1. OPERATING CADENCE (90 DAYS)

Phase 0: Readiness (Week 0-1)
- Data residency + access model confirmed (in-region).
- Security baseline: RBAC, audit logging, PII masking, vendor review.
- Intake: top 5 workflows by value/risk; owners assigned.

Phase 1: Strategy Sprint (Weeks 1-3)
- Decision rights: Steering (CIO/COO/CFO), Design Authority (CAIO + Risk), Delivery (pods).
- Guardrails: model allowlist, prompt QA, red-team on high-risk flows.
- Outputs: ROI model, control checklist, comms plan, success metrics.

Phase 2: Build Sprints (Weeks 3-10)
- Pattern library: classification, extraction, routing, summarization, generation with human gate.
- Environments: dev/sandbox, staging with test data, prod with approvals.
- QA: dual review on finance/healthcare flows; sampling on low-risk ops.
- Metrics: cycle time, error rate, human touch rate, payback clock.

Phase 3: Operate (Weeks 10-12)
- Runbook: incident types, rollback steps, ownership per workflow.
- Governance: weekly steering, monthly risk review, quarterly model refresh.
- Change management: training, adoption score, opt-out/appeal path.

2. HUMAN-IN-LOOP PATTERNS

Validation tiers:

- Tier 1 (auto): low-risk (routing, tagging); sampled review.
- Tier 2 (approve): medium-risk (ops comms, tickets); human approve/reject.
- Tier 3 (co-create): high-risk (finance, clinical); human edits + sign-off.

Controls:

- Prompts versioned; changes require dual review.
- Outputs watermarked with source + model + time; stored in audit log.
- Data: PII masked before model; retention policy aligned to org standards.
- Vendors: allowed models list; fallback model for outages.

Org model:

- CAIO office: design authority, playbooks, model evaluations.
- Domain leads: workflow owners; accountable for outcomes and risk.
- Enablement: prompts, eval sets, red-team scripts shared centrally.

3. ROI & VALUE TRACKING

Core metrics:
- Efficiency: hours removed, cycle time delta, queue clearance.
- Quality: error rate vs baseline, dispute/appeal rate, rework.
- Financial: payback days, margin impact, working capital unlocked.
- Adoption: active users, human-touch rate, opt-outs.

Measurement cadence:
- Weekly: uplift vs baseline, incidents, human-touch %, sampling results.
- Monthly: payback tracker, cost-to-serve, compliance exceptions.
- Quarterly: model refresh, vendor check, security review.

Value portfolio (flower framework):
- Run the business: finance reconciliation, procurement, support.
- Grow the business: sales assist, personalization, lead qual.
- Protect the business: compliance checks, PII guardrails, auditability.

4. STACK & SECURITY (ENTERPRISE-READY)

Stack principles:

- Vendor-agnostic LLM layer; swap by use case and data residency.
- Retrieval layer with governance: approved sources, freshness, citations.
- Observability: traces, latency, cost per call, quality evals.
- Secrets: KMS-managed; no hardcoded keys; environment isolation.

Security + compliance:

- Data hosted in-region; no cross-border unless approved.
- SOC2/ISO roadmap; least-privilege RBAC; SSO/MFA enforced.
- Red-team: jailbreak testing on launch and on prompt updates.
- Incident playbook: detection, containment, rollback, comms.

5. 90-DAY LAUNCH PLAN (CHECKLIST)

Week 0-1: Intake + controls
- Name the workflows, owners, metrics, and risk tiers.
- Approve models/providers; set audit logging; mask PII.

Week 2-3: Design authority
- Sign off prompts, eval sets, rollback criteria.
- Align steering KPIs (hours, quality, payback).

Week 3-8: Build
- Ship 3-5 workflows; run QA; track human-touch %.
- Publish runbooks; train users; instrument dashboards.

Week 8-10: Harden
- Red-team; failover model; finalize SLAs; train support.

Week 10-12: Operate
- Weekly steering; monthly risk review; quarterly model refresh.

Deliverables you should demand:
- Control checklist; RACI; model/service bill of materials.
- Eval sets and quality thresholds; rollback triggers.
- ROI tracker; adoption dashboard; incident playbook.

6. HOW WE ENGAGE (FRACTIONAL CAIO OPTION)

Engagement model:
- Leadership workshop: align priorities, risk appetite, governance.
- Strategy sprint: roadmap + ROI + guardrails (capability framework).
- Delivery sprints: 3-5 workflows shipped with human-in-loop controls.
- Fractional CAIO: ongoing steering, audits, vendor management.

Why it works:
- Human-in-loop baked in; no shadow AI.
- In-region data + security-first; compliant by default.
- Co-owned with domain leaders; measurable payback in 90 days.

Call to action:
- Book a consultation at implementai.ae/contact.html
- Or start with the AI readiness check: implementai.ae/ai-readiness.html