



CLAUDE DEPLOYMENT CHECKLIST

September 2026

A Manager's Guide for Alternative Investment Funds



Claude is not one product or one risk profile. Web, CoWork, connectors, Desktop, Code, and Office tools expose different data and actions. Choose the right plan & approved entry points, & complete Atlas Tier 0 to reduce shadow AI & establishes core control hygiene required before production use.

Phase 1: Approve Tools, Assign Owner

- **Approved Tool Matrix:** Define who can use what, for which use case, under which exception path.
- **Enterprise Identity:** Require SSO, Conditional Access, MFA, approved groups, and fast offboarding for every AI surface.
- **Named Owner:** Assign one accountable internal owner for integrations, exceptions, and escalation.
- **Logging Baseline:** Establish who used which tool, against what data, and when. Document any platform logging gaps.
- **Shadow AI Cleanup:** Move users out of personal accounts and into sanctioned, managed tenants.
- **Claude Hardening:** Disable Cowork, Desktop, Chrome, Code, connectors, plugins, skills, & write actions by default. Enable & configure retention, sharing, feedback, web, network, & logging.

Phase 2: Plan, Data & Integrations

- **Plan:** Choose Claude Business or Enterprise intentionally based on identity, provisioning, retention, compliance, audit, and group- control needs. Ask Atlas for the separate comparison sheet.
- **Entry Points:** Approve each Claude surface separately. Cowork now runs on web and mobile as well as desktop. Desktop is not required and remains disabled under Tier 0 unless approved.
- **Data Scope:** Name the exact libraries, mailboxes, applications, and data classes Claude may access. Review permissions and external sharing before connecting content.
- **Read vs. Write:** Treat read-only and write-capable access as different risk classes. Allowlist connectors, MCP servers, plugins, and skills; review scopes and data flows before approval.

Phase 3: Pilot, Monitor, Expand

- **Pilot:** Start with named users, curated data, low-risk workflows, and human approval. Exclude regulated, investment, legal, and client-facing decisions.
- **Cowork:** Recommend only enabling on sandboxed computers. If approved on non-sandboxed computers, recommend restricting to designated group of users, require per-task approval for write actions, configure network access controls, and minimize integrations. Insight into and control over CoWork is limited; see Atlas CoWork Security Brief.
- **Monitor:** Review usage, exceptions, incidents, support requests, connectors, and business value. Treat new models, features, connectors, and retention changes as change-control events.
- **Expand:** Add users, data, or capabilities only after the named owner approves the prior stage.



- Sign up for Claude Enterprise & complete Atlas Tier 0 before use.
- Grant Atlas the required admin privileges in Claude so we can monitor configuration and make authorized client-requested changes.
- Provide Atlas w/ a senior AI owner, approved users, use cases, data sources, exception paths, as well as risk approvals.
- Keep Atlas involved as Claude capabilities and defaults change.