The agent governance checklist

Comonad Limited

One page, free to print or download. No email needed.

[ ] Every agent has its own identity, with no shared human accounts or long-lived shared keys.

[ ] Every agent has a named owner.

[ ] Each permission is scoped to the task and granted for a limited time.

[ ] Actions on behalf of a person carry that person’s delegated authority, and nothing more.

[ ] Policy is checked at each tool call, at the moment of action.

[ ] High-impact actions need a person’s approval.

[ ] Every action is logged: which agent, for whom, under which policy, with what result.

[ ] Logs are kept where your security team can see them, for an agreed period.

[ ] Each agent is evaluated before release and after every change.

[ ] Content the agent reads from outside is treated as untrusted.

[ ] There is a documented way to stop each agent, tested before go-live.

[ ] Agents are reviewed and retired when their purpose ends.

https://comonad.co.uk/guides/ai-agent-governance-framework