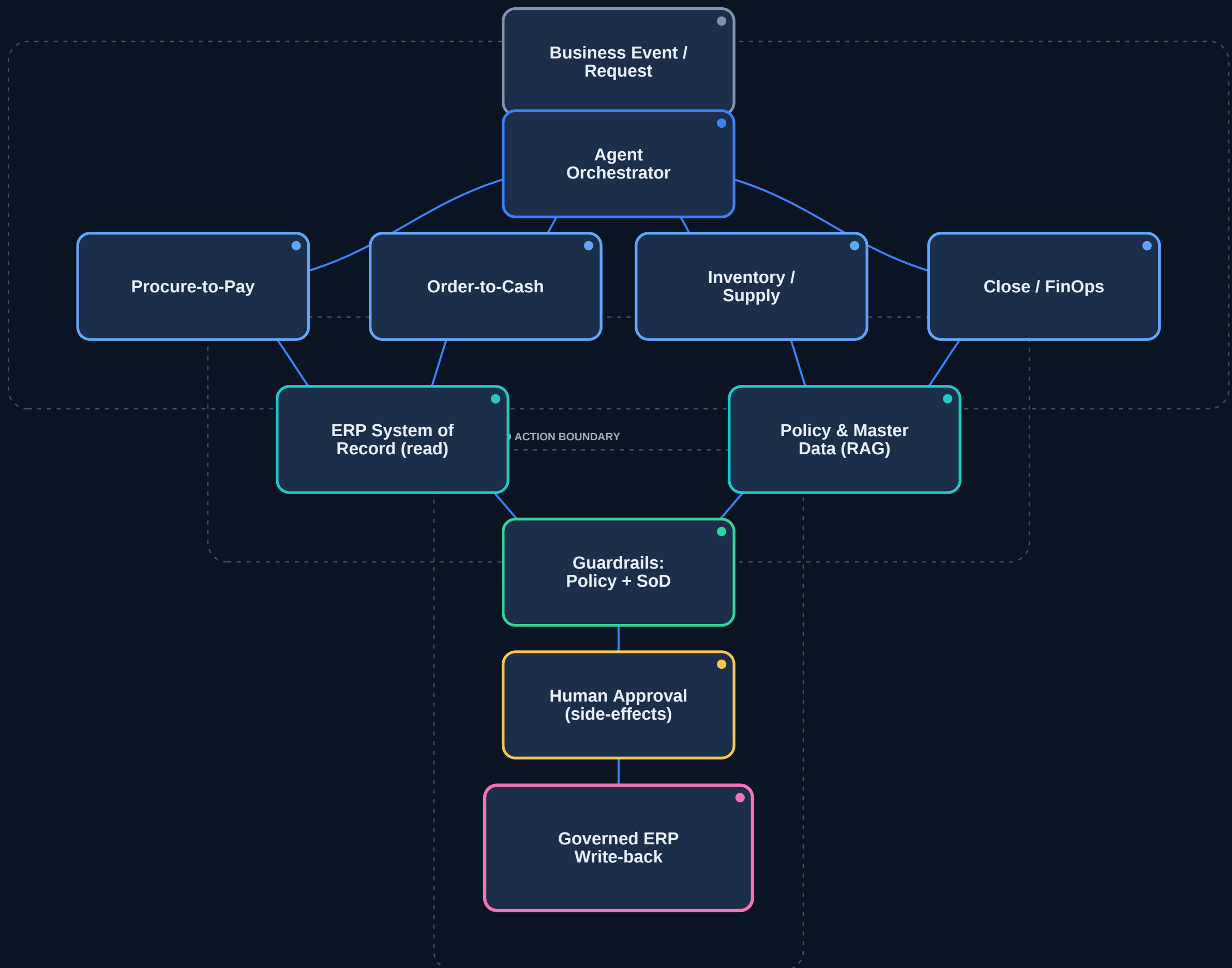


— REFERENCE ARCHITECTURE · ENTERPRISE

Agentic AI in Enterprise ERP

Putting agents into SAP, Oracle or Dynamics is a different game. The hard parts aren't the model — they're guardrails, cost boundaries, and a safe rollout.

Architecture · hurdles · guardrails · cost · rollout · specs →



Read freely, act carefully

Agents read the record freely (grounded), but every side-effecting action passes through one governed boundary: policy + SoD guardrails, human approval, and an idempotent, audited write-back.

Example: a \$48,200 PO; a \$49,900 invoice with a 3.5% overage breaches tolerance and is routed for approval before any posting.

Why ERP is different

- The ERP is the system of record — a wrong action costs real money, so determinism and auditability are non-negotiable.
- Strict RBAC and segregation of duties (SoD) — an agent must never hold more authority than the user it acts for.
- Heavy customization and brittle integrations — every SAP / Oracle / Dynamics estate is bespoke.
- Compliance is mandatory: SOX, GDPR, data residency — auditable controls, not good intentions.
- Scale and latency — high transaction volumes; agents can't bottleneck the month-end close.
- Hallucinated figures are unacceptable — grounding in the record is the price of entry.

The approach

- Read-then-act split: agents read freely (grounded), but every side-effecting action passes through one governed gateway.
- Ground every figure in the ERP record + policy — cite-or-refuse. No invented numbers ever reach a posting.
- Inherit the user's RBAC and enforce SoD: the agent's authority is capped at the user's, checked per action.
- Deterministic policy checks before posting (tolerances, GL validation, 3-way match) + human approval above thresholds.
- Idempotent, reversible write-backs with a full audit trail — who, what, why, model and prompt version.
- Tool RBAC: agents may only call the specific ERP APIs they're explicitly allow-listed for.

Keeping spend tied to value

- Per-agent and per-tenant token / \$ budgets with hard caps, alerts, and a loop budget (max iterations, tokens, wall-clock).
- Right-size the model per task: small models for extraction and classification, large models only for reasoning.
- Cache aggressively: a semantic cache plus cached master data and policies (CAG-style) kill repeat calls.
- Batch and run async for high-volume back-office work; reserve low latency for human-facing flows.
- Measure cost per workflow and per outcome — not per token — so spend ties to business value.
- Fail closed on budget exhaustion: return a partial result and escalate, never a silent overrun.

Earning autonomy in production

- Shadow mode first: the agent runs alongside humans, proposes actions, writes nothing — measure accuracy vs. people.
- Suggest -> approve: the agent drafts every action; a human approves before anything posts.
- Bounded autonomy: auto-execute only low-risk, high-confidence actions under value thresholds; everything else escalates.
- Feature-flagged canary by tenant, region, and workflow — dev-on, prod-canary; expand only on evidence.
- Continuous golden-set eval + drift monitoring + a kill switch: rollback is one flag flip.
- Widen the autonomy envelope only as measured accuracy and trust grow.

Ingress & orchestration

— Business Event / Request

Typed, traced ingress for any request

TECH Azure APIM + Service Bus / Event Grid; EDI (X12/EDIFACT), IDoc, webhook, batch; OAuth2 OBO

CTRL Edge AuthN (JWT / WAF / rate-limit); schema validation; idempotency key; PII tagging

— Agent Orchestrator

Plans, routes, holds process state

TECH .NET / Semantic Kernel on AKS or Container Apps; Durable Functions / Dapr Workflow; budget + circuit breakers

CTRL Tenant isolation + quotas; deterministic versioned routing; tool-RBAC allow-lists

Domain agents

— Procure-to-Pay

TECH SAP MM/FI (BAPI/OData), Oracle Procurement, Dynamics F&O; master data read-only

CTRL Authority <= user role; cite-or-refuse; proposes, never posts

— Order-to-Cash

TECH SAP SD/AR, Oracle Order Mgmt, Dynamics; pricing / credit / AR read

CTRL SoD: order vs. credit release; revenue-impacting actions to approval

— Inventory / Supply

TECH SAP MM/EWM, Oracle Inventory, Dynamics SCM

CTRL Plant / warehouse scoping; movement-type validation; idempotent keys

— Close / FinOps

TECH SAP FI/CO, Oracle GL, Dynamics Finance; GL + sub-ledger read

CTRL Preparer vs. approver SoD; SOX flagging; deterministic GL validation pre-post

Grounding — ERP + policy

— ERP System of Record (read)

Authoritative source of truth

TECH SAP OData v2/v4, BAPI/RFC, CDS views; Oracle Fusion REST; Dynamics Dataverse / F&O; APIM; change-data-capture

CTRL RBAC-scoped reads (OBO); field-level data residency / PII masking; read-only credentials

— Policy & Master Data (RAG)

Grounds decisions in org rules

TECH Vector store (Azure AI Search / pgvector), hybrid + rerank; lineage / version / effective-date; optional GraphRAG

CTRL Signed + versioned sources; classification-based access; effective-date (stale-policy) guard

Governed action boundary

— Guardrails: Policy + SoD

Integrity gate before any side effect

TECH Policy-as-code (OPA / Rego); SAP GRC SoD matrix; cite-or-refuse verifier (tolerances, 3-way match, GL validation)

CTRL Authority check (agent $\leq$ user); deterministic versioned rules; control-evaluation record for audit

— Human Approval (side-effects)

HITL sign-off for material actions

TECH SAP Fiori inbox / Teams actionable message / ServiceNow; threshold + risk-tiered routing; escalation on timeout

CTRL Approver authority + value limits; four-eyes / dual control; immutable decision record

— Governed ERP Write-back

The only governed write path

TECH Idempotent keyed writes (BAPI commit / OData change-set / Dataverse); saga + outbox; domain events (Service Bus / Kafka)

CTRL Reversible compensations, no partial commits; hash-chained / WORM audit (who/what/why + model & prompt); reconciliation

— YOUR TURN

Adding agents to your ERP?

I help enterprises and lean teams put agentic AI into ERP safely — grounded, governed, cost-bounded, and rolled out in stages. On Azure.

DM me “assessment”

Atiqul Islam

Fractional Cloud & AI Architect for SMBs · atiqulislam.dev