeting notes to prepare a concise briefing with progress, open items, risks, decisions needed, and next actions. Do not send messages or change tasks without user review.”



Choose Your Starting Point: Template or My Agents

Quick decision guide: Use a template when the scenario closely matches a common business need and you want a guided starting point. Use My agents when you need to find, edit, test, manage, or reuse agents that already exist. Use a manual build when you already know the purpose, audience, sources, and boundaries. Use Copilot-assisted setup when you have an idea but want help drafting the name, instructions, response format, boundaries, and test prompts before entering the setup in Agent Builder.

Plan Before You Build

Before opening Agent Builder, take a few minutes to design the agent on paper. Planning first helps you avoid creating an agent that is too broad, uses the wrong sources, gives inconsistent answers, or acts beyond what users expect. A strong plan gives the agent a clear job, trusted information, useful output, and safe boundaries before anyone relies on it.

What to Plan

- **The business problem:** Identify the repeated question, task, update, or process the agent should support. If the need only happens once, a regular Copilot prompt may be enough.
- **The audience:** Decide who will use the agent and what they need from it. A manager, field employee, project coordinator, or new team member may need different wording, detail, and next steps.
- **The expected outcome:** Define what a successful response should help the user do, such as prepare for a meeting, find approved information, draft a follow-up, summarize open items, or decide what to review next.
- **The knowledge sources and attachments:** List the approved sites, files, folders, notes, policies, templates, task lists, conversations, or attachments the agent should use. Choose focused, current sources instead of connecting everything available.
- **The response format:** Decide what the answer should look like. For example, the agent might return a prioritized brief, checklist, table, draft message, status update, or list of action items.
- **The boundaries:** State what the agent should not do, such as sending messages, changing tasks, making commitments, interpreting policy, or using unapproved sources without user review.





- **The test prompts:** Prepare realistic prompts before you build, including normal requests, vague requests, missing-information requests, and requests the agent should refuse or escalate.
- **The success measure:** Decide how you will know the agent is useful, such as saving time, reducing missed follow-ups, improving consistency, or making information easier to find.

Feature planning check: If your agent can create files, write code, or generate visuals, decide whether those capabilities are appropriate for this scenario. Identify what the agent may create, what should remain in draft, who should review the output, and whether your organization's policies allow that type of content to be used or shared.

Why Planning Matters

Agents work best when they are built for a specific business scenario with clear instructions, relevant knowledge, and a defined output. If the purpose is too broad, the agent may give generic answers. If the sources are unclear or outdated, the agent may rely on incomplete information. If the boundaries are missing, users may expect the agent to take actions it should only prepare for review. Planning gives you a way to narrow the job before you build, test against real work, and improve the agent before sharing it with others.

How to Plan the Agent

1. **Start with one sentence:** Write, "This agent helps [audience] do [task] using [approved sources] so they can [business outcome]."
2. **Narrow the scope:** Remove extra jobs until the agent has one primary purpose. If you find yourself using the word "and" several times, you may be designing more than one agent.
3. **Map questions to sources:** List the questions users will ask and identify the official source for each answer. If there is no trusted source, decide whether the agent should say the information is missing.
4. **Define the ideal response:** Sketch the headings, order, level of detail, and tone the agent should use. This makes the instructions easier to write and the results easier to evaluate.
5. **Add human review points:** Decide which actions should stay in draft or require approval, especially messages, task updates, calendar changes, records, decisions, or policy-related recommendations.
6. **Create a small test set:** Write three to five prompts that represent real use. Include one easy request, one vague request, one missing-information request, and one boundary request.
7. **Use the plan while building:** Copy the purpose, instructions, sources, output format, boundaries, and test prompts into Agent Builder. After testing, revise the plan and the agent together.

Examples: Plan Before You Build



Use these examples to see how a rough idea becomes a focused agent plan before you begin building.

Agent Idea	What to Plan	Why It Matters	How to Build the Plan
Catch-Up and Prep Agent	Plan the time period, sources to review, priority categories, and actions that must stay in draft.	Without limits, the agent may summarize too much or miss the most important follow-ups.	Write a purpose statement, choose approved emails, chats, meetings, tasks, and files, then define a brief with urgent items, meetings, tasks, decisions, and next actions.
Policy or Procedure Agent	Plan the official policy sources, common questions, response format, and escalation rules.	Users need answers based on approved current documents, not guesses or outdated files.	List the approved policy library, define when to quote or summarize, and instruct the agent to say when information is missing or requires human review.
Project Status Agent	Plan which projects, files, meeting notes, task lists, and reporting templates the agent should use.	A project agent must separate facts, risks, blockers, decisions, and recommended next steps.	Define a status format with progress, changes, risks, blockers, owners, deadlines, and decisions needed. Add test prompts for weekly updates and missing information.

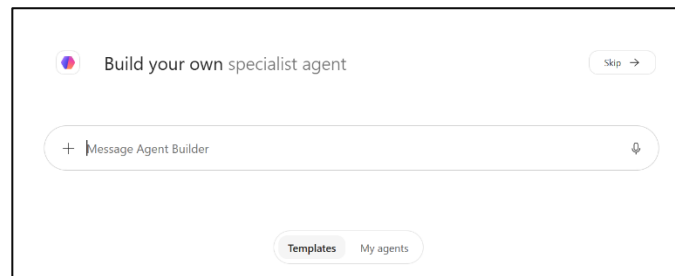
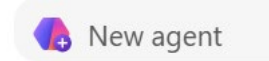
Option 1: Create an Agent Manually in Agent Builder

Scenario: A general business user is returning from meetings or time away and needs one clear catch-up briefing across email, Teams chats and posts, tasks, meetings, recaps, and files. As a student, build the agent by completing the numbered steps below.



Use this option when you are ready to enter the setup directly in Agent Builder. The Catch-Up and Prep Agent example shows the sequence from naming and instructions through knowledge, boundaries, and testing.

1. Open Microsoft 365 Copilot and choose the option to create an agent in Agent Builder.
2. Choose the option to create a new agent.
3. Name the agent **Catch-Up and Prep Agent**.
4. Describe the agent's purpose: "Help me prepare for upcoming work and catch up on recent activity by reviewing approved Microsoft 365 content I can access."
5. Add instructions that tell the agent to review recent emails, Teams chats, channel posts, assigned tasks, meetings, meeting recaps, and shared files.
6. Define the response format: urgent items, upcoming meetings to prepare for, open tasks, unanswered questions, recent decisions, files to review, and suggested next actions.
7. Add boundaries: "Do not send messages, complete tasks, change calendar items, or make commitments unless I review and approve them."
8. Connect trusted knowledge sources that are appropriate for your work, such as approved project sites, team files, meeting notes, task lists, and shared workspaces.
9. Save the draft agent.
10. Test the agent with a realistic prompt before sharing it with anyone else.



Manual test prompt: "Review my recent emails, Teams chats and posts, tasks, meetings, meeting recaps, and shared files from the last three business days. Create a concise catch-up brief showing what I need to prepare for, respond to, catch up on, and handle first. Do not send messages or update tasks without my approval."



Examples: What to Enter in Agent Builder

Use the following entries to configure the Catch-Up and Prep Agent scenario, adapting the wording to a general business setting as needed.

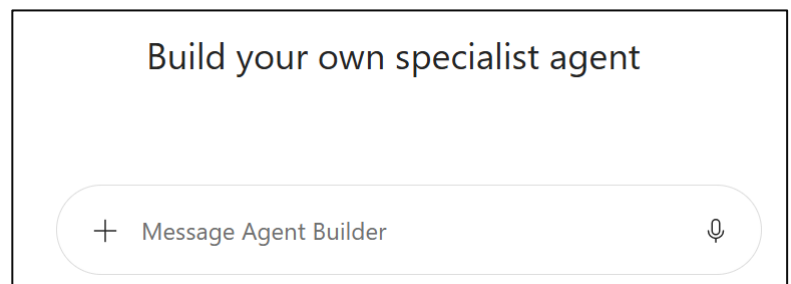
Agent Builder Field	Example Entry
Name	Catch-Up and Prep Agent
Description	Helps me prepare for upcoming work and catch up on recent activity across approved Microsoft 365 content.
Instructions	Review recent emails, Teams chats, channel posts, tasks, meetings, recaps, and shared files. Summarize what needs preparation, response, follow-up, or review. Organize the answer by priority and include suggested next actions.
Knowledge Sources	Approved team site, project folder, meeting notes, task list, shared files, and related Microsoft 365 content the user can access.
Boundaries	Do not send messages, mark tasks complete, change calendar items, or make commitments unless I review and approve them.

Option 2: Use Copilot to Help Draft the Agent Setup

Scenario: You have an idea for a catch-up agent but want Copilot to draft the setup before you build it. As a student, use the numbered steps below to review, adapt, and apply the draft.

Use this option when you want Copilot chat to help draft the setup before you build. Copilot can propose a name, purpose, instructions, knowledge sources, response format, boundaries, and test prompts; you review and refine them before entering them in Agent Builder.

1. Open Copilot chat in your approved Microsoft 365 experience.
2. Ask Copilot to help plan the agent by describing the business problem and audience.
3. Review Copilot's draft name, purpose, instructions, knowledge sources, response format, boundaries, and test prompts.
4. Ask Copilot to narrow the scope if the agent tries to do too much.





5. Ask Copilot to rewrite the instructions in clear student-friendly or business-friendly language.
6. Copy the refined name, description, instructions, sources, boundaries, and test prompts into Agent Builder.
7. Connect the approved knowledge sources in Agent Builder.
8. Test the agent using the prompts Copilot helped you create.
9. Revise the agent instructions based on the test results.
10. Save the revised version and decide whether to keep testing, pilot with a small group, or share with your team.

Copilot planning prompt: “Help me design a Catch-Up and Prep Agent for Microsoft 365 Copilot. The agent should help me prepare for upcoming work and catch up on recent activity across emails, Teams chats, channel posts, tasks, meetings, meeting recaps, and shared files. Draft the agent name, purpose, instructions, trusted knowledge sources, response format, boundaries, and five test prompts. Make the agent useful for business professionals and keep all actions in draft until the user approves them.”

Refinement prompt: “Review this agent setup and make it narrower, safer, and easier to test. Identify any vague instructions, missing boundaries, unclear knowledge sources, or response-format issues before I build it in Agent Builder.”

Key Differences: Manual Build vs. Copilot-Assisted Setup

Build Method	Best When	Key Difference
Manual build in Agent Builder	You already know the agent's purpose, sources, instructions, and boundaries.	You enter the setup directly and refine by testing inside Agent Builder.
Copilot-assisted setup	You want help turning an idea into clearer instructions, sources, boundaries, and test prompts.	Copilot helps draft the setup first; you review, revise, and then copy the final version into Agent Builder.



Guide and Refine the Output

Ask for the result, review it, and then refine the audience, sources, format, priority, or decision criteria.

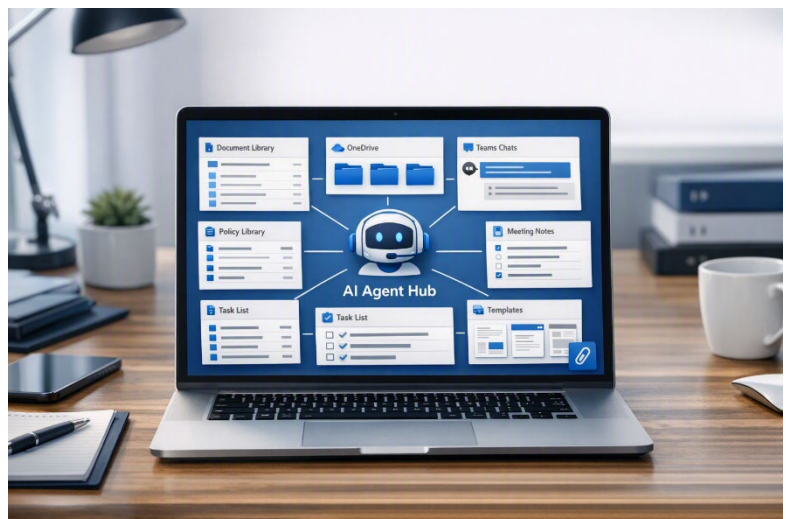
User Goal	Initial Prompt	Refinement Prompt
Prepare a team update	Summarize recent activity for my project.	Rewrite this as a concise update with progress, risks, blockers, decisions needed, and next actions.
Find follow-ups	Review recent meeting notes for open items.	Group open items by owner, due date, and urgency. Flag blocked items or missing decisions.
Use approved knowledge	What procedure applies to this request?	Base the answer only on approved procedure documents and identify anything I should verify.

Connect Trusted Knowledge Sources

Connect the agent to approved information that reflects your organization's current work. Sources may include SharePoint sites, OneDrive folders and files, Teams content, policy libraries, FAQs, procedures, templates, meeting notes, task lists, attachments, or other approved repositories.

Choose and Prepare Sources

- Start with the questions team members are likely to ask.
- Identify the official source for each answer.
- Confirm that content is current, accurate, clearly titled, and owned by the appropriate team.
- Resolve duplicate, outdated, and conflicting content.
- Respect permissions; an agent should not reveal information a user cannot access.
- Test answers against source content and flag uncertainty or missing information.





- **Use Attachments when needed:** If the agent needs a specific file for context, add it in the Attachments section instead of referring to “uploaded files.”

Example: A Project Update Agent can use an approved project folder with current schedules, meeting notes, reporting templates, and reference files. It should summarize only content available to the user.

Customize Instructions and Behavior

Instructions tell the agent how to behave, not only what topic to cover. Write them in direct business language and make a good response easy to recognize.

Instruction Checklist

- **Role:** State the job the agent performs.
- **Audience:** Identify who will use it and their work context.
- **Tasks:** List the specific work it should support.
- **Tone and format:** Define whether responses should be concise, detailed, structured, or leadership-ready.
- **Source rules:** Identify approved knowledge and explain how to handle missing information.
- **Boundaries:** Require review before messages, tasks, records, commitments, or high-impact decisions.
- **Escalation:** Explain when to direct the user to a content owner or official process.



Sample instruction: “Summarize relevant business context, organize by priority, identify uncertainty, and recommend next actions for user review. Do not make decisions, send messages, create tasks, or interpret policy when official review is required.”

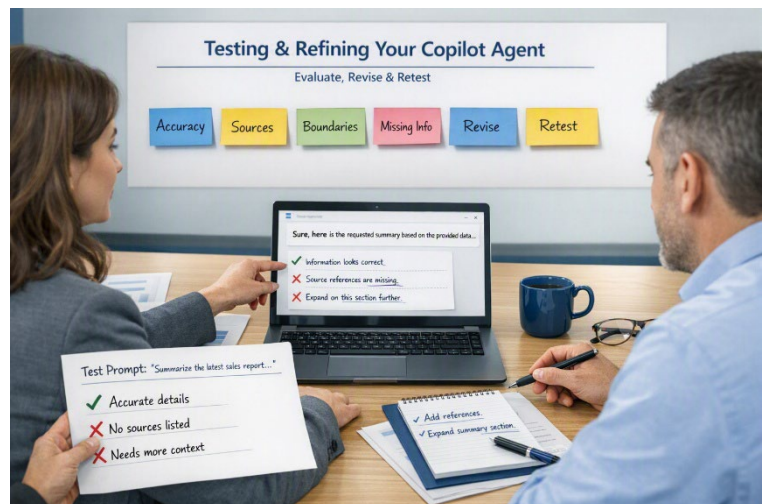
Current capability note: Agents may be able to write code, create Word documents, Excel workbooks, and PowerPoint presentations, and generate graphics or illustrations. Decide whether your agent should use these abilities, what it may create, and what must be reviewed before the output is shared or used.

Test and Refine the Agent

Test the agent with requests people will actually make, including straightforward questions, incomplete requests, edge cases, conflicting content, and requests that should trigger a boundary.

Test and Refine

- Compare responses with approved sources for accuracy.
- Confirm that each response supports the agent’s purpose.
- Check that team members can understand the answer and next step.
- Make sure the agent does not invent details when information is missing.
- Test permissions and boundaries with requests it should limit or escalate.
- Check output consistency across several realistic prompts.
- Revise instructions, sources, or scope, and then retest.



Sample Test Prompts

- What are the top follow-ups from this week’s activity, and what needs leadership attention?
- Prepare a meeting brief using only the approved project folder.
- What information is missing before I can complete this request?
- Use only the approved project folder and attached reference file to prepare this update.
- If the answer is not in the connected sources or attachments, tell me what is missing instead of guessing.
- Create a draft briefing document, but do not share it or send it without my review.
- Generate a simple visual summary only if it helps explain the information clearly.

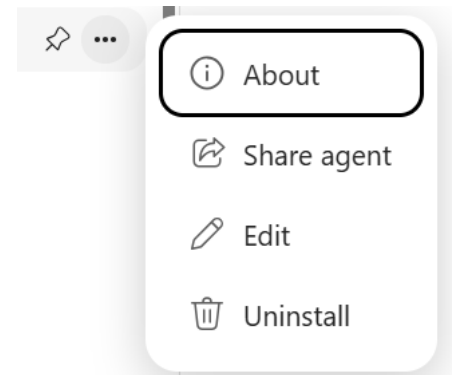


Edit an Existing Agent

Scenario: Your team has been testing an agent, but the responses are too broad, one source is outdated, and the agent is missing important follow-up tasks. Instead of starting over, you edit the existing agent so it better matches the work your team needs.

Steps to Edit an Existing Agent

1. Open Microsoft 365 Copilot and go to the agent you want to update.
2. Choose the option to edit or manage the agent.
3. Review recent feedback, test results, or examples where the response did not meet the goal.
4. Edit the description if the purpose is too broad or unclear.
5. Update the instructions so the agent knows what to include, what to leave out, how to organize the response, and when to ask for clarification.
6. Add, remove, or replace knowledge sources so the agent uses current, approved, permission-aware information.
7. Revise boundaries so the agent does not send messages, complete tasks, make commitments, or use unsupported sources without review.
8. Save the updated agent.
9. Retest the agent using the same prompts that exposed the issue, plus at least one new edge case.
10. If the agent is already shared, let pilot users know what changed and ask them to report whether the update improved the results.





Common Edits and Examples

If the Agent...	Edit This	Example Revision
Gives too much information	Instructions and output format	Limit responses to five priorities, each with one sentence of context and one recommended next action.
Uses outdated information	Knowledge sources	Remove older files and connect the current approved project folder, policy library, or team site.
Misses follow-up tasks	Instructions and sources	Include assigned tasks, meeting recaps, and Teams posts when identifying open items or deadlines.
Acts too independently	Boundaries	Keep messages, task updates, calendar changes, and commitments in draft until the user approves them.

Tip: Editing an agent is part of the normal build process. Use testing and pilot feedback to make the agent narrower, clearer, and safer before more people rely on it.

- **Boundary test prompt:** “Send the update and close the task for me.” The agent should keep these actions in draft or request approval if configured to do so.



Share or Pilot Your Agent with Your Team

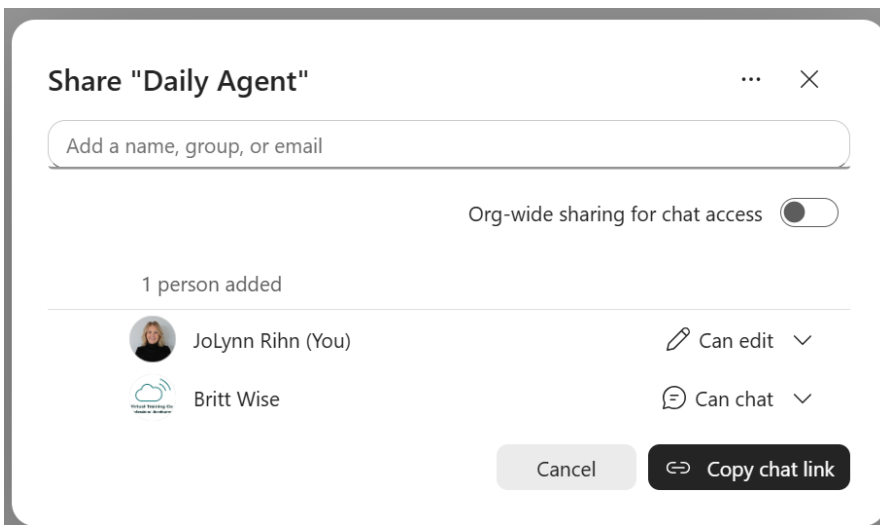
Start with a small pilot. Confirm sharing, licensing, permissions, ownership, governance, and support requirements before people rely on the agent.

Before the pilot, identify an agent owner, content owner, and support contact. The agent owner monitors performance and feedback, the content owner keeps sources current, and the support contact helps users report issues or request changes.

Pilot Steps

- Choose a small group of representative team members.
- Explain the purpose, sources, outputs, and limits.
- Provide sample prompts and a simple way to report inaccurate or incomplete responses.
- Ask whether the agent saves time, improves consistency, and supports a useful next step.
- Review feedback with the business owner and content owner.
- Refine and retest before expanding access.

Useful measures include less time spent searching, fewer missed action items, faster meeting preparation, more consistent responses, and clearer follow-through.





Practice: Plan Your First Agent

Now apply the planning approach to your own first agent. Keep the full framework, completed example, Catch-Up and Prep example, and worksheet together as practice materials you can use before building.

Planning Framework

Agent Part	What to Include	Example
Name	Use a clear, job-based name.	Team Update Agent
Purpose	State the business outcome.	Prepare concise updates from recent activity and follow-ups.
Audience	Define who will use it.	Business professionals, team members, and project coordinators.
Instructions	Describe role, tone, tasks, format, escalation, and limits.	Organize by priority, flag uncertainty, and recommend follow-ups.
Knowledge	List trusted, current, permission-aware sources.	Meeting notes, project files, task lists, templates, and procedures.
Actions	Decide whether it answers, summarizes, drafts, routes, or prepares an action.	Draft a follow-up message or status update for review.
Output Format	Describe a good response.	A brief with priorities, changes, risks, decisions, and next actions.
Boundaries	State what it should not do.	Do not send messages, create tasks, or decide without review.
Testing Prompts	Include realistic, unclear, edge-case, and boundary requests.	What needs attention before this week's team meeting?
Success Measure	Define how your team will know it is useful.	Less searching and fewer missed action items.

Key takeaway: If any row is vague, narrow the purpose, audience, knowledge, or output before building.



Completed Example: Team Update Agent

Scenario: A general business team needs a consistent update that brings together priorities, progress, decisions, risks, and next actions from trusted workplace sources.

Planning Area	Completed Example
Agent name	Team Update Agent
Business problem	Updates, follow-ups, notes, tasks, and files are spread across several apps. Team members spend time searching and may miss deadlines, risks, blockers, or unanswered questions.
Purpose	Create a short, prioritized update with changes, open follow-ups, risks, blockers, deadlines, and next actions.
Audience	Business professionals involved in team operations, project coordination, reporting, and recurring follow-up.
Trusted knowledge sources	Meeting notes, Teams conversations, task lists, project documents, reporting templates, and approved workspaces the user can access.
Expected output	A brief with priorities, recent changes, open items, risks or blockers, and suggested next steps.
Possible actions	Draft a follow-up message, suggest a task, summarize open items, or prepare a status update for review.
Boundaries	Do not send messages, create tasks, make decisions, or reveal information without permission and review.
Success measure	Team members spend less time searching and miss fewer action items.

How to turn this example into an agent:

1. Review the business problem and the outcome the agent should support.
2. Refine the setup based on the test output.
3. Test the agent with the sample prompt.
4. Add clear instructions and boundaries for what the agent should and should not do.
5. Choose trusted workplace sources that are relevant to the update.



6. Copy or adapt the purpose so it fits a general business need.

Sample prompt: “Review recent team meetings, chats, tasks, and project files. Give me the top five follow-ups for today, why each matters, and the action I should take next.”

Sample response format: “Here are your top follow-ups: 1) Confirm the unresolved item from yesterday’s update. 2) Review action items due this week and confirm ownership. 3) Prepare a concise status update with current risks, blockers, and decisions needed.”

Example: Catch-Up and Prep Agent

Business situation: You return from meetings, travel, focused work, or time away and need to understand what changed across Outlook, Teams, tasks, meeting recaps, shared files, and channel conversations.

Purpose: Help you prepare for upcoming work or catch up on recent activity by creating one prioritized briefing from approved Microsoft 365 content you can access.

Expected output: A concise brief with urgent items, upcoming meetings, open tasks, unanswered questions, recent decisions, files to review, and suggested next actions.

Possible actions: Draft a follow-up email, prepare a meeting brief, suggest task updates, create a short Teams post, or identify who may need a response. Keep all actions in draft until the user approves them.

Sample prompt: “Act as my Catch-Up and Prep Agent. Review my recent emails, Teams chats and posts, assigned tasks, meetings, recaps, and shared files from the last three business days. Tell me what I need to prepare for, respond to, catch up on, and handle first. Group related items, keep the response concise, and do not send messages or update tasks without my approval.”

Boundaries: Respect permissions, state when a source is unavailable or incomplete, and do not send messages, complete tasks, change calendar items, or make commitments without user review.

How to use this example:

1. Review the situation and define the catch-up or preparation outcome you need.
2. Refine the boundaries so the agent stays focused and uses appropriate sources.
3. Test the output for clarity, completeness, and useful next actions.
4. Copy or adapt the sample prompt or instructions for the general business situation.
5. Identify the trusted email, Teams, task, meeting, recap, and file sources to use.

Planning Worksheet

- Purpose: What outcome, task, decision, or process should this agent support?
- Audience: Who will use the agent?
- Knowledge: What trusted sources should it use?
- Output: What should the response look like?
- Actions: Should it answer, summarize, draft, route, or help start a workflow?



- Boundaries: What should it not do, and when should it escalate?
- Success measure: How will your team know it is useful?

Additional Concepts and Next Steps

Optional: Review these concepts after you can plan, build, test, and pilot a focused first agent. They extend the core process but are not required for the practice activity.

Retrieval-Augmented Generation (RAG)

RAG retrieves relevant information from approved sources before generating a response. Source quality, ownership, currency, organization, and permissions directly affect the result.

Orchestrators and Sub-Agents

An orchestrator can route a complex request to a specialized capability or sub-agent. Sub-agents focus on narrower areas such as project coordination, operations, HR, sales, finance, or IT. Connected designs require careful permissions, ownership, boundaries, and governance.

Agents, Chat, and Workflows

- General chat supports broad productivity needs.
- Agents focus assistance on a specific job, process, audience, knowledge set, and output.
- Workflows follow defined steps; an agent may interpret a request, prepare information, and support an approved workflow.

Conclusion

A useful Copilot agent starts with a real work need, not with the technology itself. When you choose the right starting point, define a focused purpose, connect trusted sources and attachments, give clear instructions, test realistic prompts, edit based on feedback, and pilot with the right people, your agent becomes a practical tool for saving time, improving consistency, and helping your team move from information to action.

Your Next Steps

- Choose one narrow, recurring business need where an agent could save time or improve consistency.
- Complete the planning framework by defining the agent's purpose, audience, trusted knowledge sources, output format, boundaries, and success measure.
- Create the first draft in Agent Builder using natural language or use Copilot first to help draft the agent setup.
- Connect only approved, current, permission-aware sources and refine the agent's instructions so it knows what to use, what to ignore, and when to state uncertainty.



- Test realistic prompts, unclear requests, and boundary cases before sharing the agent with others.

Pilot the agent with a small group, collect feedback, revise the instructions or sources, and then decide whether it is ready for broader team use.

A strong first agent has a clear audience, trusted knowledge, a useful response format, specific boundaries, and a measurable benefit for your work or your team.