

Is this agent ready for production?

Answer yes or no for one agent. Every "no" is a question IT, security, architecture or finance will ask. Fix it before the meeting, or bring the plan to fix it.

Agent:

Owner:

Users (group):

Date:

IT ASKS

- 1 The agent is in a list of agents, with the person who made it and who may use it.** ☐ Yes ☐ No
Good answer: one list with maker, users, systems, model and location.
- 2 People sign in to it through your identity provider.** ☐ Yes ☐ No
Groups follow your directory, so joiners and leavers are handled there.
- 3 It runs where your data is allowed to be.** ☐ Yes ☐ No
Vendor cloud, your own cluster, or air-gapped.

SECURITY ASKS

- 4 It reaches each system with the access of the person who asks, or with a narrow account made for it.** ☐ Yes ☐ No
No shared admin account behind a shared agent.
- 5 Risky actions wait for a named person to approve them.** ☐ Yes ☐ No
Good answer: list the actions that wait, and who decides each one.
- 6 Every action it takes is recorded under the person who asked.** ☐ Yes ☐ No
Including who approved or declined each held action.

ARCHITECTURE ASKS

- 7 You can move it to another model in one place, without changing code.** ☐ Yes ☐ No
Good answer: the agent's model is a platform setting. Change it in one place, and new conversations use it. People's tools call an alias with a fallback.

FINANCE ASKS

- 8 It has a budget, and the budget stops it, not only reports it.** ☐ Yes ☐ No
Good answer: a monthly cap per agent and per person, a warning at 75%, a stop at 100%.