

Score ten of your team's tasks

Write ten tasks that eat the team's week. For each, answer the three questions, set the ceiling, and pick the tool. Then start every task at level 1 or 2, whatever its ceiling.

TASK	1. Can it be undone easily?	2. Does it leave the team?	3. Does it read outside content?	Ceiling level	Tool: Chat, Deep research, Agent or Automation
EX Research a company before a call (illustration)	Yes	No	Yes	Ceiling 3, start at 1	Deep research
01	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No		
02	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No		
03	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No		
04	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No		
05	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No		
06	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No		
07	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No		
08	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No		
09	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No		
10	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No		

SETTING THE CEILING

- Start from 4. "No" to question 1, or "Yes" to question 2: 3 at most.
- "Yes" to question 3: it may not also send, pay or delete without asking. 3 at most, with the approval set in the tool.
- Runs on a schedule or on an event: 1. Decisions about people: none.

PICKING THE TOOL

- **Chat:** one answer you will use yourself.
- **Deep research:** many sources, found and cited.
- **Agent:** the next step depends on what it finds.
- **Automation:** every step can be written down in advance.

Up one level after five clean runs; down at once after a surprise. To score the list with the whole team, use Workshop in a Box: Brief an Agent.

Questions for your IT or admin

Ten questions to ask whoever runs your organisation's AI tools before your team hands work to agents. Write the answers in, and keep this with your rules sheet.

ASKED _____ DATE _____

01 Who owns our agents?

Who approves a new agent or a new connection? Who do we tell when one does something odd?

02 Do agents act as us, or as themselves?

Do agents get their own identity or account, or do they use ours? Can we tell their actions from ours afterwards?

03 Where is the record of what an agent did?

Is there an audit trail? Who can read it, how long is it kept, and can it be changed?

04 Which apps may we connect?

Which connectors are allowed? Which of them can write (send, edit, delete), and can those be set to ask first?

05 Which approval modes may we use?

Can modes that skip approvals be turned off for our team?

06 Can agents browse, or use our signed-in browser?

Is browser use on for us? Which sites are blocked?

07 What may run on a schedule or start on an event?

Is there a list of what is scheduled now, with an owner for each?

08 What do our assistants remember, and where does our data go?

What is memory set to by default? Is our data used for training? Where is it processed and kept?

09 Who checks a skill or plugin before we install it?

Is there an approved list?

10 How do we pull the plug?

How do we stop every agent at once, who can do it, and has anyone tried it?

WHY ASK: UK NCSC, 20 AUG 2026

It advises "making named individuals or group responsible for agentic AI activities", and says "All agents should be assigned their own unique identity in a class which differentiates them from human or individual systems."