AI Agent Deployment Checklist

SOLUTIONS24X7 · TCS FRAMEWORK | STARTER EDITION

What to define, test, and verify before any AI agent goes live. Starter Edition shows Phases 1–2 of 7.

About This Document

42 checks across 7 phases. Complete all phases before go-live. Pair with the AI Risk Assessment Checklist and HITL Pattern Library.

Phase 1 · Problem Definition & Scoping

- ☐ 1.1 Business problem clearly defined — not "use AI" but a specific outcome
- ☐ 1.2 Success criteria agreed and measurable before build begins
- ☐ 1.3 Out-of-scope scenarios documented
- ☐ 1.4 Human touchpoints identified — what does the agent escalate, hand off, or defer?
- ☐ 1.5 Data inputs inventoried — sources, formats, refresh frequency
- ☐ 1.6 Data classification confirmed — what tier is the agent working with?

Phase 2 · Model & Stack Selection

- ☐ 2.1 Model selected with documented rationale (capability vs cost vs latency)
- ☐ 2.2 Fallback model defined in case primary model fails or rate-limits
- ☐ 2.3 Model routing layer configured (gateway, load balancing, caching)
- ☐ 2.4 Token budget established — max input + output per call
- ☐ 2.5 Tool / function call list finalised — agent cannot call tools outside this list
- ☐ 2.6 Memory strategy defined — stateless, session, persistent, or vector
- ☐ 2.7 Prompt version controlled — system prompt stored in version control

---

— Phases 3–7 (Guardrails & Safety · Integration & Testing · Observability · Governance · Go-Live) in Full Version — 28 additional checks —

Deployment Summary Record

Field	Value
Agent name	
Agent ID	
Owner	
Launch date	
Model(s)	
Rosetta layer	Intake / Orchestration / Execution / Automation
Data classification	Public / Internal / Confidential / Restricted
HITL required	Yes / No — trigger:
Review date	
Sign-off	

What's in the Full Version?

- Phase 3: Guardrails & Safety (8 checks) — input/output validation, PII detection, HITL trigger points, jailbreak testing.
- Phase 4: Integration & Testing (7 checks) — dependency testing, load testing, regression suites.
- Phase 5: Observability & Monitoring (6 checks) — logging, alerting, cost tracking, anomaly detection.
- Phase 6: Governance & Compliance (7 checks) — NHI identity, agent registry, EU AI Act checklist, rollback plan.
- Phase 7: Go-Live & Post-Deployment (6 checks) — canary rollout, user communication, deprecation criteria.

Full version included in our AI Framework Engagement — solutions24x7.com