Project Title

Agentic Compliance & Risk Intelligence Platform Using RAG and LLMs

Problem Statement

Organizations operating in regulated industries such as banking, insurance, fintech, healthcare, and manufacturing must continuously comply with evolving regulatory frameworks, internal policies, and risk management guidelines. These regulations are documented across large volumes of unstructured data including regulatory circulars, compliance manuals, audit reports, risk assessment documents, internal controls, and standard operating procedures.

Compliance and risk teams face significant challenges in:

- Quickly interpreting regulatory requirements
- Assessing policy adherence across business units
- Responding to audit and regulator queries with traceable evidence
- Identifying potential compliance gaps and emerging risks

Traditional rule-based systems and keyword search tools are inadequate because they lack contextual understanding, cannot reason across multiple documents, and are unable to provide concise, explainable, and audit-ready responses. Manual review processes are time-consuming, error-prone, and do not scale with increasing regulatory complexity.

The organization requires an **intelligent, explainable, and auditable AI-driven system** that can understand natural language queries, retrieve relevant regulatory and policy content, reason across risk and compliance domains, and generate accurate, context-aware responses grounded in authoritative sources.

Proposed Solution Overview

Design and develop an **Agentic Compliance & Risk Intelligence Platform** using **Large Language Models (LLMs)** integrated with **LangChain, LangGraph, Retrieval-Augmented Generation (RAG), FAISS**, and advanced **prompt engineering** techniques.

The system will ingest internal compliance documents and external regulatory guidelines, transform them into semantic embeddings, and store them in a FAISS vector database for high-performance similarity search. A RAG pipeline will ensure that all AI-generated responses are grounded in verified compliance sources, reducing hallucinations and ensuring regulatory accuracy.

Multiple specialized AI agents will be orchestrated using **LangGraph**, each responsible for distinct compliance and risk functions such as regulatory interpretation, policy mapping, risk assessment, audit support, and escalation analysis. Queries will be dynamically routed to the appropriate agent based on intent and risk classification.

Prompt engineering will be used to enforce regulatory tone, structured outputs, explainability, and source attribution, ensuring that generated responses meet audit, governance, and risk management standards.

Key Functional Capabilities

- Conversational querying of regulatory and compliance documents
- Context-grounded answers with source traceability (RAG)
- Multi-agent reasoning for compliance, audit, and risk analysis
- Semantic search using FAISS vector storage
- Explainable responses suitable for audits and regulators
- Scalable, modular workflows using LangGraph

Technology Alignment

- **LLM:** Gemini / GPT / LLaMA (pluggable)
- **LangChain:** Prompt templates, chains, tool integration

- **LangGraph:** Agent orchestration and decision routing
- **RAG:** Verified context injection from compliance corpus
- **FAISS:** Vector database for semantic retrieval
- **Prompt Engineering:** Role-based, few-shot, structured, and safety prompts

Expected Outcome

The platform will significantly improve compliance response time, reduce operational risk, enhance audit readiness, and provide explainable, traceable AI-assisted decision support. It will demonstrate how **agentic GenAI architectures** can be responsibly applied to high-risk, regulated environments while maintaining governance, transparency, and accuracy.