

Agentic AI Deployment Pack

Readiness checklist — 20 checks across 5 categories. Nothing proceeds until every box is honestly ticked.

Pack	Agentic AI Deployment Pack
Document	Readiness checklist (20 items)
Use	Gate reviews · phase entry criteria · go/no-go
Date	2026-09

AnovaCloud — Engineering the AI-Native Enterprise. Frisco, Texas. This pack is a working instrument, not a brochure: complete it with your team, score honestly, and bring it to your discovery call. © 2026 AnovaCloud.

USE CASE & SCOPE

Use case & scope

☐

Use case scored ≥ 3 on candidacy

Questionnaire sections 1-2 average ≥ 3 ; weak use cases deferred in writing.

☐

Success criterion written

One-sentence objective acceptance criterion, agreed with the business owner.

☐

Blast radius documented

Worst-case failures listed with reversibility and customer impact per action.

☐

Autonomy tier assigned

Copilot → supervised → autonomous; starting tier explicit, not aspirational.

TOOLS & DATA

Tools & data

- ☐ **Tool contracts frozen**
Every tool has a versioned schema, auth, timeout, retry, and idempotency contract.
- ☐ **Sandbox parity**
Staging replicas of all integrated systems available for agent testing.
- ☐ **Data access governed**
Row/document-level access control enforced on everything the agent can read.
- ☐ **Rollback paths defined**
Every mutating action has a tested reversal procedure.

EVALUATION

Evaluation

☐

Golden task set built

≥50 tasks with expected outcomes and grading rubrics for the target use case.

☐

Eval harness automated

Task success, tool correctness, latency, and cost measured on every run.

☐

Regression gate in CI

Model, prompt, or tool changes cannot ship without passing the eval gate.

☐

Failure-mode register

Known failure modes listed with detection and mitigation each.

SAFETY & COMPLIANCE

Safety & compliance

☐

Prompt-injection controls

Input handling, instruction hierarchy, and tool-output validation implemented and tested.

☐

Least-privilege permissions

Agent identity scoped per use case; secrets vaulted and rotated.

☐

Red-team pass complete

Adversarial testing done; findings remediated or risk-accepted in writing.

☐

PII handling verified

Redaction on prompts, tool I/O, and logs; data-retention policy applied.

OPERATIONS

Operations

- ☐ **Full tracing live**
Every run traceable: prompts, tool calls, decisions, costs; retention per policy.
- ☐ **Approval workflow live**
Human gates enforced in the path, not documented beside it.
- ☐ **Cost guardrails live**
Per-task budgets and spend-anomaly kill switches configured and tested.
- ☐ **Incident runbook published**
Halt, rollback, and comms procedures rehearsed with the on-call team.

SIGN-OFF

Checked means done, not planned

Each category owner initials when every item is complete with evidence attached. Items marked N/A need a written reason — 'not applicable' without justification scores as incomplete.

Use case & scope

Owner _____ Date _____

Tools & data

Owner _____ Date _____

Evaluation

Owner _____ Date _____

Safety & compliance

Owner _____ Date _____

Operations

Owner _____ Date _____