

AI Agent Governance Checklist

By Dux Raymond Sy

<http://dux.ai>



A short team review for AI agents and workflows that use tools or take action. Examples include an internal knowledge assistant, a customer-service agent or IT automation. The next page contains nine confirmations across Observe, Protect, Govern and Optimize.

Observe

Know what is running.

Protect

Secure data, contain harm and recover.

Govern

Assign ownership and enforce permissions, policies and approvals.

Optimize

Prove value and manage cost.

Purpose

Catch important gaps before an agent launches or gains more authority. Finish with a decision to Proceed, Limit or Hold, an approved scope and clear next actions.

Who it is for

Business leaders accountable for the outcome, process owners responsible for the workflow, and IT or security leads who can verify the controls. Bring in other specialists when the use requires them.

When to use it

Bring one workflow to your existing launch or change review, after setup and testing. Revisit affected checks after an incident and at the agreed review date. If tests are not ready, use the implementation guide first.

How to use it

1. Agree the workflow, accountable owner and intended outcome.
2. The accountable owner leads the checks aloud. Process and IT leads bring current tests or settings. Mark any applicable part that is partial, failed or unknown as Gap. Use N/A only when the whole check does not apply to this scope; record why.
3. Invite concerns. Proceed only with confirmed checks and required approvals. Limit use to a smaller scope with verified safeguards, or Hold the affected use. Record scope, next actions, owners and dates.
4. Use the optional AI Agent Governance Implementation Guide when a check needs explanation or work. Return to this checklist to record the decision.

Print or use page 2 for the team review. Keep this introduction as a quick reference.

AI Agent Governance Checklist

For business leaders, process owners and IT decision makers. Use this page to confirm critical checks before an AI agent launches, gains more authority or changes materially.

The accountable owner leads the review aloud. Process and IT leads confirm what they can verify from current tests or settings. If any applicable part is unverified, mark Gap. Use N/A only when the whole check does not apply to this scope; record why. Anyone can raise a concern.

Agent or workflow and version _____ Accountable owner _____

Intended outcome _____ Review date _____

Yes = confirmed by evidence Gap = partial, failed or unknown N/A = not applicable to this scope; explain why

Observe	Yes	Gap	N/A
01 Inventory and sources checked. Agents, models, tools and data dependencies are listed; owners and sources are current.	☐	☐	☐
02 Important activity traceable. We can trace an important action or answer to its request, authority or required approval, and result.	☐	☐	☐
Protect	Yes	Gap	N/A
03 Stop and recovery rehearsed. We can contain activity and restore needed data and settings. We have a plan for effects that cannot be undone.	☐	☐	☐
04 Malicious instructions tested. In tested attacks, prohibited actions stayed blocked; remaining limits are recorded.	☐	☐	☐
Govern	Yes	Gap	N/A
05 Access limits tested. Access is purpose-limited; denied requests and permission removal are tested.	☐	☐	☐
06 Data policies enforced. We tested where data may go, how long it is kept and where it may be stored.	☐	☐	☐
07 Human approval tested. Tests block execution without required human approval.	☐	☐	☐
Optimize	Yes	Gap	N/A
08 Quality and value tested. Realistic results meet quality requirements and justify the work and cost.	☐	☐	☐
09 Usage limits tested. Tested limits control spending and runaway activity.	☐	☐	☐

Decision ☐ Proceed ☐ Limit ☐ Hold

Ask together: Any unresolved concern? **Proceed:** applicable checks are confirmed and required approvals complete. **Limit:** confirm applicable checks and required approvals for a smaller scope; set a review date. **Hold:** do not enable the affected use while a critical safeguard is unknown or failed.

Link existing evidence below. Give every gap an action, owner and date in your task list; record N/A reasons and restart conditions.

Evidence and gap record link or ID: _____

Approved scope: _____ Decision owner: _____

Next action: _____ Owner: _____ Due: _____

Next review date: _____ Recheck after material changes or incidents. Ownership and the intended outcome must be agreed before proceeding.

Practical review aid, not a compliance certification. Use the optional implementation guide to close gaps.