

Use this checklist to assess whether your organisation is ready to deploy AI Agents **safely, responsibly, and at scale**.

You do **not** need to answer “yes” to everything but unanswered questions represent **risk**.

1. Strategy and Value

- We can clearly articulate *why* we are deploying AI Agents
- The expected business outcomes are measurable and owned
- AI Agents are aligned to strategic priorities, not experimentation
- There is agreement on where AI should **not** be used

2. Accountability and Ownership

- A named executive is accountable for AI Agent outcomes
- Decision rights for AI-driven actions are clearly defined
- Escalation paths exist when AI outputs are disputed
- Ownership does not sit solely with IT or vendors

3. Governance and Oversight

- AI Agent decisions can be explained to non-technical stakeholders
- We can demonstrate how AI decisions are logged and reviewed
- Governance exists beyond initial deployment
- AI Agents are included in existing risk and assurance frameworks

4. Risk, Legal and Compliance

- Regulatory obligations related to AI are understood
- Legal accountability for AI-driven actions is clear
- We understand where AI Agents interact with sensitive data
- There is a defined process for incidents or unintended outcomes

5. Security and Controls

- AI Agents operate within defined security boundaries
- Identity, access, and privilege controls are enforced
- We understand how AI Agents connect to systems and data
- Third-party and supply-chain risks are assessed

6. Operating Model and Change

- Teams understand how AI Agents will change day-to-day work
- Human oversight responsibilities are defined
- Training and adoption have been considered
- Change impact has been assessed, not assumed

7. Data and Decision Quality

- AI Agents are trained on relevant, controlled data
- Data quality and bias risks are understood
- We know how AI decisions will be validated over time
- There is a process to retrain or retire agents safely

8. Auditability and Assurance

- AI Agent actions are traceable
- Decisions can be reconstructed after the fact
- Independent assurance is possible if required
- We are comfortable defending AI use to boards, auditors, and regulators

Interpreting your results

- **Mostly Yes** - You may be ready to proceed with governance
- **Mixed** - High likelihood of stalled pilots or blocked deployment
- **Mostly No** - AI Agents introduce unmanaged risk today

The **AI Agent Reality Check** will help turn this checklist into **clear decisions**.

[Book an AI Agent Reality Check](#)

About oxhey.ai

oxhey.ai helps organisations move from AI intent to **trusted, governed AI Agents** safely and at scale.

We design, govern, and embed AI Agents that deliver measurable outcomes while meeting the expectations of boards, regulators, security teams, and the people who rely on them day to day.

Our work is grounded in decades of experience delivering complex enterprise change, cybersecurity programmes, and high-stakes transformations across regulated industries.

No hype. No uncontrolled pilots. Just structured, defensible AI that leaders can stand behind.

How to connect with us

If you have questions about AI readiness, governance, or next steps after completing this assessment, we're here to help.

Book a conversation

Schedule a short, no-obligation discussion with an oxhey.ai specialist.

Email

contactus@oxhey.ai

Phone

+61 (0)2 9188 1681

Learn more

Visit www.oxhey.ai for insights on AI Agents, governance, and responsible adoption.