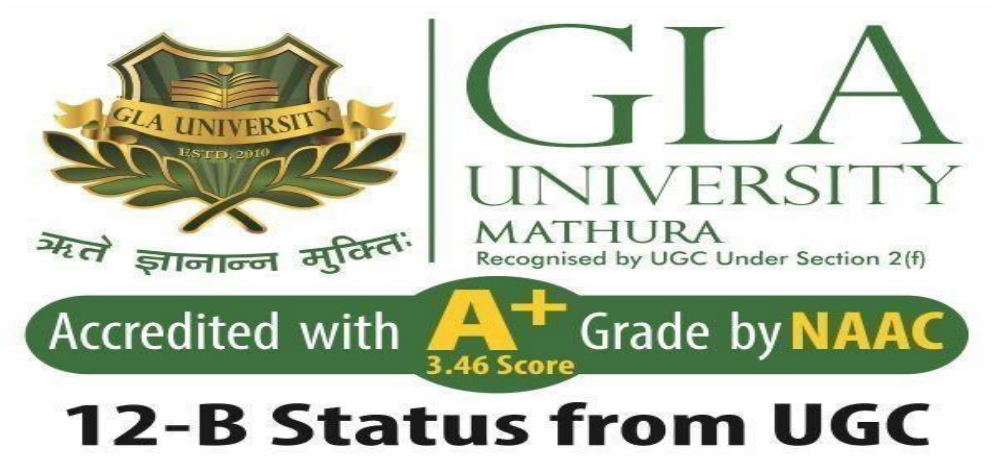
B.Tech CSE Hons. (III YEAR – VI SEM) (2025-26)

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

& APPLICATIONS



GLA UNIVERSITY

17km Stone, NH-2, Mathura-Delhi Road, P.O. Chaumuhan,
Mathura – 281406 (Uttar Pradesh) India

Project Title: Context-Aware Financial Concept Explanation System (Non-Advisory)

Team Leader	Ansham Maurya	2315800011
Team Member 1	Jayendra Singh	2315800040
Team Member 2	Yashraj Mishra	2315800095

Project Mentor: Mr. Shivanshu Upadhyay Signature:_____

1. Overview

1.1 Problem Statement

Current FinTech conversational systems struggle to balance **user personalization with regulatory compliance**, often leading to **implicit financial advisory, hallucinations, or misleading explanations**. Most existing tools either provide **generic definitions** or **direct recommendations**, which can confuse users and may violate regulatory boundaries.

Furthermore, there is no **scalable, region-aware, non-advisory AI system** that can explain financial concepts in a **personalized, risk-aware, legally compliant, and transparent** manner while maintaining explainability.

1.2 Objective (Goal)

The objective of this project is to design and develop a **Context-Aware, Non-Advisory AI Framework** that:

- Identifies user intent through **intent classification**
- Grounds responses in **India-specific regulatory knowledge bases (RBI-aligned)**
- Enforces a **compliance and policy control layer** to prevent financial advice
- Uses **LLM-based generation** to produce clear, personalized explanations
- Ensures all outputs are **risk-aware, transparent, and explainable**

The system focuses on **financial understanding and literacy**, not decision-making or recommendation.

1.3 Key Contributions (What this work achieves)

This system will:

- Provide **personalized explanations** based on user financial context
- Remain strictly **non-advisory by design**
- Align explanations with **Indian financial regulations (RBI framework)**
- Reduce hallucinations through **RAG-based grounding**
- Disclose **risks, assumptions, and uncertainties** in every response

2. Scope and Control

2.1 In-Scope

The scope of this project includes the design and implementation of a **Context-Aware, Non-Advisory Financial Explanation System** with the following capabilities:

- Collection and interpretation of **user financial context** (income, savings, liabilities, and goals).
- **Intent classification** to distinguish between educational and advisory requests.
- A **Region-Aware Compliance Engine** aligned with Indian financial regulations and RBI guidelines.
- An **LLM-based Risk-Aware Explanation Generator** that produces personalized explanations.
- **Retrieval-Augmented Generation (RAG)** using curated Indian financial and legal documents.
- A **Non-Advisory Policy Enforcement Layer** to prevent prescriptive financial advice.
- An **Explainable AI layer** that provides source-grounded reasoning and transparency.

2.2 Out-of-Scope

The following are explicitly excluded from the scope of Version 1 of this project:

- Live financial transactions or payment processing.
- Automated budgeting or financial planning tools.
- Portfolio tracking or investment performance analysis.
- Credit scoring or loan eligibility assessment.
- Stock, cryptocurrency, or market trend analysis.
- Mobile application development.

2.3 Assumptions

The project is developed based on the following assumptions:

- Users provide **accurate and truthful financial information.**
- Relevant **RBI circulars and government financial documents** are available for retrieval and grounding.
- The LLM operates under predefined **safety and compliance guardrails**.

2.4 Constraints

The system development is subject to the following constraints:

- Limited academic project timeline.
- No access to proprietary or paid financial datasets.
- Possible **API rate limits** when using external LLM services.
- Limited computational and hardware resources.

2.5 Dependencies

Successful implementation of the system depends on:

- An **LLM provider** (OpenAI or an open-source alternative).
- A curated **Indian financial and legal document repository** for RAG.
- A **FastAPI backend framework** for API development.
- A suitable **frontend UI framework** for user interaction.

2.6 Acceptance Criteria and Sign-Off

The system will be considered acceptable and ready for final evaluation if it satisfies the following acceptance criteria:

AC-1: Correct Response Generation

GIVEN a user provides valid financial context and asks an educational question,
WHEN the system processes the request,
THEN it must generate a **personalized, non-advisory, risk-aware explanation within 5 seconds**.

AC-2: Non-Advisory Enforcement

GIVEN a user submits an advisory-seeking prompt (e.g., "What should I invest in?"),

WHEN the system detects advisory intent,
THEN it must **refuse to provide advice and reframe the response as educational content**.

AC-3: Compliance Alignment

GIVEN a financial explanation is generated,
WHEN the output is reviewed,
THEN it must be **aligned with India-specific (RBI) regulatory principles** and include clear risk disclosures.

AC-4: Explainability Requirement

GIVEN a response is produced,
WHEN presented to the user,
THEN it must include **clear reasoning, assumptions, and source-grounded references**.

Sign-Off Requirement

The project will be considered complete only after:

- Successful system demonstration
- Submission of final report and documentation
- Approval from the project mentor and evaluation panel

2.7 Deliverables

The following deliverables will be produced at the end of the project:

Technical Deliverables

- Functional **FastAPI backend** with:
  - Intent classifier
  - RAG engine
  - Compliance filter
  - LLM-based explanation generator
- **Web-based conversational UI** for user interaction
- Curated **Indian financial and RBI-aligned knowledge repository** for RAG
- Secure configuration files with environment-based API key management

Documentation Deliverables

- Software Requirements Specification (SRS)
- System Architecture Diagram
- Data Flow Diagram (DFD)
- Use Case Diagram
- Final Project Report
- User Manual / Demo Guide
- PowerPoint presentation for viva

Evaluation Deliverables

- Test report with sample inputs and outputs
- Compliance test cases (advisory vs educational prompts)
- Performance metrics (latency, accuracy, explainability check)

3. Stakeholders and RACI

Activity	Responsible	Accountable	Consulted	Informed
Requirements	Ansham	Ansham	Mentor	Team
Design	Jayendra/Yashraj	Ansham	Mentor	Team
Implementation	Ansham	Ansham	Mentor	Team
Testing	Jayendra	Ansham	Mentor	Team
Release	Yashraj	Ansham	Mentor	Dept

4. Team and Roles

Member	Role	Responsibilities	Key Skills	Availability
Ansham Maurya	Product Lead & Backend	Architecture, APIs, Pipelines	Python, AI/ML	7 hrs/week
Jayendra Singh	Backend Integration	Moduler Integration and Data Formatting	Python, FastAPI	7 hrs/week
Yashraj Mishra	AI & RAG Engineer	RAG, Guardrails	NLP, Python	7 hrs/week

5. Week-Wise Plan and Assignments

Week	Timeline (Approx.)	Milestones	Responsibilities	Key Deliverables	Status
Week 1	Days 1–7	Requirements Freeze	Ansham: Finalize scope Jayendra: UI-wireframes Yashraj: Collect RBI/financial docs	Draft SRS	Planned
Week 2	Days 8–14	System Architecture	Ansham: System design Jayendra: UI kit Yashraj: RAG setup	ERD + API Specification	Planned
Week 3	Days 15–21	Backend Development	Ansham: FastAPI core APIs Jayendra: UI skeleton Yashraj: RAG prototype	Backend v1	Planned
Week 4	Days 22–28	Frontend Development	Ansham: API integration Jayendra: Dashboard UI Yashraj: Initial model tuning	UI v1	Planned
Week 5	Days 29–35	Core Feature Implementation	Ansham: Non-advisory layer Jayendra: Chat UI Yashraj: LLM pipeline	Demo v1	Planned
Week 6	Days 36–42	Testing & Refinement	Ansham: Bug fixes Jayendra: UX polish Yashraj: RAG improvement	Test Report	Planned
Week 7	Days 43–49	System Hardening	Ansham: Compliance checks Jayendra: UI refinements Yashraj: Guardrails	Final Build	Planned
Week 8	Days 50–56	Final Release	Ansham: Final sign-off Jayendra: Presentation Yashraj: Documentation	v1.0 + Slides	Planned

6. Users and UX

6.1 Personas

The system is designed for the following primary user personas:

- **Financial Beginner**
  A user with limited financial literacy who requires **simple, clear, and jargon-free explanations** of basic financial concepts.
- **Young Professional**
  A salaried individual seeking **context-aware understanding** of topics such as loans, savings, taxes, and investments without receiving financial advice.
- **Small Business Owner**
  A user who needs **clarity on legal and regulatory aspects** of financial decisions while avoiding prescriptive recommendations.

6.2 Top User Journey

The primary user interaction with the system follows the sequence below:

- User enters their **financial context** (income, savings, loans, goals).
- User asks a financial question in natural language.
- The system performs **intent classification** to detect whether the request is educational or advisory.
- Relevant information is retrieved from **RBI-aligned knowledge sources** using RAG.
- The system generates a **personalized, risk-aware explanation**.
- The output is presented along with **explainability sources, risks, and assumptions**.

6.3 Accessibility and Localization

To ensure usability and inclusivity, the system adheres to the following principles:

- Uses **simple and clear English explanations** to support users with varying literacy levels.
- Provides a **responsive, mobile-friendly user interface** for accessibility across devices.
- Clearly states **risks, assumptions, and uncertainties** in every response.
- Avoids technical jargon unless it is clearly defined in plain language.

7. Market and Competitors

7.1 Competitor Analysis

Competitor	Product	Strengths	Weaknesses	Our Differentiator
ChatGPT	General AI assistant	Powerful language understanding and generation	May provide implicit financial advice	Strict **non-advisory guardrails** with compliance control
Groww	Retail finance platform	Well-structured educational content	Explanations are largely generic and not personalized	**Context-aware explanations** based on user inputs
Zerodha Varsity	Financial literacy platform	High-quality structured learning material	Static, non-conversational content	**Interactive conversational AI** for personalized understanding

7.2 Positioning

The proposed system is positioned as a **financial literacy AI assistant rather than a financial advisor**, addressing a critical gap in compliant, personalized, and explainable FinTech education in India.

8. Objectives and Success Metrics

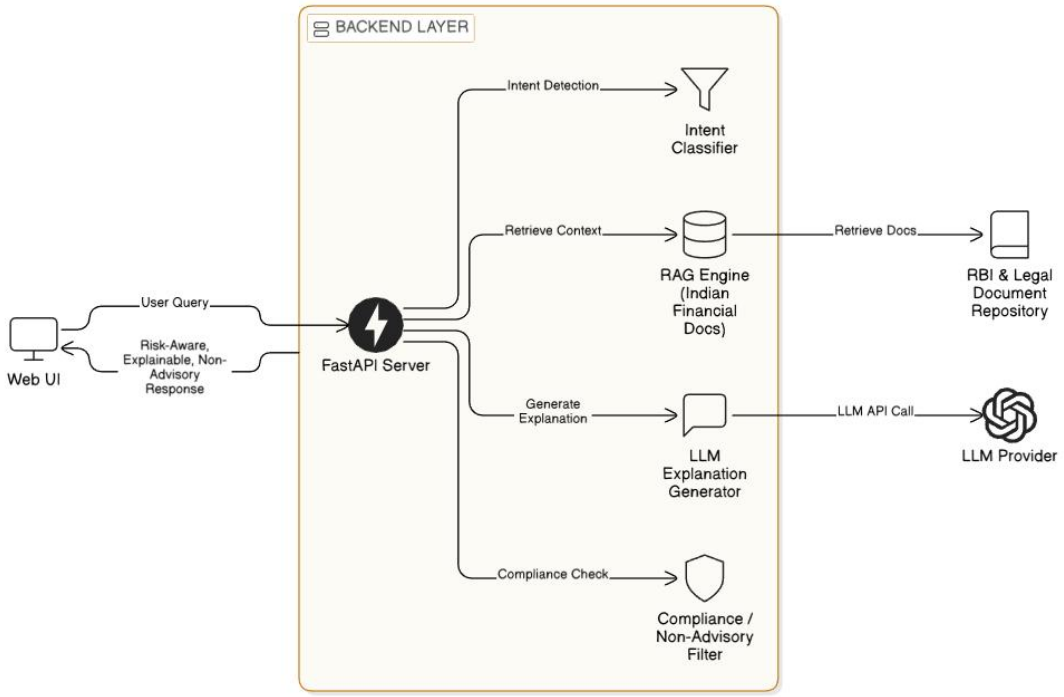
The following objectives and measurable success metrics define the effectiveness of the system:

Objective	Key Performance Indicator (KPI)	Target
Personalization	Accuracy of extracted financial context	**≥ 85%**
Compliance	Prevention of advisory outputs	**100% (zero leakage)**
System Performance	Average response time	**≤ 5 seconds**
Explainability	Availability of source citations in responses	**100%**

9. Key Features

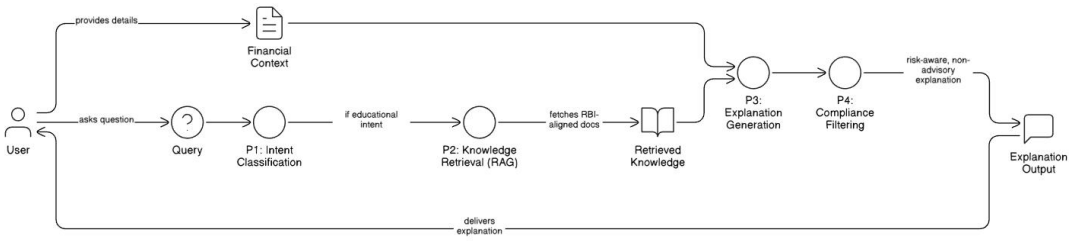
Feature	Description	Priority	Acceptance Criteria
Non-Advisory Filter	Detects and blocks advisory content	Must	System produces **no prescriptive outputs**
Region-Aware Compliance Engine	Aligns responses with India/RBI regulations	Must	Explanations reference **RBI documents** where relevant
Risk-Aware Explanation Generator	Highlights uncertainties and limitations	Must	Every response **lists assumptions and risks**
Explainable AI (XAI) Layer	Provides transparent reasoning	Must	Responses include **clear source citations**
LLM Integration	Generates natural, conversational explanations	Must	All outputs comply with **safety and policy guardrails**

10. Architecture

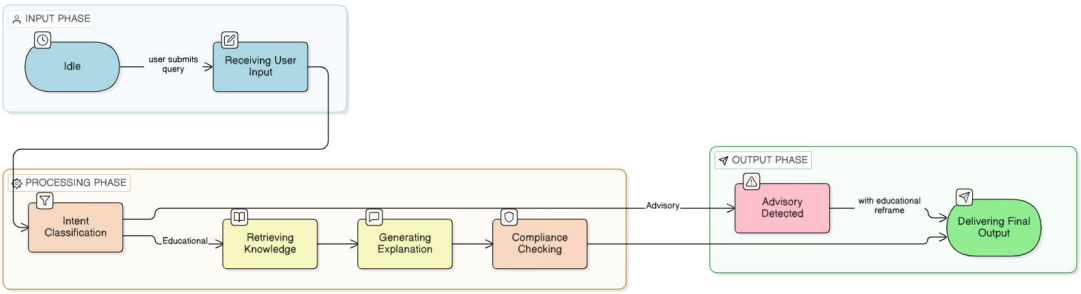


11. Diagrams

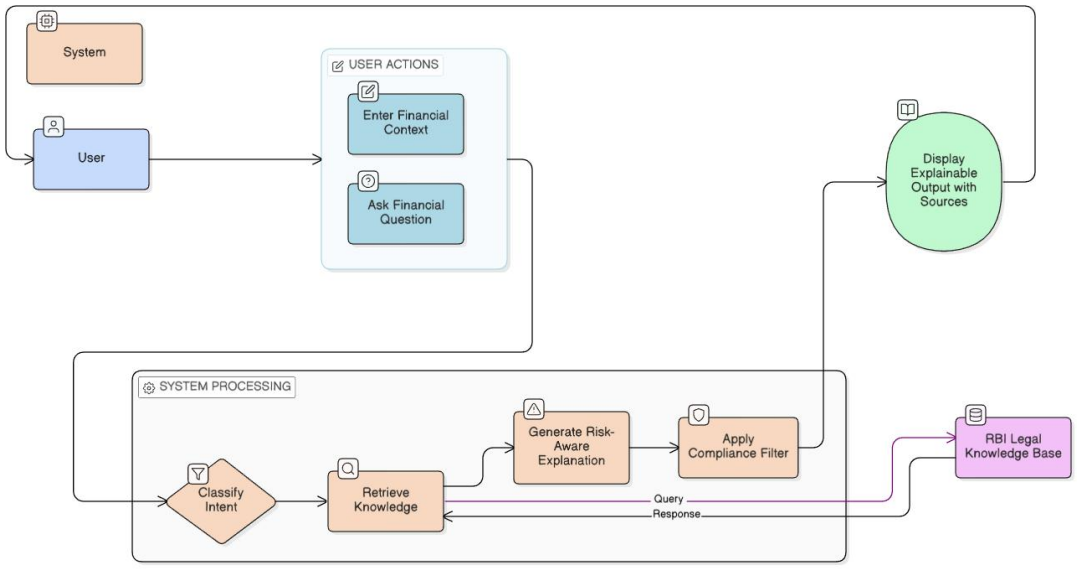
11.1 DataFlow Diagram



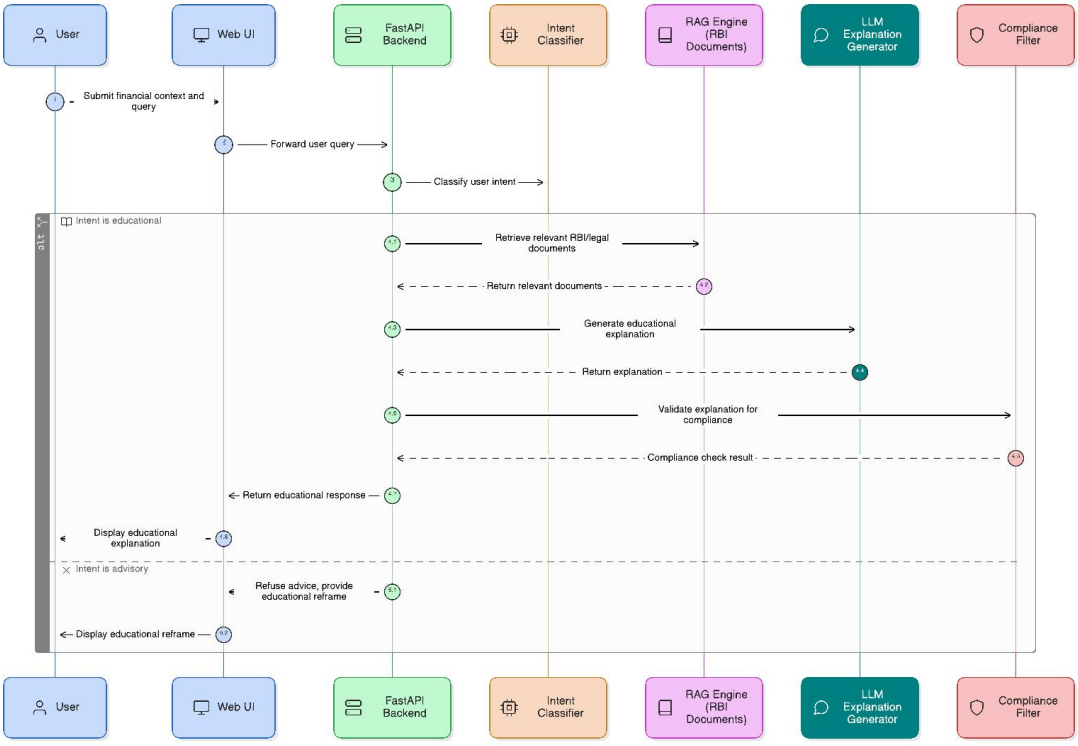
11.2 State Transition Diagram



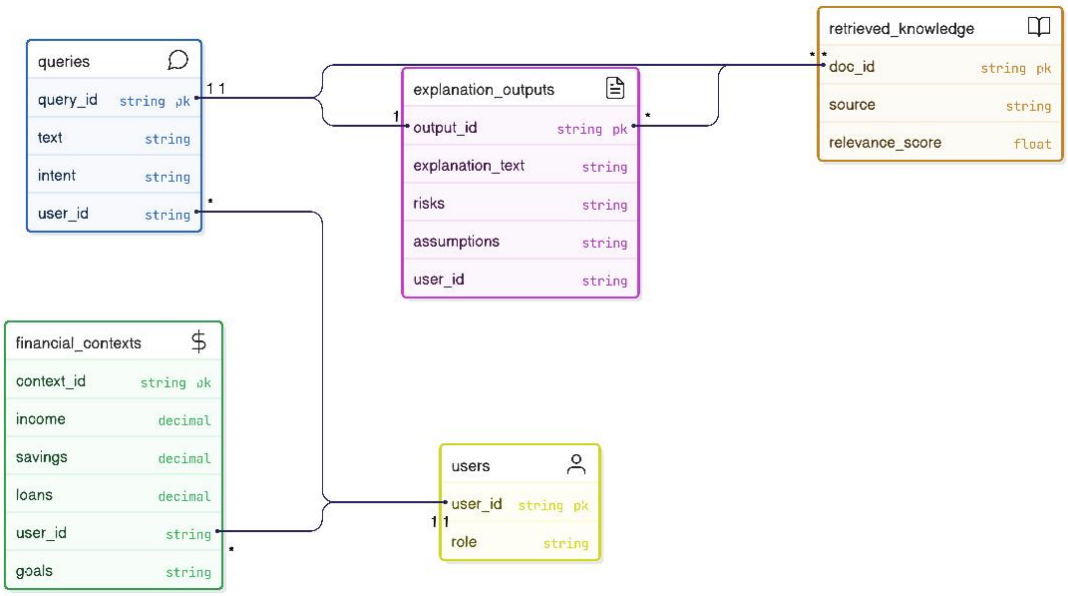
11.2 Use Case Diagram



11.3 Sequence Diagram



11.5 ER (Entity Relationship) Diagram



12. Quality: Non-Functional Requirements (NFRs)

The system is designed to meet the following non-functional requirements to ensure reliability, usability, and security:

Metric	Target	Description / Justification
Availability	**≥ 99%**	The system should remain operational and accessible during normal academic evaluation and testing periods.
Latency	**≤ 5 seconds**	The system should generate responses within 5 seconds to ensure a smooth user experience and real-time interaction.
Error Rate	**≤ 1%**	The system should minimize failures, crashes, or incorrect API responses to maintain user trust.
Security	**No critical vulnerabilities**	The system must be free from major security risks such as unauthorized access, API key leakage, or data misuse.

Additional Non-Functional Considerations:

- **Scalability:** The architecture should support multiple users with minimal performance degradation.
- **Maintainability:** Code should be modular, well-documented, and easy to extend.
- **Explainability:** Every system output should be traceable to its source and reasoning.
- **Compliance:** All outputs must adhere to non-advisory and regulatory guidelines.

13. Security & Compliance

13.1 Threat Model (STRIDE-based Analysis)

Asset	Threat	Impact	Likelihood	Mitigation Strategy
API Keys	Leakage or exposure	Unauthorized access to LLM services	Medium	Store in environment variables; never hardcode in source code
User Data	Misuse or retention	Privacy violation	Low	No long-term storage policy; anonymized processing
LLM Output	Hallucination / incorrect info	Misinformation	Medium	RAG-based grounding using trusted sources
System Integrity	Tampering or unauthorized changes	Data corruption	Low	Secure authentication and access control
Backend API	Unauthorized access	System compromise	Medium	Secure HTTPS endpoints and validation checks

13.2 Compliance Considerations

The system is designed to be compliant with:

- **RBI Financial Literacy Principles:**
  - Focus on education rather than financial advice
  - Transparent explanations of risks and uncertainties
  - No prescriptive investment or financial recommendations
- **Non-Advisory by Design:**
  - Strict intent classification to prevent advisory outputs
  - Compliance filter to block or reframe advisory queries
  - Clear disclaimers when necessary

14. Delivery & Operations

14.1 Release Plan

- **Version v1.0** will be demonstrated during final project submission.
- The system will include a functional web interface, working backend, and policy-controlled LLM pipeline.
- A final project presentation, documentation, and demonstration will accompany the release.

14.2 CI/CD (Continuous Integration and Deployment)

A basic deployment pipeline will be followed:

- Code maintained in a version-controlled repository.
- Regular commits and incremental development.
- Local testing before final integration.
- Deployment on a local server or cloud (if available).

15. Risks & Mitigations

Risk	Probability	Impact	Mitigation Strategy	Owner
LLM Hallucination	Medium	High	Use RAG with trusted sources	Yashraj
Compliance Breach	Low	High	Strong policy filters and validation	Ansham
Timeline Delay	Medium	Medium	Weekly milestones and progress tracking	Team
API Downtime	Medium	Medium	Fallback responses and local knowledge cache	Team
Data Quality Issues	Low	Medium	Validation checks on user input	Jayendra

16. Research & Evaluation

16.1 Study of Existing Systems

A comparative study was conducted on existing platforms including:

- **ChatGPT:** Powerful language model but lacks strict non-advisory controls.
- **Groww:** Provides financial education but lacks personalized, conversational explanations.
- **Zerodha Varsity:** High-quality content but static and non-interactive.

This analysis revealed a clear gap in **compliant, personalized, and explainable financial education tools**, motivating the proposed system.

16.2 Evaluation Plan

The system will be evaluated based on:

- User Testing
  - A group of student users will interact with the system.
  - Feedback will be collected on:
    - Clarity of explanations
    - Trustworthiness of responses
    - Ease of use
    - Perceived compliance
- Performance Metrics
  - Response time (≤ 5 seconds)
  - Accuracy of intent classification
  - Quality of risk disclosures
  - Presence of explainability and source grounding
- Compliance Testing
  - The system will be tested with advisory-seeking prompts to ensure it refuses or reframes appropriately.

17. Appendices

17.1 Glossary

- **LLM (Large Language Model):** AI model capable of understanding and generating human-like text.
- **RAG (Retrieval-Augmented Generation):** Technique combining information retrieval with LLMs for grounded responses.
- **XAI (Explainable AI):** AI systems designed to provide transparent and interpretable outputs.
- **RBI (Reserve Bank of India):** Central banking authority of India.

17.2 References

- RBI Financial Literacy Portal – https://www.rbi.org.in/financialeducation/
- SEBI Financial Education Booklet – https://investor.sebi.gov.in/pdf/downloadable-documents/Financial%20Education%20Booklet%20-%20English.pdf
- FastAPI Official Documentation – https://fastapi.tiangolo.com/