

The Agent Governance Readiness Checklist

Thirteen questions about your agent estate. Most organisations answer four to six.

How to score. One point per question you can answer **with evidence, not intention**. If the honest answer is “probably, but I would have to check”, that is a no. Tick as you go and total each section.

Ownership and accountability	Yes	No / unsure
1. Does every agent running in production have a named accountable owner who is a current employee?		
2. Is it documented who has authority to approve an agent for production, and does that authority vary by risk tier?		
3. Do the people actually building agents know who that approver is, without having to ask?		
4. Is there a defined escalation path, with a named recipient, for when an agent behaves unexpectedly?		

Subtotal: ____ / 4

Inventory and classification	Yes	No / unsure
5. Do you have a complete inventory of agents, including those built outside IT by business users?		
6. Do you have an agent risk classification scheme with defined tiers, and is every agent assigned to one?		
7. Can you list which agents interact directly with people or generate content that requires marking under Article 50 of the EU AI Act, in force since 2 August 2026?		

Subtotal: ____ / 3

Scope and authorisation	Yes	No / unsure
8. Is it documented, per agent, which tools, connectors and data sources it is authorised to call?		
9. Are scope boundaries and action approval gates defined by risk tier, rather than agent by agent?		
10. Are human-in-the-loop requirements specified per risk tier and technically enforced — not merely documented as expected practice?		

Subtotal: ____ / 3

Lifecycle	Yes	No / unsure
11. Is there a review cadence and a re-certification schedule, with a date for the next review of each agent?		
12. Is there a defined retirement process for agents, and a way to detect agents whose owner has left or whose purpose has lapsed?		
13. Does your audit trail record each tool the agent invoked — every connector query, data source read and outbound action — or only the prompt and the final response? If an agent sent an email or wrote to a system last week, can you retrieve the recipient, the content and the timestamp?		

Subtotal: / 3

TOTAL: / 13

11-13	You are ahead of almost every organisation of your size. Your exposure is in the detail, not the structure.
6-10	The common position. You have an inventory; you do not yet have an operating model. The gap usually shows up first in lifecycle and audit.
0-5	Normal, and not a criticism. The platform arrived faster than the rules. Almost nobody built the governance before the agents.

The gap is not a technology problem. Microsoft Agent 365 gives you the registry, the lifecycle controls and the approval flows. What no platform decides for you is who approves what, at which tier, on what evidence, and how often it is reviewed. That part is an operating model, and it has to be designed.

Want to work through this against your own estate?
A 60-minute review scores all thirteen points against your environment, followed by a written note on your three highest-risk gaps. [\[booking link\]](#)