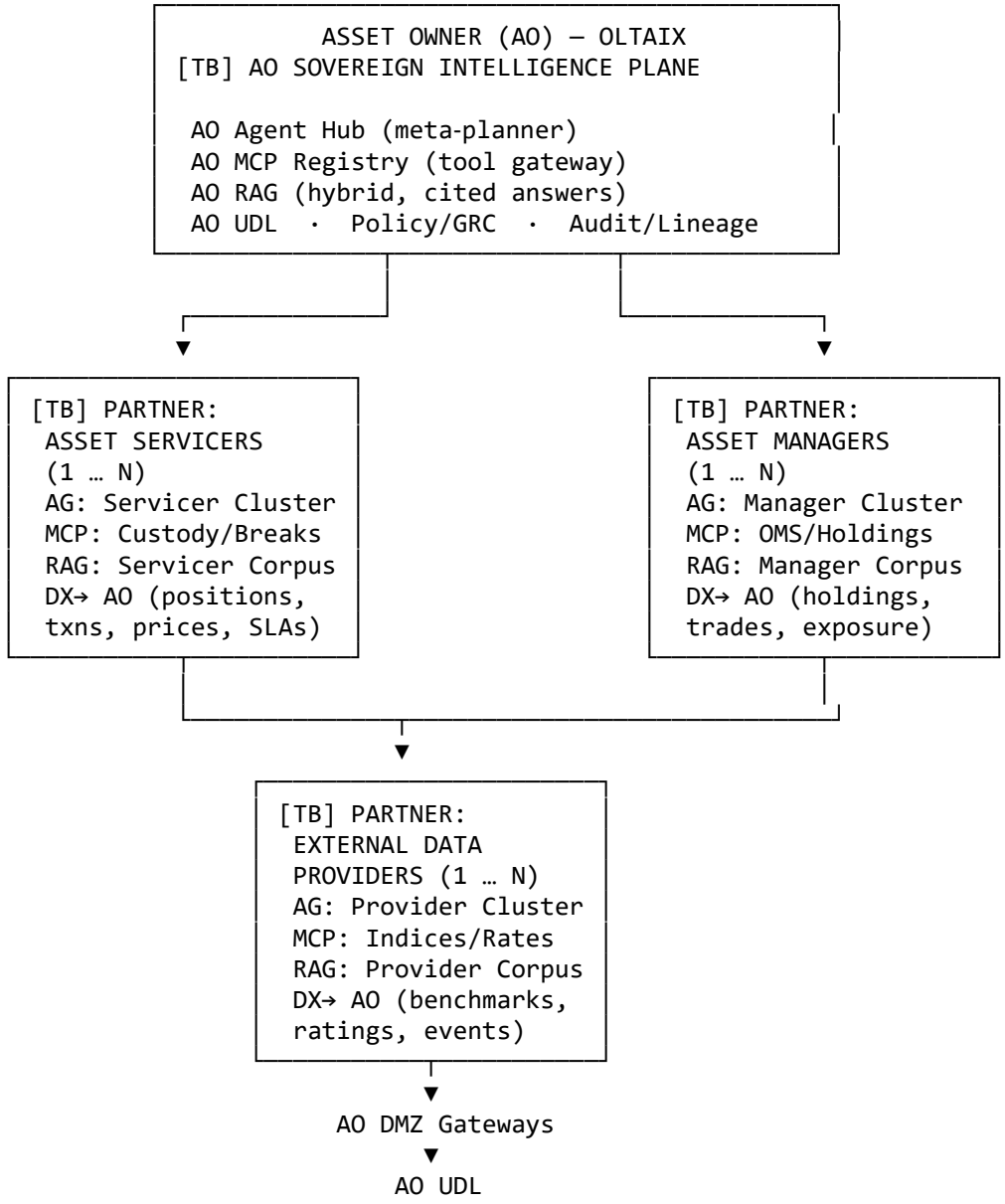
OLTAIX Topology — One Asset Owner with Three Partner Types (Asset Servicer, Asset Manager, Data Provider)

Goal: One Asset Owner (AO) operating OLTAIX where each **partner type** runs its own **Agentic AI cluster (AG)** with a dedicated **MCP registry** and **RAG index**. AO keeps sovereign control, evidence, and audit.

Legend: [TB]=Trust Boundary · AG=Agentic AI (planner/executor/critic) · MCP=Model Context Protocol · RAG=Retrieval-Aug. Gen. · DX=Data Exchange · UDL=Unified Data Lakehouse · GRC=Governance/Risk/Compliance

---

1) High-Level Topology (compact ASCII for Word portrait)



2) Design Principles

1) **Sovereign AO Control:** AO owns meta-planner, unified MCP gateway, authoritative RAG, and UDL. Partners cannot see each other.
2) **Per-Type Autonomy:** Each partner **type** (Servicers, Managers, Providers) operates its own AG + MCP + RAG; scope limited to its artifacts/APIs.
3) **Contracted DX:** Typed feeds/events cross boundaries via schema contracts, CDC/eventing, and policy enforcement (minimize data, mask PII).
4) **Trust Boundaries:** All calls traverse AO DMZ with allow-lists, rate limits, content filters, and entitlements-aware retrieval.
5) **Cite-or-Fail & Audit:** Every output is evidence-backed with citations and full prompt/action lineage.

---

3) What Lives Where

Asset Owner (AO)

- **AO Agent Hub:** Orchestrates multi-party workflows (recon, valuation, compliance).
- **AO MCP Registry:** AO-approved tools + partner gateway adapters.
- **AO RAG:** Consolidated, deduped, point-in-time corpus (positions, cash, breaks, capital calls, policies, contracts, minutes).
- **AO UDL:** Versioned facts + semantic layer; **GRC** for IPS/limits, liquidity ladders; **Audit** for prompts/tools/actions.

Asset Servicers (1 … N)

- **AG:** Exceptions detection, reconciliation, SLA status, remediation playbooks.
- **MCP:** Custody APIs, exceptions DB, corp actions, pricing files.
- **RAG:** Procedures, file specs, KBs, ticket history.
- **DX→ AO:** Positions, transactions, prices, breaks, timeliness events.

Asset Managers (1 … N)

- **AG:** Mandate compliance, exposure deltas, performance commentary.
- **MCP:** OMS/EMS, holdings/exposure APIs, fee schedules.
- **RAG:** PM letters, guidelines, model books, factor notes.
- **DX→ AO:** Holdings, trades, exposure, commentary, accruals.

External Data Providers (1 … N)

- **AG:** Index changes, ratings actions, macro series, social-impact metrics.
- **MCP:** REST/FTP/S3 access, entitlements checks, throttling.
- **RAG:** Methodologies, licenses, coverage notes, point-in-time guides.
- **DX→ AO:** Benchmarks, classifications, curves, events (rebalances/downgrades).

4) Orchestration Pattern (Example: T+1 NAV Variance > 50 bps)

1) **Plan:** AO meta-planner creates sub-goals: Servicers (breaks/SLAs), Managers (exposure/factors), Providers (index events).
2) **Delegate:** AO calls each partner AG via MCP gateway; each performs local RAG retrieval.
3) **Gather:** Partners return cited artifacts (exceptions file, trade/exposure notes, index bulletin).
4) **Reason & Propose:** AO aligns timelines in UDL, explains root cause, proposes actions with confidence scores.
5) **Approve & Act:** Dual-control actions; tasks opened; DX requests issued; everything logged.

5) Security, Governance & KPIs

- **Zero-Trust:** Token-scoped, least-privilege, time-boxed access across [TB]s.
- **Data Minimization:** Only necessary fields/rows cross boundaries; masking/redaction at ingest/serve.
- **Model Governance:** Versioned prompts, eval suites, drift monitors, cost/latency SLOs.
- **KPIs:** Evidence coverage ≥95%; query-to-cited-answer P95 <120s; −60% exception cycle time by Day 90.

Summary: Each partner type runs its own autonomous Agentic stack (AG+MCP+RAG). The AO retains sovereign intelligence, merges evidence, and executes auditable, decision-grade workflows in OLTAIX.