# Product Requirements and Specification Document (PRD)

## Project Name

**FinScenarioMap - AI-Powered Banking Scenario Mapping Tool**

## 1. Overview

| Item | Description |
|------|-------------|
| Purpose | Enable users to input/upload hypothetical banking scenarios and receive AI-driven mappings to similar historical cases with recommended actions. |
| Target Users | Banking analysts, compliance officers, fraud detection teams, and financial institutions. |
| Key Value | Accelerates scenario analysis, improves decision-making, and enhances security/compliance. |

## 2. Objectives

- Map user-provided banking scenarios to similar historical cases.
- Generate actionable recommendations using AI.
- Ensure modular, secure, and scalable workflow design.
- Support both manual input and file uploads.

## 3. Core Features

| Feature | Description |
|---------|-------------|
| Scenario Input | Users can input scenarios via form or upload (CSV, JSON). |
| Scenario Mapping | AI maps input to similar historical banking cases using agentic-ai and langgraph. |
| Recommendation Generation | Generative AI (OpenAI) provides recommended actions for each mapped scenario. |
| Workflow Visualization | Visual representation of mapping and recommendation workflow. |
| Security & Compliance | Data encryption, access control, and audit logging. |
| Modular Architecture | Components are decoupled for easy extension and maintenance. |

## 4. User Stories

| ID | As a… | I want to… | So that… |
|----|-------|-----------|----------|

| US1 | Analyst | Input/upload a scenario | I can analyze potential risks or issues |
|-----|---------|-------------------------|----------------------------------------|
| US2 | Compliance Lead | See similar historical cases | I can benchmark and justify decisions |
| US3 | Fraud Team | Get AI-driven recommended actions | I can respond quickly and effectively |
| US4 | Admin | Manage user access and view audit logs | I ensure security and compliance |

## 5. Functional Requirements

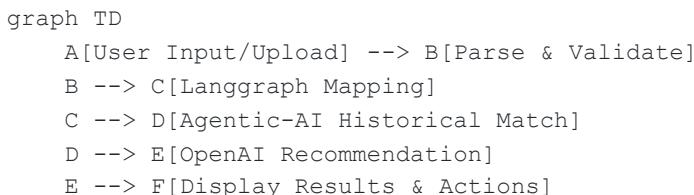| ID | Requirement | Priority |
|----|-------------|----------|
| FR1 | Accept scenario input via form and file upload (CSV, JSON) | High |
| FR2 | Parse and validate scenario data | High |
| FR3 | Use langgraph to structure mapping workflow | High |
| FR4 | Use agentic-ai to match scenarios to historical cases | High |
| FR5 | Use generative-ai (OpenAI) to generate recommended actions | High |
| FR6 | Display mapping results and recommendations in UI | High |
| FR7 | Visualize workflow steps and results | Medium |
| FR8 | Implement user authentication and role-based access | High |
| FR9 | Encrypt sensitive data at rest and in transit | High |
| FR10 | Log all scenario submissions and actions for audit | Medium |
| FR11 | Modularize components for future extensibility | Medium |

## 6. Non-Functional Requirements

| ID | Requirement | Priority |
|----|-------------|----------|
| NFR1 | System uptime ≥ 99% | High |
| NFR2 | Response time < 3 seconds per scenario | High |
| NFR3 | GDPR and banking compliance | High |
| NFR4 | Scalable to 100 concurrent users | Medium |
| NFR5 | Secure API endpoints | High |

## 7. Technical Specifications

| Area | Specification |
|------|---------------|
| Language | Python 3.10+ |
| Frameworks | FastAPI (backend), React (frontend, optional), Langgraph, agentic-ai, OpenAI |
| Data Storage | PostgreSQL (scenarios, users, logs), S3-compatible for file uploads |

| | |
|---|---|
| Security | JWT authentication, HTTPS, AES-256 encryption |
| Deployment | Docker containers, Kubernetes (optional), CI/CD pipeline |
| Integrations | OpenAI API, internal historical case database |

## 8. Workflow Overview

```
graph TD
    A[User Input/Upload] --> B[Parse & Validate]
    B --> C[Langgraph Mapping]
    C --> D[Agentic-AI Historical Match]
    D --> E[OpenAI Recommendation]
    E --> F[Display Results & Actions]
```

## 9. Example API Endpoints

```
POST /api/scenarios/upload      # Upload scenario file
POST /api/scenarios/input       # Manual scenario input
GET  /api/scenarios/{id}/map    # Get mapping and recommendations
GET  /api/audit/logs            # Retrieve audit logs (admin)
```

## 10. Acceptance Criteria

- Users can input or upload scenarios and receive mapped cases with recommendations.
- System returns results within 3 seconds for standard scenarios.
- All sensitive data is encrypted and access-controlled.
- Audit logs are available for all scenario submissions and actions.
- Modular components can be extended or replaced independently.

## 11. Risks & Mitigations

| Risk | Mitigation |
|---|---|
| Data privacy breach | End-to-end encryption, strict access controls |
| AI recommendation inaccuracy | Human-in-the-loop review, continuous model tuning |
| API rate limits (OpenAI) | Caching, fallback messaging |

## 12. Milestones

| Milestone | Target Date |
|---|---|

| | |
|---|---|
| Requirements Finalized | Week 1 |
| MVP Backend Complete | Week 3 |
| AI Integration Complete | Week 5 |
| UI & Workflow Visualization | Week 6 |
| Security & Compliance | Week 7 |
| User Testing & Feedback | Week 8 |
| Launch | Week 9 |

**End of Document**