EXHIBIT: OpenCompliance-AI (Governance as Code)

Project Scope: Open-Source, Local-First GRC Assessment Engine

Tech Stack: Python (FastAPI), SQLModel, Tailwind CSS, Ollama (Mistral-Nemo)

Core Objective: To replace expensive, cloud-dependent GRC tools with a private, AI-assisted compliance auditor.

---

1. THE PROBLEM: The "Compliance Tax"

Standard GRC platforms are often "security-through-cloud," requiring organizations to upload their most sensitive security gaps to a third-party vendor. For small-to-medium teams, the cost of these tools and the risk of data leakage often lead to "Compliance by Spreadsheet," which is difficult to audit and version control.

2. THE SOLUTION: Local-First AI Auditing

I developed **OpenCompliance-AI**, a lightweight engine designed specifically for **NIST 800-53 Rev. 5** assessments.

Key Architectural Pillars:

- **AI-Assisted Expert Review:** Integrated **Ollama (Mistral-Nemo)** to act as a virtual auditor. The AI evaluates implementation statements against NIST requirements and provides a 2-sentence sufficiency opinion—all running locally to ensure 100% data sovereignty.
- **Maturity-Based Scoring:** Implemented a 5-tier maturity model (Initial to Optimized) that automatically generates "PASS/FAIL/PARTIAL" status badges.
- **Dynamic NIST Catalog Integration:** Developed a custom ingestion engine that seeds a local SQLite database directly from the official NIST CSV catalog, providing instant tooltips and supplemental guidance for auditors.

3. TECH STACK & INTEGRATION

- **Backend Autonomy:** Built with **FastAPI** and **SQLModel**, allowing for sub-millisecond database queries and a clean, interactive API documentation (Swagger/OpenAPI).
- **Frontend Simplicity:** Utilized **Tailwind CSS** and Vanilla JS to maintain a high-performance, framework-agnostic dashboard that can be served from any internal web server.
- **Remediation Mapping:** Built-in tracking for failed controls, allowing teams to document and export **Plan of Action and Milestones (POA&M)** reports directly to PDF.

---

4. IMPACT ON THE "AUTONOMOUS DATACENTER"

OpenCompliance-AI serves as the **Governance Layer** of my 6-Layer Datacenter model.

- While **Ansible** manages the *state* of the servers...
- And **OpenVAS** scans for *vulnerabilities*...
- **OpenCompliance-AI** tracks the *policy maturity*, providing the "Paper Trail" required for HIPAA, SOC2, and NIST audits.

---

5. TECHNICAL DOCUMENTATION INDEX

- **GitHub Repository:** github.com/davidculp-tech/OpenCompliance-AI
- **Demo/SOP:** Included in the *Autonomous Datacenter Deployment Guide*.