# Unified Governance Layer - Acquisition Diligence Packet

Purpose: Provide a concise technical and compliance snapshot for buyer diligence. Not a certification.

## 1) Product Summary

Drop-in policy-as-code and evidence engine for third-party and AI data access governance. Core value: enforce access policies, record decisions, and export tamper-evident evidence packs.

## 2) Current Capabilities

- Multi-tenant org isolation with API key scopes
- Policy engine with allow/deny decisions
- Evidence export (JSON/CSV) with HMAC signatures
- Hash chain for evaluation logs
- Retention enforcement endpoint
- Connector SDK with sample connectors (Snowflake, Google Drive)
- OPA policy export for external policy engines
- SSO and SCIM configuration stubs

## 3) Architecture Overview

FastAPI microservice with SQLite or Postgres persistence. Core tables: orgs, users, memberships, api keys, policies, resources, evaluations, sso configs. Evidence logs include hash chain fields for integrity. Postgres supported via DB_URL; SQLite via DB_PATH.

## 4) Security Model

API keys with scoped permissions; rotation and revocation endpoints. Evidence export signed with HMAC. Retention enforcement deletes records older than configured window.

## 5) Compliance Alignment (Summary)

SOC 2 Security: partial coverage for access control, logging, integrity, retention.
ISO 27001 Annex A: partial coverage for asset management, logging, cryptography.
NIST AI RMF: Govern and Measure supported; Map and Manage partial.

## 6) Core API Endpoints

- POST /orgs, /users, /orgs/{org_id}/memberships
- POST /orgs/{org_id}/keys, /rotate, /revoke
- POST /policies, GET /policies/{id}/opa
- POST /resources, POST /evaluations
- POST /evidence/retain, GET /evidence/export
- GET /connectors, GET /connectors/{name}/sample
- SCIM: POST/GET/DELETE /scim/Users

## 7) Diligence Checklist

Code review: API auth, scopes, evidence integrity, retention.
Security review: key rotation and revocation flows.
Data model: resources include source_system and external_id.
Deployment: Docker + Postgres support.
Evidence: export signatures and hash chain presence.

## 8) Known Gaps (Next Phase)

- SSO enforcement (current: configuration stub only)
- Formal incident response playbook
- Change management policy and audit trails
- Continuous monitoring and alerting stack

## 9) Repository

https://github.com/brokenbartender/unified-governance

Prepared: Unified Governance Layer