

Neotheta Enterprise AI Control Plane Readiness Checklist

September 11, 2026 Edition

Use this worksheet before moving an AI assistant, agent, or model-powered workflow from experimentation into production. Mark each control **Ready**, **Needs evidence**, or **Not applicable**, and assign an owner.

1. Use Case and Authority

Check	Owner	Status / Evidence
The business outcome and measurable success criteria are defined.		
The workflow's permitted actions and prohibited actions are documented.		
A named business owner can approve, pause, or retire the workflow.		
Human approval is required for irreversible, financial, legal, safety, or external-facing actions.		
Maximum task scope, time, spend, and action count are bounded.		

2. Identity, Permissions, and Tool Access

Check	Owner	Status / Evidence
The workflow uses a dedicated service identity rather than a personal credential.		
Permissions follow least privilege and are separated by environment.		
Credentials are short-lived, rotated, and revocable.		
Tool calls, destinations, and egress paths are allow-listed.		
External actions have idempotency, rollback, or a compensating procedure.		

3. Data and Model Boundaries

Check	Owner	Status / Evidence
Sensitive data classes and allowed model destinations are documented.		
Retention, training-use, residency, and deletion terms are verified.		
Retrieval sources are permission-aware and traceable to source records.		
Model and prompt versions are recorded for material outputs.		
Open-weight, managed, and custom-infrastructure trade-offs are documented.		

4. Evaluation and Observability

Check	Owner	Status / Evidence
Evaluation covers task success, refusal quality, latency, cost, and policy compliance.		
Tests include adversarial prompts, tool misuse, prompt injection, and data exfiltration.		
Every action produces an immutable or access-controlled audit record.		
Alerts exist for anomalous volume, destinations, privileges, and repeated failures.		
Users can inspect source evidence and distinguish model output from verified facts.		

5. Operations and Incident Response

Check	Owner	Status / Evidence
A kill switch can stop the workflow and revoke its credentials.		
Incident severity, escalation, communications, and evidence-preservation rules are defined.		
Recovery and rollback have been tested in a non-production environment.		
Vendor incident disclosure, support, and service-level obligations are documented.		
Review cadence is defined for model updates, tools, data, and policy changes.		

6. Executive Gate

Before approval, answer in one sentence each:

1. What value does this workflow create that a non-agentic process cannot create as effectively?
2. What is the worst plausible failure and how quickly can the organization stop it?
3. What evidence will demonstrate that the workflow is reliable, compliant, and economically worthwhile?
4. Which dependency could create unacceptable vendor, infrastructure, or data-residency exposure?
5. Who has authority to pause or retire the workflow?

Decision: ☐ Approve pilot ☐ Approve limited production ☐ Require remediation ☐ Do not proceed

Review date: _____ **Executive owner:** _____

Prepared by Neotheta – AI Research Lab. This checklist is an operational planning aid, not legal, security, medical, or regulatory advice.