Business Requirements Document (BRD)

Project Title

Agentic AI for Automated Requirement Gathering and Documentation in Financial Institutions

Objective

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
- Integrate outputs into enterprise tools (e.g., Jira)

High-Level Architecture

[Architecture diagram removed for plain text formatting]

Components & Tech Stack

1. **Input Layer**
   - Meeting transcripts (audio -> text via Whisper or AWS Transcribe)
   - Emails (.eml parsing via email module)
   - PDFs/DOCX (via PyPDF2, python-docx)
   - Web scraping for regulatory documents
2. **Agents**
   - IngestorAgent: Extracts text from source files
   - ParserAgent: Filters and segments relevant content
   - ContextAgent: Extracts stakeholders, goals, risks
   - RequirementAgent: Generates user stories, specs
   - ComplianceAgent: Validates against internal policy docs

   - ValidationAgent: Routes output to SMEs for feedback

   - TraceAgent: Logs all transformations for auditing

3. **Memory & Reasoning**

   - Short-term memory: In-session context

   - Long-term memory: Vector DB (Chroma, FAISS) for RAG

4. **Tools & APIs**

   - OpenAI GPT-4 / Anthropic Claude

   - Jira API (atlassian-python-api)

   - Email integrations (SMTP/SendGrid)

   - Vector store for document retrieval

5. **Orchestration Framework**

   - LangChain or CrewAI to manage agent workflows

Sample Flow: PDF to Jira

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

Security & Compliance

- 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

Benefits

- Accelerates requirements capture
- Ensures consistent formatting and compliance
- Maintains traceability and audit readiness
- Reduces manual SME effort by 70%+

MVP Goals

- Upload PDF/email transcript
- Auto-generate 3 user stories + acceptance criteria
- Push to Jira
- Store logs in a dashboard

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