Business Requirements Document (BRD)

Project Name

Agentic AI for Automated Requirement Gathering and Documentation in Financial Institutions

1. Background

The objective of this project is to automate the requirement gathering, documentation, and validation process using LLM-powered agents that ingest unstructured data (meetings, emails, PDFs), interpret context and extract relevant information, generate formal requirements/user stories/specifications, ensure regulatory compliance and traceability, and integrate outputs into enterprise tools (e.g., Jira).

2. As -is Process

To be defined

3. Business Requirements

3.1 Functional Requirements

3.1.1 Process Details

The project involves the development of an AI system that will automate the requirement gathering and documentation process. The system will ingest unstructured data, interpret context, extract relevant information, generate formal requirements/user stories/specifications, ensure regulatory compliance and traceability, and integrate outputs into enterprise tools.

3.1.2 Process Steps

1. Upload policy PDF
2. IngestorAgent extracts text
3. ContextAgent identifies context elements
4. RequirementAgent generates structured requirements
5. ComplianceAgent validates alignment with policies
6. TraceAgent logs all steps

7. Result pushed to Jira

3.2 System orchestration requirements

The system will use LangChain or CrewAI to manage agent workflows.

3.3 UI/UX Requirements (MVP -1)

The MVP Goals are as follows:

- Upload PDF/email transcript

- Auto-generate 3 user stories + acceptance criteria

- Push to Jira

- Store logs in a dashboard

3.4 Non -Functional Requirements

The system will implement the following key features to ensure robust functionality and security:

- PII redaction & anonymization pre-step

- Audit logs stored in append-only DB or JSON

- Role-based SME validation loop

- Secure deployment in on-prem or VPC environments

4. To Be Process

The anticipated procedural steps for MVP-1 are as follows:

- Upload PDF/email transcript

- Auto-generate 3 user stories + acceptance criteria

- Push to Jira

- Store logs in a dashboard

5. Assumptions

To be defined

6. Inclusions and Exclusions

Inclusions and exclusions are to be defined.

7. Data Sources

7.1 Input data sources

The input data sources include meeting transcripts, emails, PDFs, and web scraping for regulatory documents.

7.1.1 Key volumetrics of the as -is User Flow

To be defined

7.2 Output data sources

The output data sources include Jira and a dashboard for storing logs.

8. Glossary of Data

To be defined

Compliance Rules

|---|---|---|---|---|

| R1 | All unstructured data (meetings, emails, PDFs) must be ingested and interpreted by the AI system. | Data | High | ISO/IEC 27001 |

| R2 | The AI system must generate formal requirements/user stories/specifications. | Operational | High | ISO/IEC 27001 |

| R3 | The AI system must ensure regulatory compliance and traceability. | Legal | High | GDPR, ISO/IEC 27001 |

| R4 | The AI system's outputs must be integrated into enterprise tools like Jira. | Operational | High | ISO/IEC 27001 |

| R5 | The AI system must have a secure deployment in on-prem or VPC environments. | Security | High | ISO/IEC 27001, GDPR |

| R6 | The AI system must redact and anonymize PII data. | Security | High | GDPR |

| R7 | The AI system must store audit logs in an append-only DB or JSON. | Security | High | ISO/IEC

27001, GDPR |

| R8 | The AI system must have a role-based SME validation loop. | Operational | Medium | ISO/IEC 27001 |

| R9 | The AI system must reduce manual SME effort by at least 70%. | Operational | Medium | N/A |

| R10 | The AI system must be able to upload PDF/email transcript. | Data | High | ISO/IEC 27001 |

| R11 | The AI system must auto-generate at least 3 user stories + acceptance criteria. | Operational | High | ISO/IEC 27001 |

| R12 | The AI system must push generated user stories to Jira. | Operational | High | ISO/IEC 27001 |

| R13 | The AI system must store logs in a dashboard. | Data | High | ISO/IEC 27001 |

Compliance Rules

|---|---|---|---|---|

| Rule ID | Description | Category | Severity | Applicable Standards |

|---|---|---|---|---|

| R1 | All unstructured data (meetings, emails, PDFs) must be ingested and interpreted by the AI system. | Data | High | ISO/IEC 27001 |

| R2 | The AI system must generate formal requirements/user stories/specifications. | Operational | High | ISO/IEC 27001 |

| R3 | The AI system must ensure regulatory compliance and traceability. | Legal | High | GDPR, ISO/IEC 27001 |

| R4 | The AI system's outputs must be integrated into enterprise tools like Jira. | Operational | High | ISO/IEC 27001 |

| R5 | The AI system must have a secure deployment in on-prem or VPC environments. | Security | High | ISO/IEC 27001, GDPR |

| R6 | The AI system must redact and anonymize PII data. | Security | High | GDPR |

| R7 | The AI system must store audit logs in an append-only DB or JSON. | Security | High | ISO/IEC

27001, GDPR |

| R8 | The AI system must have a role-based SME validation loop. | Operational | Medium | ISO/IEC 27001 |

| R9 | The AI system must reduce manual SME effort by at least 70%. | Operational | Medium | N/A |

| R10 | The AI system must be able to upload PDF/email transcript. | Data | High | ISO/IEC 27001 |

| R11 | The AI system must auto-generate at least 3 user stories + acceptance criteria. | Operational | High | ISO/IEC 27001 |

| R12 | The AI system must push generated user stories to Jira. | Operational | High | ISO/IEC 27001 |

| R13 | The AI system must store logs in a dashboard. | Data | High | ISO/IEC 27001 |