

Production Deployment Checklist

- [Production Deployment Checklist](#)
- [Build Strategy](#)

Production Deployment Checklist

Before Launch

- Secrets in vault
- Rate limiting
- Retry logic
- Queueing
- Structured logs
- Health checks
- DB pooling
- CI/CD
- Rollback strategy
- Human approval console
- Policy engine live
- Audit logs enabled
- Monitoring dashboards
- Incident runbooks
- MCP servers pinned to a known-good tool-definition hash, with re-approval required on change (New)
- OAuth issuer validation enabled on every MCP client (New)

Build Strategy

Build in This Order

- Single agent + retrieval
- Add memory (start with Pattern B — retrieval-augmented)
- Add tools via MCP
- Add policy engine
- Add verifier
- Add human approvals
- Add multi-agent roles
- Optimize cost routing
- Formalize the harness — write down the planner/executor/verifier contracts and context-assembly rules as a versioned spec, not implicit code structure (New)
- Add simulations/evals, including harness-vs-model attribution (New)
- Expand autonomy slowly