Electronic Assignment Cover sheet

Student Declaration:

By submitting this assignment, I confirm that I am aware of DBS's policy regarding cheating, plagiarism and all other forms of academic impropriety. The coursework submitted is my own or my group's work, and all other sources consulted have been appropriately acknowledged. I am aware that in the case of doubt an investigation will be held.

Student Name:	**Aditya Khandelwal**	**Student No.:**	**20029947**
	Kartik Satish Koldilkar		**10601324**

Assignment Title: Decision Support System For Fraud Detection In Financial Institutions

Date of Submission: 16th December 2024

Word Count: 8100 Words

Signed: ________________________________

Contents

1. Introduction

Decision Support system for fraud detection in financial institutions is designed to enhance fraudulent activities with help of machine learning, artificial intelligence and rule-based decision making. It aims to reduce financial losses to individuals and financial institutions significantly by detecting suspicious transaction in real time while facilitating operational efficiency and compliance with financial regulatory standards. Automating fraud detection processes through scaling into high volumes of transactions, continuous adaptation to emerge patterns of fraud, and integrate with existing infrastructure. It will be and efficient and robust solution with security for financial institution.

2. Goals

2.1. Real-time Fraud Detection

Developing a system that detects fraudulent transactions as it occurs and minimizes the impact on financial institutions

1. **Strength:** Ability to identify suspicious activities in real time and take action on them immediately reducing financial losses and protects customer accounts.
2. **Weakness:** To maintain high performance, real-time systems require a significant infrastructural investments and computational resources
3. **Opportunities to improve:** In order to reduce both false positives and negatives, refine the detection algorithm. Which further increases accuracy and limiting unnecessary disruption to legitimate transactions.

2.2. Automated Fraud Detection

A significant amount of reduction in manual intervention will be done by implementing AI and machine learning which will automate the detection of fraud.

1. **Strength:** Human errors will be minimized, as it will provide operational efficiency by freeing the resources.
2. **Weakness:** Customer inconvenience can be caused due to automated system as it may produce false positives, which is that system can distrust by flagging the legitimate transactions.
3. **Opportunities to improve:** Updating the new fraud patterns for model training and using advance machine learning models with continuous feedback which will lead to fine-tune detection parameters, better performance and adaptation of automation towards future threats.

2.3. Scalability & Integration

To handle a large volume transaction, a scalable systems need to be created which can integrate seamlessly with existing IT infrastructure.

1. **Strength:** A scalable integrated platform ensures to grow with the needs of institution and can handle large volume data without affecting performance.
2. **Weakness:** Integration challenges can occur while connecting with legacy systems which will then lead to higher costs and extensions in project timelines.
3. **Opportunities to improve:** Simplifying integration process by building modular architecture which will allow incremental implementation in phased rollouts. Ensuring system performance for extreme load transactions and work on seamless APIs for better integration with diverse banking systems.

2.4. Compliance With Regulations

Systems adherence to financial regulations such as GDPR and PCI-DSS, protecting customers data and meeting legal obligations.

1. **Strength:** Working with compliance and regulatory bodies enables the corporation to earn trust of clients by staying away from legal implications due to data compromise and fraud incidents on its revenue.
2. **Weakness:** It can be complex and time consuming for ensuring compliance in different regions due to varying regulations in those regions.
3. **Opportunities to improve:** Based on geographic and regulatory changes a centralized compliance module can be implemented which further can ensure updating the systems effortlessly.

3. Objectives

- To design and develop an AI-powered expert systems which detects suspicious transactions and frauds in real time.
- For more effective model training and fraud detection accuracy, integration of data from various resources such as transactions logs, customer profiles and historical fraud data will be required.
- A rule-based component shall be deployed to detect fraudulent patterns based on predefined fraud characteristics and behaviour analytics.
- Evolution of system and improvement in practice shall be done through continuous learning and knowledge feedback loops.
- Integration tests and perform unit should be done in timely intervals to ensure that the system is accurate, reliable and can scale.
- Compliance with regulatory standards and easy integration with any financial institution’s IT infrastructure is must.

4. Project Cost and budget

Component	Subcomponent	Cost	Total
Salaries (Team)	Project Manager	€ 50,000	
	Data Scientist (2 members)	€ 100,000	
	Data Engineer	€ 50,000	
	Business Analyst	€ 40,000	
	Software Developer	€ 40,000	
	QA Engineer	€ 20,000	
			€ 300,000
Hardware & Software	High-Performance Laptops (5 units)	€ 15,000	
	Cloud Computing Services (e.g., AWS)	€ 20,000	
	Data Visualization Tools (Tableau/Power BI licenses	€ 10,000	
	Programming Tools (Python libraries, IDEs)	€ 5,000	
			€ 50,000
Data Acquisition	Historical Fraud Dataset (Purchase)	€ 15,000	
	Data Cleaning Services	€ 10,000	
			€ 25,000
Model Development & Testing	Feature Engineering and EDA	€ 20,000	
	Fraud Detection Model (Development)	€ 30,000	
	Model Validation and Optimization	€ 20,000	
			€ 70,000
Training & Documentation	User Manuals	€ 10,000	
	Training Sessions for End-Users	€ 10,000	
			€ 20,000
Deployment Costs	Integration with Banking Systems	€ 20,000	
	Real-Time Monitoring Setup	€ 10,000	
			€ 30,000
Total			**€ 495,000**
Contingency Reserve (10%)		€ 49,500	
Management Reserve (5%)		€ 26,475	
			€ 75,975
Grand Total Estimated Budget			**€ 571,975**

5. Project Justification

Fraud Detection in Financial Institutions - a Decision Support System

1. **Problem Statement:** Issues with financial institutions indicate that the question of fraud detection and prevention becomes increasingly difficult in the course of time due to increased and complex financial transactions. Fraudulent activities like identity theft, money laundering, credit card fraud, and inside trading may lead to huge losses in term of finance and also hampers overall reputation of the institution concerned. Current methods in fraud detection are usually reactive in nature, lacking the competence to find out sophisticated fraud patterns. A more robust data-driven proactive solution is hence justified.
2. **Vision Statement:** To design DSS using advanced data analytics, machine learning and real-time monitoring for fraud detection, prevention and effective response against fraudulent activities in financial institutions to enhance security, compliance and customer trust in them.
3. **Key Performance Indicators (KPIs):**
    - **Accuracy In Fraud Detection:** The percentage of properly identified fraudulent activities against the false alerts
    - **Reduction In Fraud Losses:** The decrease in the rate of financial losses caused by fraudulent activities after the implementation of the system.
    - **How Time is Respond To:** The time taken by a system to detect and respond to suspicious transactions or alerts.
    - **Compliance Rate:** The percentage of transactions flagged and reported in compliance with regulatory requirements.
    - **User Satisfaction Rate:** Analyst/Manager satisfaction when using the system, based upon feedback survey.
4. **Persona:**
    - **Job Title:** Senior Risk Analyst.
    - **Goals:** A system capable of quick identifying suspicious activities and alert her to them, so she can take quick actions to investigate them effectively. She also wants tools that can give her deep dives into history and pattern analysis or fraud investigations.
    - **Expectation:** Sarah would like user friendly interface which quickly helps her get work done, reduced false positive of data and provides actionable insights from data.

6. Deliverables

- Detailed project report, system architecture, data resources and methodologies for fraud detections.
- Expert systems prototype with basic fraud detection mechanism and initial rule-based implementation.
- Final AI-powered system integrated with advance machine learning models and rule-based detection mechanism with capability to do real-time fraud detections.
- Testing results and validation reports that guarantee the accuracy, performance and robustness of the systems under different conditions
- Training materials and manuals for financial institutions personnel to use, monitor and update the system.
- Compliance documentation such systems compliance with regulatory and legal requirements with respect to fraud detection in financial services.

7. Milestones

Milestone	Sprint	Description	Completion Time
Project Kick-off	Pre-Sprint	Initiation and team alignment; scope definition	Week 0
Basic Fraud Detection Ready	Sprint 1	Initial rule-based system for flagging potential fraud	Week 3
Enhanced Fraud Detection Complete	Sprint 2	Priority-based flagging and identification of high-value transactions	Week 6
Initial User Interface Developed	Sprint 3	Basic dashboard for viewing flagged transactions and reporting	Week 9
AI Model Integrated (Phase 1)	Sprint 4	Integration of initial AI model for anomaly detection	Week 12
Continuous Learning Mechanism	Sprint 5	AI adapts to new fraud patterns; initial feedback loop	Week 15
Advanced Fraud Detection (Phase 2)	Sprint 6	Risk scoring for flagged transactions and highlighting threats	Week 18
Real-Time Alerts Implemented	Sprint 7	Real-time fraud detection and immediate alerts	Week 21
Full System Deployment	Sprint 8	Complete AI-powered system with compliance and scalability features	Week 24
Project Closure and Evaluation	Post-Sprint	Final evaluation, documentation, and stakeholder approval	Week 26

7.1. Milestone Overview

1. **Project Kick-off (Week 0):** Project initiation, team alignment, and scope definition**.**
2. **Basic Fraud Detection Ready (Week 3):** Initial fraud detection system with manual audit capabilities.
3. **Enhanced Fraud Detection (Week 6):** Priority-based flagging and highlighting of high-value transactions.
4. **Initial User Interface (Week 9**): Basic dashboard for transaction viewing and reporting.
5. **AI Model Integration (Week 12):** AI model integrated for anomaly detection.
6. **Continuous Learning Mechanism (Week 15):** AI adapts to evolving fraud patterns.
7. **Advanced Fraud Detection (Week 18**): Risk scoring and threat prioritization.
8. **Real-Time Alerts (Week 21):** Real-time monitoring and alert system**.**
9. **Full System Deployment (Week 24**): Final AI system with full compliance and scalability.
10. **Project Closure (Week 26**): Final project evaluation, documentation, and approval.

8. Project Requirements

8.1. Business Requirements.

1. The system shall reduce the financial losses in real-time by detecting and preventing fraudulent activities
2. It should cater to automated fraud detection with minimum human interventions, hence giving complete operation efficiency.
3. The system shall be capable of handling voluminous transactions and shall identify anomalies without slowing down transaction processing
4. The solution should be scalable and implementable in various financial products such as credit cards, loans and payments.
5. The system should be fully complied with regulatory and legal requirements for fraud detection and data protection

8.2. Solution Requirements

8.2.1. Functional Requirements

i. The system shall detect fraudulent transactions in real time.

ii. The system shall use machine-learning models which are already trained with historical data to recognize patterns and anomalies.

iii. A rule-based engine, while utilizing already predefined rules and known fraud indicators, which shall be able to detect frauds

iv. Integration of systems with existing monitoring systems and databases of the financial institutions.

v. System embedding with continuous learning feedback mechanism and model updating concerning new fraud cases.

vi. A dashboard which produces reports on detection fraud cases, risk scores and system performance metrics.

8.2.2. Non-Functional Requirements

i. Ensuring Data security and privacy for sensitive financial information.

ii. Scalable system to support high volume transactions without degradation of performance.

iii. System should be able to response within less that 1 second on any transaction for fraud detection

iv. Provide high availability and minimal downtime, with target of 99% uptime.

8.3. Transition Requirements

1. Providing migration plan to migrate historical data into new system for training purposes in modelling
2. Integration with already existing infrastructure, such as databases, transaction systems and user authentication modules.
3. The fraud analysts and technical teams at the financial institutions will be trained in its usage and monitoring.
4. Specify a piloting phase where the system work alongside currently existing fraud detection mechanisms.

5. Support and maintenance teams will be set up for smooth operations is transitions and post-transitions.

8.4. Project Requirements

1. Establishment of clear timelines for projects and milestones against which progress can be tracked in light of the agreed timelines.
2. A dedicated project manager, along with dedicated team consisting of data-scientists, software developers and business analysts should be assigned.
3. Planning project budget which includes cost of hardware, software, development, testing and personnel.
4. Conducting risk assessments to identify valid risks, such as delays, data breach or system performance issues.
5. Implementing communication plan for updating on progress and issues to all stake holders.

8.5. Quality Requirements

1. Accuracy rate for detection of fraudulent transactions by the systems should be 95%.
2. Able to handle transaction volume of at least 10,000 transaction/second.
3. To ensure compliance with security and fraud detection standards regular system audits should be conducted.
4. System should provide a detailed report on false positives and negatives for monitoring purposes.
5. Customer satisfaction with minimization in transactional disruptions, false fraud alerts which affects legitimate transactions.

9. Acceptance Criteria

- The fraud transaction should at least be at 80% in pilot phase compared to present system.
- The system should be able to track fraudulent transaction in real-time with response time of 1 second.
- Regulatory compliance standards such as GDPR and PCI-DSS should be achieved by solution.
- Without degrading or performance issues, the system should be able to scale up to double the current volume.
- Detection accuracy with machine learning models should be 95% with less than 5% false positives.
- Classification of fraud types including transaction anomalies, identity theft and money laundering should be detected by system.
- Seamless integration of proposed system with existing systems of financial institutions without disruption in ongoing operations.
- Customized rule-based engine to assist analysts in easily changing and adding detection rules.
- A dashboard for monitoring fraud alerts, case tracking and system performance metrics.
- Historical fraud data are to be migrated successfully for the training of the model with no loss of data.
- Complete integration of the system and tested within live environment without any major disruptions of the transactions.
- 80% of staff training and assessments for competence should be completed who are involved in system monitoring.
- All critical milestones of the project must be on schedule.
- The project budget must not exceed by more than 10%.
- Risk assessments and mitigation strategies should be performed and identify risk rated as critical.
- System shall be highly available with 99% uptime.
- Test results should indicate system efficiency of the working under load and stress conditions.
- Ensuring data protection by going under security audits.
- Customer satisfaction should be achieved and not less than 85%.

10. Project Assumptions

- The infrastructure of financial institutions (databases, transaction systems and APIs) will already support integration with expert system with substantial modifications.
- Enough historical fraud data will be available for training machine learning models and setting accurate rules of detection.
- The system should process and analyse transaction data in real-time, without delays for timely fraud detection.
- Regulatory requirements will be stable within project timelines with adaption and accommodation of any minor changes in project scope.
- Timely mannered feedback will be provided to stake holders during the development, testing and pilot phases which will ensure that the system meets business and technical requirements.
- Sufficient funds and resources like developers, data scientists and infrastructure will be allocated to the project for developing and deploying the system.
- Change management processes including training staff to use the system effectively will be supported by financial institutions.
- Machine learning models of the system will refine by improving their accuracy when more data have been processed, with minimal manual intervention for fine-tuning.
- The project team will be afforded with appropriate freedom to employ industry best practices, processes and tools that ensure quality system design and deployment.
- The project will proceed without having any major legal, political and technological disruptions which could impact the timelines and scope of project.

11. Project Constraints

- **Time Constraint:** The event should occur in a period of 26 continuous weeks involving design, development, testing and deployment.
- **Budget Constraint:** The budget for this project is limited, hence any additional costs above than the allocated funds may not be approved which impacts the timelines and scope.
- **Data Privacy:** The system shall be obliged to comply with strict data privacy laws such as GDPR and PCI-DSS which will limit processing and storage of customer data.
- **Accuracy Requirements:** Potential complexity in the model or sources applied in the system can be caused due to accuracy requirement where system should be able to detect fraud with 95% accuracy and less than 5% false positive.
- **Scalability:** High volume in number of transactions requires the system to be highly scalable and involve substantial investments in infrastructure with cautious architectural planning.
- **Integration with Legacy Systems:** The financial institution with various legacy systems can poses integration challenges, extending development time or limiting some system functionalities.
- **Regulatory Compliance:** Maintaining updated financial regulations by the system can introduce new requirements during the development or after deployment.
- **Resource Availability:** The project is dependent on skilled personnels such as developers, data scientists and subject matter experts which can further affect project timelines.
- **User Adoption:** The system effectiveness will be limited by how quick and effectively the institution's personnel adopt and use the system.
- **Infrastructure Dependency:** Upgradation in existing IT infrastructure of financial institutions will be need for real-time processing capabilities of the system.

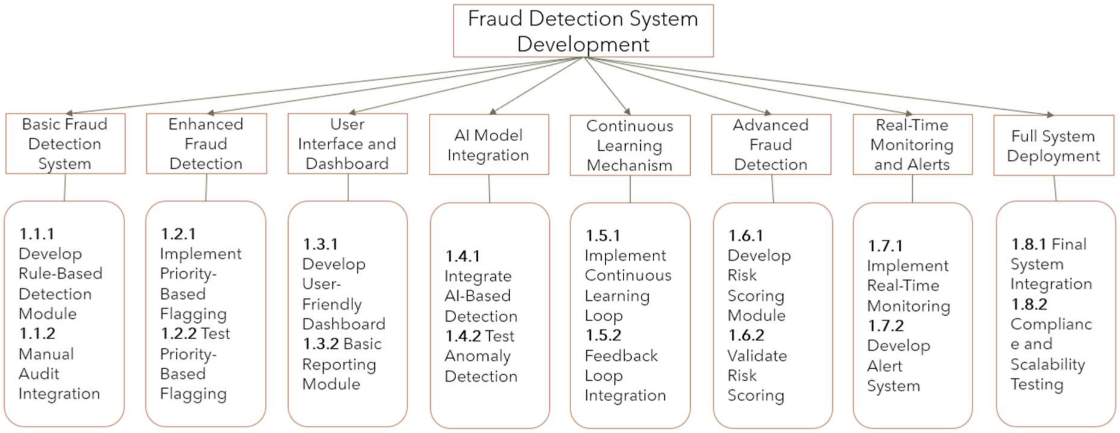
12. Scope Management

The scope management is an integral part of the Fraud Detection System project, ensuring that all activities are aligned with the project objectives and stakeholders' expectations. The scope defines the characteristics, outputs, and activities needed in the development of an artificial intelligence-based system capable of performing real-time fraud detection, automated notifications, and compliance with regulatory requirements.

This project entails the key characteristics of rule-based and artificial intelligence-driven fraud detection, prioritization-based flagging, risk assessment scoring, real-time surveillance, and an intuitive interface for notifications and reporting. The work scope of this project was broken down into manageable chunks using a **Work Breakdown Structure (WBS)** that included activities like data preparation, model creation, system integration, training, and deployment.

The **Change Control process** was in place to ensure that any kind of scope deviation should undergo review, analysis, and approval by the **Change Control Board (CCB)** before implementation. The scope creep was prevented; this means that the project was on track with integrity, and scope verification happened in the Sprint Reviews to ensure the deliverables would meet the requirements stipulated. The project team gave much attention to scope management, which guarantees that a final system would be realized on time and within the budgetary constraints, together with all functionalities required by the financial institutions and the stakeholders.

12.1. Work Breakdown Structure


Fraud Detection System Development
Basic Fraud Detection System
Enhanced Fraud Detection
User Interface and Dashboard
AI Model Integration
Continuous Learning Mechanism
Advanced Fraud Detection
Real-Time Monitoring and Alerts
Full System Deployment
1.1.1 Develop Rule-Based Detection Module 1.1.2 Manual Audit Integration
1.2.1 Implement Priority-Based Flagging 1.2.2 Test Priority-Based Flagging
1.3.1 Develop User-Friendly Dashboard 1.3.2 Basic Reporting Module
1.4.1 Integrate AI-Based Detection 1.4.2 Test Anomaly Detection
1.5.1 Implement Continuous Learning Loop 1.5.2 Feedback Loop Integration
1.6.1 Develop Risk Scoring Module 1.6.2 Validate Risk Scoring
1.7.1 Implement Real-Time Monitoring 1.7.2 Develop Alert System
1.8.1 Final System Integration 1.8.2 Compliance and Scalability Testing

The Work Breakdown Structure (WBS) of the Fraud Detection System Development project puts work in an organized way into manageable components. Broken down from the top level, the project has been put into eight major deliverables: Basic Fraud Detection System, Enhanced Fraud Detection, User Interface and Dashboard, and Full System Deployment. Each of these major deliverables is then broken down into specific tasks and subtasks. For instance, the basic fraud detection system includes tasks like developing a rule-based detection module and manual audit integration. This hierarchical structure brings clarity, hence allowing an easy way of making an assignment of responsibilities, resources estimation, and tracking. It supports effective planning, risk management, and communication with segmentation of work into clear and incremental components within a WBS for the project team. This approach is aligned with Agile methodologies, ensuring that every sprint delivers working, incremental outputs toward the effective realization of project goals.

12.2. Requirement Management Plan

The Requirements Management Plan for the Fraud Detection System to be installed in Financial Institutions outlines the process for identifying, documenting, analysing, prioritizing, and managing project requirements. It ensures consistency between the project scope, budget, and deliverables, as outlined in the cost breakdown structure. It enables effective traceability of requirements and change management within the life cycle of the project.

12.2.1. Requirement List

Category	Requirement Description	Related Subcomponent
Salaries (Team)	Assign personnel to project tasks, ensuring roles are clearly defined and documented.	Project Manager, Data Scientists, Data Engineer, Business Analyst, Software Developer, QA Engineer
Hardware & Software	Procure necessary hardware and software for system development and deployment.	High-Performance Laptops, Cloud Computing Services, Data Visualization Tools, Programming Tools
Data Acquisition	Obtain and clean datasets for training and testing the AI models.	Historical Fraud Dataset, Data Cleaning Services
Model Development & Testing	Develop, optimize, and validate AI fraud detection models.	Feature Engineering, Fraud Detection Model Development, Model Validation and Optimization
Training & Documentation	Create user manuals and conduct training sessions for end-users.	User Manuals, Training Sessions for End-Users
Deployment Costs	Integrate the system with banking infrastructure and set up real-time monitoring.	Integration with Banking Systems, Real-Time Monitoring Setup

12.2.2. Requirement Prioritization

Requirements will be prioritized based on project objectives and stakeholder needs. The prioritization will follow the **MoSCoW Method** (Must-Have, Should-Have, Could-Have, Won't-Have):

- **Must-Have**: Critical components for system functionality (e.g., AI model development, real-time monitoring).
- **Should-Have**: Important but not critical (e.g., enhanced dashboards).
- **Could-Have**: Optional features (e.g., additional reporting modules).
- **Won't-Have**: Features that can be deferred.

Action Priority Matrix for Fraud Detection System

Task	Impact	Effort	Category
Implement Rule-Based Detection	5	2	Quick Wins
Develop Priority-Based Flagging	4	3	Major Projects
Create User-Friendly Dashboard	4	3	Major Projects
Integrate AI-Based Detection	5	5	Major Projects
Continuous Learning Loop	5	5	Major Projects
Develop Risk Scoring Module	4	4	Major Projects
Real-Time Monitoring and Alerts	5	3	Quick Wins
Compliance and Scalability Testing	2	5	Thankless Tasks

12.2.3. Requirement Traceability Matrix

A traceability matrix will be maintained to ensure each requirement is linked to specific deliverables, tasks, and milestones. This will facilitate tracking and verification throughout the project.

Requirement ID	Requirement Description	Task/Subcomponent	Sprint	Status
R1	Develop Rule-Based Detection Module	Develop Rule-Based Detection	Sprint 1	In Progress
R2	Integrate AI-Based Detection	AI Model Integration	Sprint 4	Planned
R3	Real-Time Monitoring Setup	Real-Time Monitoring	Sprint 7	Planned
R4	User Training Sessions	Conduct Training Sessions for End-Users	Sprint 8	Planned

12.3. Change Management Process (Change Control Process)

12.3.1. Submission of Change Request

The change control process commences with a request for change being put in by the requestor. The Requester fills in the Change Request Form with information that includes the Project Name, Change Request Number, name of the Requestor, contact details, date of request, priority level, which could either be high, medium or low. The item to be changed, the detailed description of the change, the time by which the change would be forecasted to take place, and the costs estimated for it. This will ensure the need of the change is well communicated and documented for review by the project manager and other concerned stakeholders.

12.3.2. Change Evaluation

Once a change request is received, an evaluator conducts an assessment of the request. The evaluator assesses the anticipated consequences and identifies the work that would be required to effect the change. The impact of the change is assessed on key parameters: scope, schedule, cost, and quality. Each area of impact is covered in detail, and an impact rating (low, medium, or high) is assigned so that the consequences of the change can be clearly understood. This detailed analysis helps to distinguish the potential risks and benefits associated with the change.

12.3.3. Review and Approval

The Change Control Board is composed of the project manager and all key stakeholders. The CCB reviews the findings of the evaluator; based on that, a decision is made either to approve, reject, or defer the change. The decision is documented, including the name of the reviewer, the date of the review, and the reviewer's signature; comments may also be added to give context to the decision. This stage ensures that all changes are carefully assessed, and that approval is based on the project's priorities and constraints.

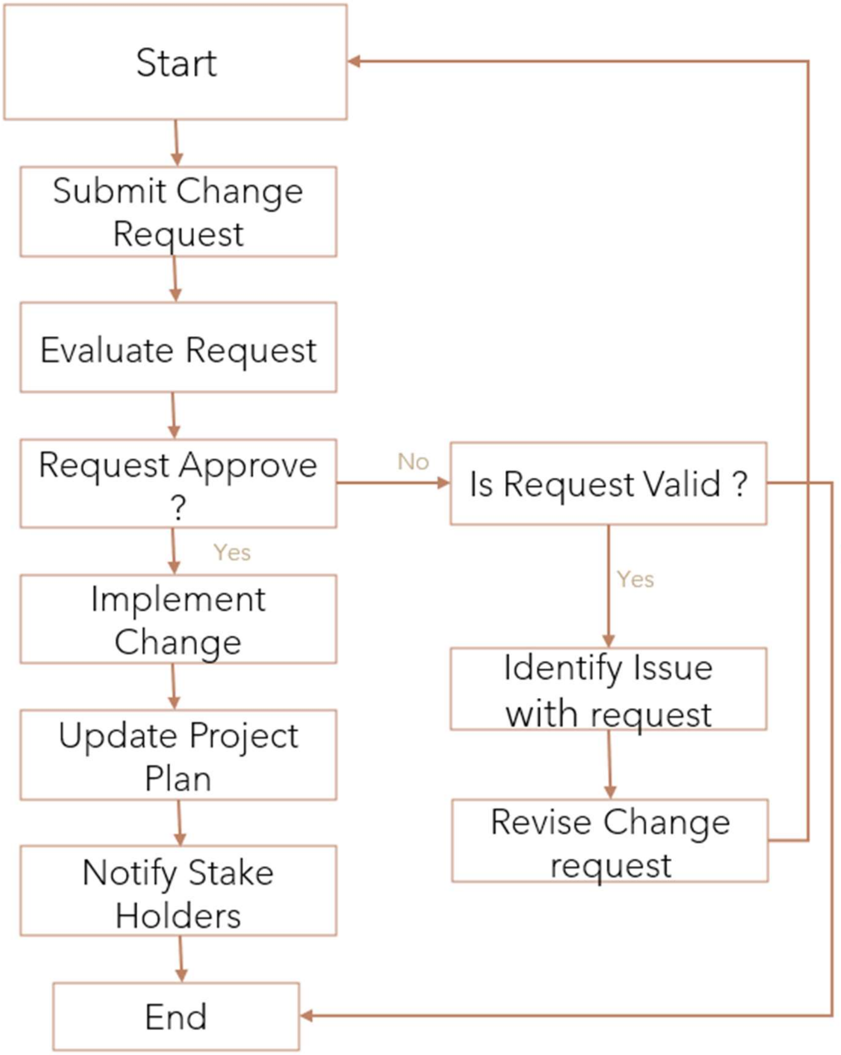
12.3.4. Implementation of change

Once the change has been approved, the project team carries out the change. The Project Plan is updated to reflect the change, and necessary adjustments are made in the tasks, timelines, and resources. All stakeholders are informed of the changes, and relevant documentation is updated to maintain consistency and transparency. This ensures that the change is seamlessly integrated into the project without affecting the bigger picture of objectives and goals.

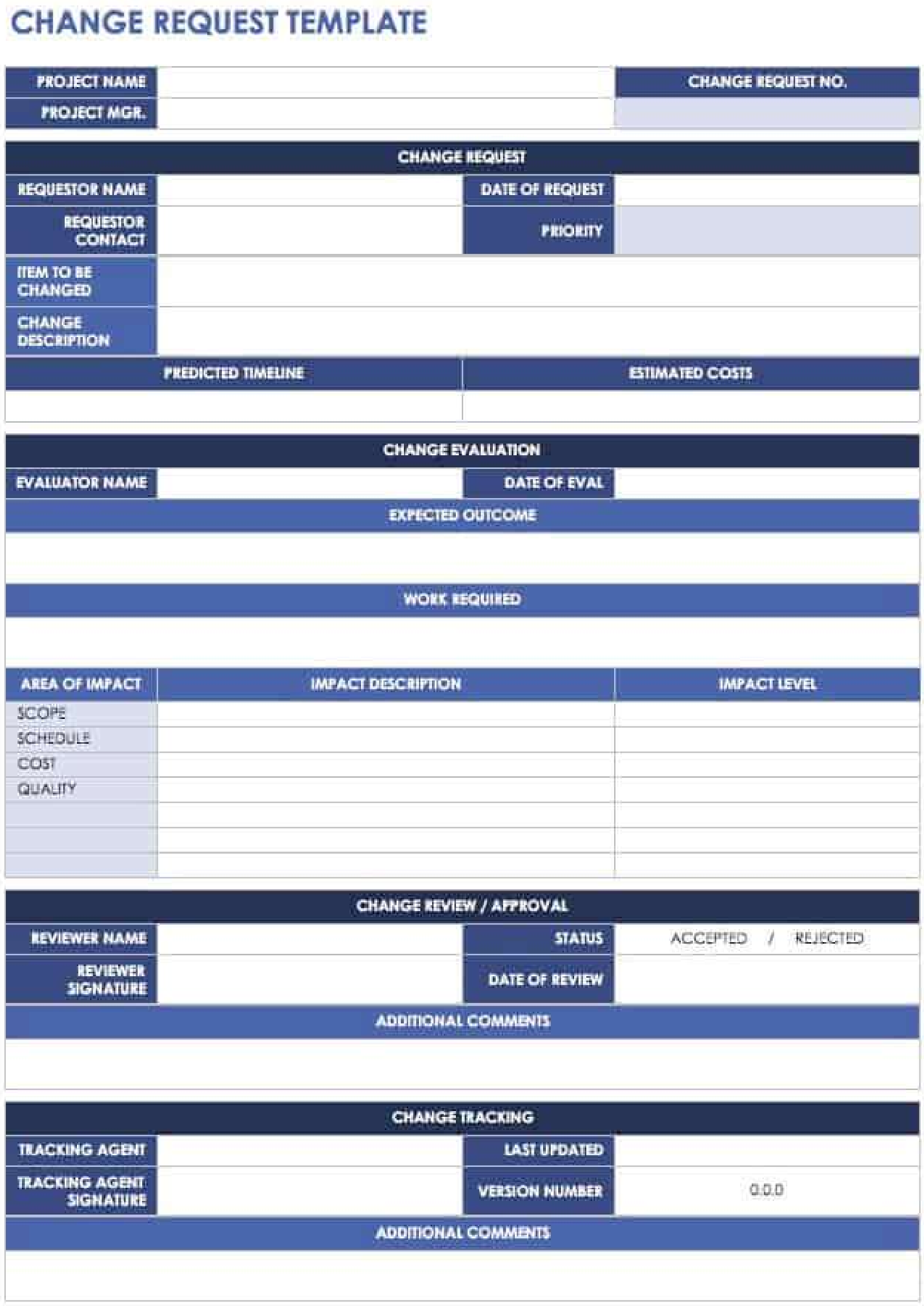
12.3.5. Change Tracking

The last step in the change control process is to track the implemented change. A tracking agent will monitor the change and update the form with details such as the last updated date, version number (for example, 1.1 or 2.0), and their signature. Further comments can be added to track progress or address any issues. This tracking ensures that changes are properly monitored and documented, hence helping to keep control over the project and avoid scope creep.

Change Control Flow Diagram



Change Request Template



CHANGE REQUEST TEMPLATE

PROJECT NAME		CHANGE REQUEST NO.
PROJECT MGR.		

CHANGE REQUEST			
REQUESTOR NAME		DATE OF REQUEST	
REQUESTOR CONTACT		PRIORITY	
ITEM TO BE CHANGED			
CHANGE DESCRIPTION			
PREDICTED TIMELINE		ESTIMATED COSTS	

CHANGE EVALUATION			
EVALUATOR NAME		DATE OF EVAL	
EXPECTED OUTCOME			
WORK REQUIRED			

AREA OF IMPACT	IMPACT DESCRIPTION	IMPACT LEVEL
SCOPE		
SCHEDULE		
COST		
QUALITY		

CHANGE REVIEW / APPROVAL			
REVIEWER NAME		STATUS	ACCEPTED / REJECTED
REVIEWER SIGNATURE		DATE OF REVIEW	
ADDITIONAL COMMENTS			

CHANGE TRACKING			
TRACKING AGENT		LAST UPDATED	
TRACKING AGENT SIGNATURE		VERSION NUMBER	0.0.0
ADDITIONAL COMMENTS			

13.Schedule Management

13.1. Sprint Planning and Deliverables

Sprint planning is a critical component of Agile project management; it defines what has to be done during a sprint. In the context of the Fraud Detection System for Financial Institutions, sprint planning ensures that each development cycle has a well-defined scope, realistic objectives, and clearly articulated deliverables. The process involves the project team coming together in order to decide which tasks and features will be accomplished within each sprint, based on the product backlog, team capacity, and project priorities. Proper sprint planning ensures that the team is focused, aligned, and productive throughout the whole project life cycle.

Sprint	Duration	Version	Deliverable	Key Features
Sprint 1	3 Weeks	v1.0	Basic fraud detection system that flags suspicious transactions.	Rule-based system for flagging potential fraud; requires manual audit.
Sprint 2	3 Weeks	v1.1	Enhanced fraud detection with priority-based flagging.	Flags suspicious transactions and highlights high-value transactions.
Sprint 3	3 Weeks	v1.2	Improved user interface and basic reporting dashboard.	User-friendly dashboard to view flagged transactions and generate basic reports.
Sprint 4	3 Weeks	v1.3	Integration of initial AI model for anomaly detection.	Combines rule-based and AI-based anomaly detection; flags unusual patterns.
Sprint 5	3 Weeks	v2.0	Continuous learning mechanism integrated into the AI model.	AI adapts to new fraud patterns; feedback loop for improving accuracy.
Sprint 6	3 Weeks	v2.1	Advanced fraud detection with risk scoring for flagged transactions.	Assigns risk scores to flagged transactions; highlights critical threats.
Sprint 7	3 Weeks	v2.2	Real-time monitoring and alert system implemented.	Real-time fraud detection and immediate alerts to users.
Sprint 8	3 Weeks	v3.0	Full-featured AI-powered fraud detection system with compliance and scalability.	Combines rule-based and AI detection, risk scoring, real-time alerts, and compliance features.

This project was allocated a uniform duration of 3 weeks for each sprint, allowing the team to plan, execute, and review consistently. The deliverables were broken down into smaller, manageable tasks, ensuring that at the end of every sprint, a working increment of the system was realized. For example, Sprint 1 was devoted to delivering the basic fraud detection system with rule-based flagging, while Sprint 2 added enhanced functionality with priority-based flagging for high-value transactions. Such an incremental approach would mean the project continuously delivers value to stakeholders while allowing time for feedback and adjustments.

During sprint planning, the team estimated several aspects to determine the expected story points for each sprint.

These would also contain the complexity of the tasks, dependencies on other features, and the team's historical velocity. In our case, tasks like AI model integration and continuous learning mechanisms were given higher story points because of their complexity and the need for strong testing. By estimating story points on these grounds, the team was able to plan and set realistic goals; therefore, expectations were appropriately managed.

Sprint planning: Each sprint started with a sprint planning meeting where the team discussed the product backlog and selected user stories to work on. The meeting included detailed discussions about the scope of each task, the criteria for completion, and expected challenges. This process ensured that everyone on the team understood their roles, responsibilities, and what was expected from the sprint.

Sprint planning also included the creation of a sprint backlog, which served as an adaptive list of tasks for the length of the sprint. The sprint backlog consisted of the selected user stories, tasks, and estimated story points, thus providing a clear plan for the team.

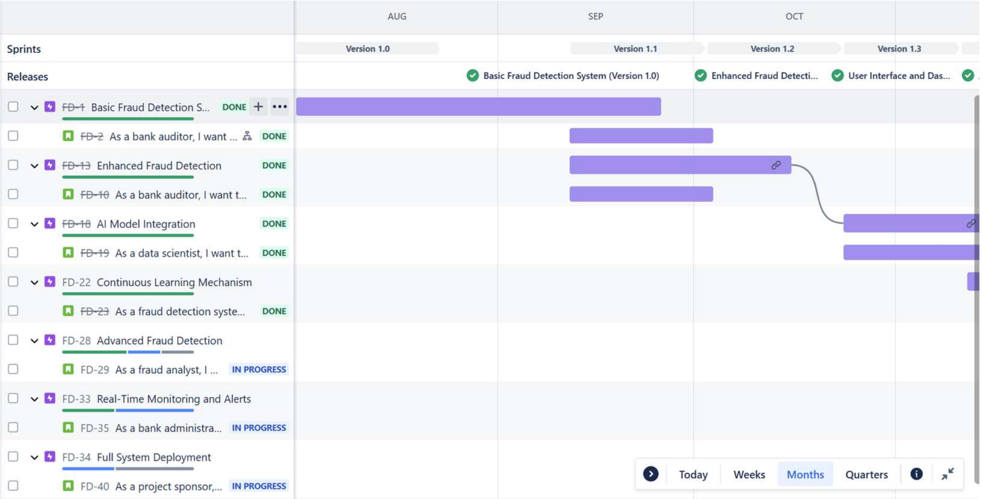
Throughout the sprint, the team held itself to daily stand-up meetings to review progress, acknowledge blockers, and adapt the plan as needed. That allowed the team to stay on top of their goals while adapting to changing requirements or new challenges.

At the end of every sprint, the team conducted a sprint review to demonstrate the work done to stakeholders and get their feedback. This feedback was used to update the product backlog and inform the following sprint planning meetings.

Moreover, the team held a sprint retrospective to review their performance, identify areas for improvement, and implement changes in future sprints. This continuous improvement helped the team grow in terms of efficiency, collaboration, and quality of delivery over time.

In summary, the sprint planning associated with the Fraud Detection System initiative facilitated a development process that was organized, clear, and flexible. Through the provision of incremental advancements during each sprint, the project fulfilled stakeholder anticipations and effectively tackled the complexities inherent in creating an advanced AI-driven system.

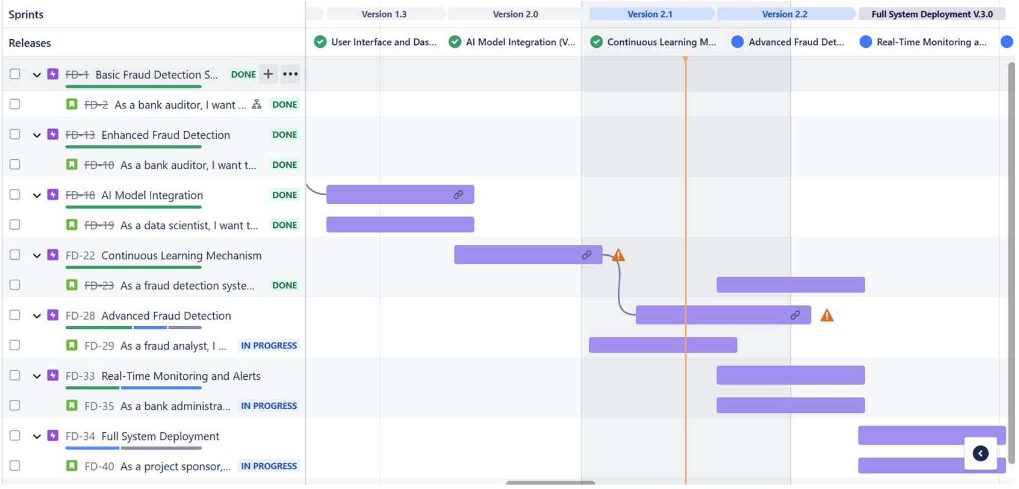
13.2. Roadmap (Timeline) in Jira- Gantt Chart



Sprints: Version 1.0 | Version 1.1 | Version 1.2 | Version 1.3

Releases: ✓ Basic Fraud Detection System (Version 1.0) | ✓ Enhanced Fraud Detecti... | ✓ User Interface and Das... | ✓ .

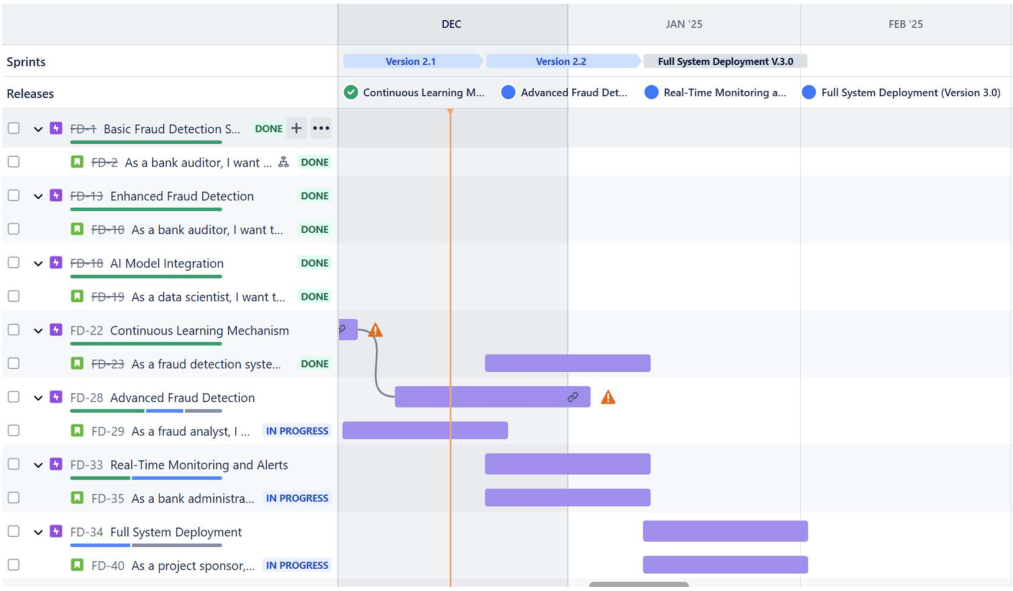
~~FD-1~~	Basic Fraud Detection S...	DONE
~~FD-2~~	As a bank auditor, I want ...	DONE
~~FD-13~~	Enhanced Fraud Detection	DONE
~~FD-10~~	As a bank auditor, I want t...	DONE
~~FD-18~~	AI Model Integration	DONE
~~FD-19~~	As a data scientist, I want t...	DONE
FD-22	Continuous Learning Mechanism	
~~FD-23~~	As a fraud detection syste...	DONE
FD-28	Advanced Fraud Detection	
FD-29	As a fraud analyst, I ...	IN PROGRESS
FD-33	Real-Time Monitoring and Alerts	
FD-35	As a bank administra...	IN PROGRESS
FD-34	Full System Deployment	
FD-40	As a project sponsor,...	IN PROGRESS



Sprints: Version 1.3 | Version 2.0 | Version 2.1 | Version 2.2 | Full System Deployment V.3.0

Releases: ✓ User Interface and Das... | ✓ AI Model Integration (V... | ✓ Continuous Learning M... | ● Advanced Fraud Det... | ● Real-Time Monitoring a... | ●

~~FD-1~~	Basic Fraud Detection S...	DONE
~~FD-2~~	As a bank auditor, I want ...	DONE
~~FD-13~~	Enhanced Fraud Detection	DONE
~~FD-10~~	As a bank auditor, I want t...	DONE
~~FD-18~~	AI Model Integration	DONE
~~FD-19~~	As a data scientist, I want t...	DONE
FD-22	Continuous Learning Mechanism	
~~FD-23~~	As a fraud detection syste...	DONE
FD-28	Advanced Fraud Detection	
FD-29	As a fraud analyst, I ...	IN PROGRESS
FD-33	Real-Time Monitoring and Alerts	
FD-35	As a bank administra...	IN PROGRESS
FD-34	Full System Deployment	
FD-40	As a project sponsor,...	IN PROGRESS



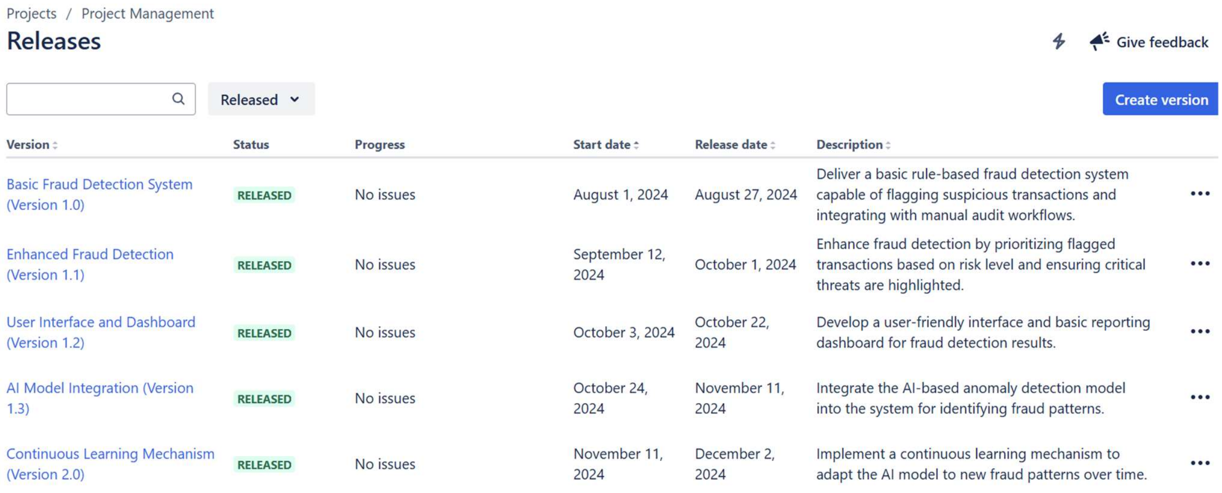
Sprints: Version 2.1 | Version 2.2 | Full System Deployment V.3.0

Releases: ✓ Continuous Learning M... | ● Advanced Fraud Det... | ● Real-Time Monitoring a... | ● Full System Deployment (Version 3.0)

~~FD-1~~	Basic Fraud Detection S...	DONE
~~FD-2~~	As a bank auditor, I want ...	DONE
~~FD-13~~	Enhanced Fraud Detection	DONE
~~FD-10~~	As a bank auditor, I want t...	DONE
~~FD-18~~	AI Model Integration	DONE
~~FD-19~~	As a data scientist, I want t...	DONE
FD-22	Continuous Learning Mechanism	
~~FD-23~~	As a fraud detection syste...	DONE
FD-28	Advanced Fraud Detection	
FD-29	As a fraud analyst, I ...	IN PROGRESS
FD-33	Real-Time Monitoring and Alerts	
FD-35	As a bank administra...	IN PROGRESS
FD-34	Full System Deployment	
FD-40	As a project sponsor,...	IN PROGRESS

13.3. Release Plans in Jira

Below are the screen shots of the version that has been released till date for each sprint. As mentioned in the schedule management, after each sprints a version of the app has been released.

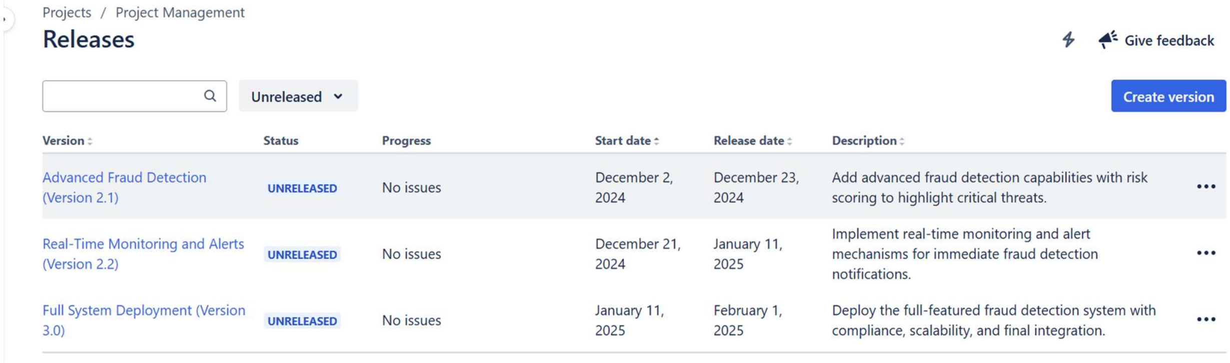


Projects / Project Management

Releases

Version	Status	Progress	Start date	Release date	Description
Basic Fraud Detection System (Version 1.0)	RELEASED	No issues	August 1, 2024	August 27, 2024	Deliver a basic rule-based fraud detection system capable of flagging suspicious transactions and integrating with manual audit workflows.
Enhanced Fraud Detection (Version 1.1)	RELEASED	No issues	September 12, 2024	October 1, 2024	Enhance fraud detection by prioritizing flagged transactions based on risk level and ensuring critical threats are highlighted.
User Interface and Dashboard (Version 1.2)	RELEASED	No issues	October 3, 2024	October 22, 2024	Develop a user-friendly interface and basic reporting dashboard for fraud detection results.
AI Model Integration (Version 1.3)	RELEASED	No issues	October 24, 2024	November 11, 2024	Integrate the AI-based anomaly detection model into the system for identifying fraud patterns.
Continuous Learning Mechanism (Version 2.0)	RELEASED	No issues	November 11, 2024	December 2, 2024	Implement a continuous learning mechanism to adapt the AI model to new fraud patterns over time.

Below are the planned version releases where the work is still in progress, the release dates have been set and these versions should be released by end of each last 3 sprints which are under progress at this point.



Projects / Project Management

Releases

Version	Status	Progress	Start date	Release date	Description
Advanced Fraud Detection (Version 2.1)	UNRELEASED	No issues	December 2, 2024	December 23, 2024	Add advanced fraud detection capabilities with risk scoring to highlight critical threats.
Real-Time Monitoring and Alerts (Version 2.2)	UNRELEASED	No issues	December 21, 2024	January 11, 2025	Implement real-time monitoring and alert mechanisms for immediate fraud detection notifications.
Full System Deployment (Version 3.0)	UNRELEASED	No issues	January 11, 2025	February 1, 2025	Deploy the full-featured fraud detection system with compliance, scalability, and final integration.

13.4. Tools and Approaches

The Fraud Detection System is implemented using Jira as the main tool for project management and hence the proper implementation of Agile methodologies. Jira supports many aspects related to the project, such as Gantt charts visualization, sprint planning, backlog management, and release tracking. The Gantt charts by Jira give a unique view of times, interdependencies, and critical paths of the projects, which allows the team to manage all schedules in an efficient way and to identify possible bottlenecks.

In sprint planning and backlog management, Jira allows for the creation and organization of user stories, tasks, and subtasks. The backlog is continuously refined to ensure that the most critical features are given priority for delivery. The use of sprint boards and Kanban views in Jira helps the team track progress in real time, thus facilitating daily stand-ups, sprint reviews, and retrospectives for process improvement and the timely removal of impediments.

Release management is supported using Jira, which enables the team to plan and manage the delivery of incremental versions of software iterations. Each sprint delivers a working component of the Fraud Detection System, thus assuring continuous integration and feedback from stakeholders. The release plan in Jira specifies milestones for each version, such as **v1.0 Basic Fraud Detection System**, **v1.1 Enhanced Fraud Detection, and v3.0 Full System Deployment**.

In its integration with Confluence and Slack, Jira enables the sharing of information, documentation, and real-time discussions for communication and collaboration. Teams can document requirements, changes, and sprint outcomes in Confluence to ensure that everything is transparent and traceable.

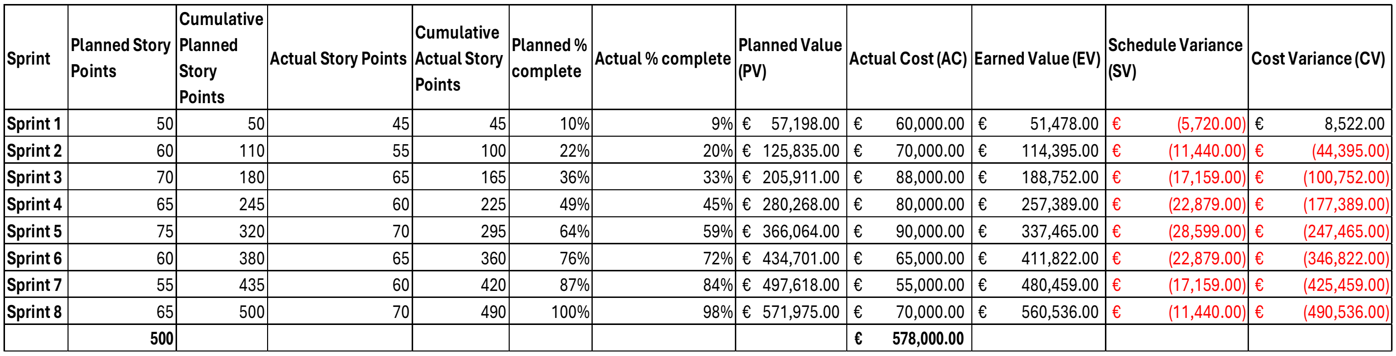
Jira dashboards provide the most powerful reporting and visualization capabilities for key metrics: sprint progress, task completion rates, and Earned Value Management (EVM) metrics such as cost variance (CV) and schedule variance (SV). Through Jira, the team ensures that the development of the Fraud Detection System is on time, in scope, and responsive to change.

14.Project Budget

The financial plan of the project is designed to include all critical elements, such as staff salaries, equipment, software, data procurement, model creation, training, and implementation expenses. It allows for a **10% contingency reserve and a 5% management reserve** to handle unforeseen problems, which keeps the project financially stable and flexible.

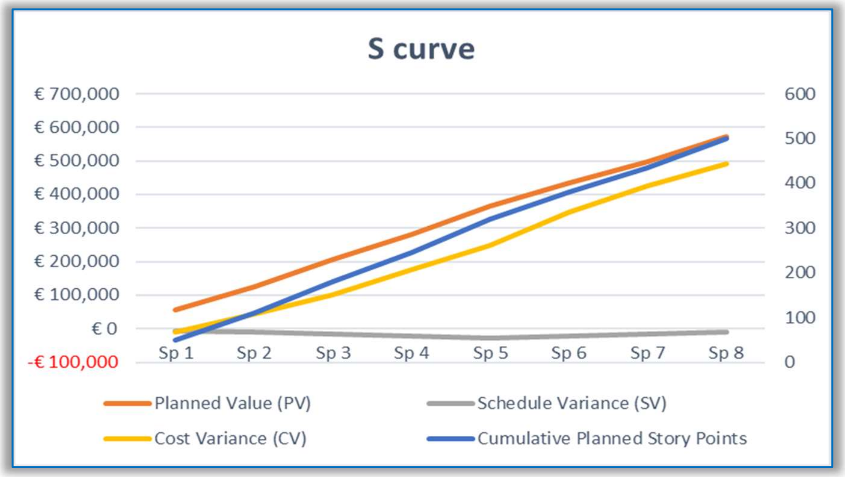
Component	Subcomponent	Cost	Total
Salaries (Team)	Project Manager	€ 50,000	
	Data Scientist (2 members)	€ 100,000	
	Data Engineer	€ 50,000	
	Business Analyst	€ 40,000	
	Software Developer	€ 40,000	
	QA Engineer	€ 20,000	
			€ 300,000
Hardware & Software	High-Performance Laptops (5 units)	€ 15,000	
	Cloud Computing Services (e.g., AWS)	€ 20,000	
	Data Visualization Tools (Tableau/Power BI licenses	€ 10,000	
	Programming Tools (Python libraries, IDEs)	€ 5,000	
			€ 50,000
Data Acquisition	Historical Fraud Dataset (Purchase)	€ 15,000	
	Data Cleaning Services	€ 10,000	
			€ 25,000
Model Development & Testing	Feature Engineering and EDA	€ 20,000	
	Fraud Detection Model (Development)	€ 30,000	
	Model Validation and Optimization	€ 20,000	
			€ 70,000
Training & Documentation	User Manuals	€ 10,000	
	Training Sessions for End-Users	€ 10,000	
			€ 20,000
Deployment Costs	Integration with Banking Systems	€ 20,000	
	Real-Time Monitoring Setup	€ 10,000	
			€ 30,000
Total			**€ 495,000**
Contingency Reserve (10%)		€ 49,500	
Management Reserve (5%)		€ 26,475	
			€ 75,975
Grand Total Estimated Budget			**€ 571,975**

15.Earned Value Management



Sprint	Planned Story Points	Cumulative Planned Story Points	Actual Story Points	Cumulative Actual Story Points	Planned % complete	Actual % complete	Planned Value (PV)	Actual Cost (AC)	Earned Value (EV)	Schedule Variance (SV)	Cost Variance (CV)
Sprint 1	50	50	45	45	10%	9%	€ 57,198.00	€ 60,000.00	€ 51,478.00	€ (5,720.00)	€ 8,522.00
Sprint 2	60	110	55	100	22%	20%	€ 125,835.00	€ 70,000.00	€ 114,395.00	€ (11,440.00)	€ (44,395.00)
Sprint 3	70	180	65	165	36%	33%	€ 205,911.00	€ 88,000.00	€ 188,752.00	€ (17,159.00)	€ (100,752.00)
Sprint 4	65	245	60	225	49%	45%	€ 280,268.00	€ 80,000.00	€ 257,389.00	€ (22,879.00)	€ (177,389.00)
Sprint 5	75	320	70	295	64%	59%	€ 366,064.00	€ 90,000.00	€ 337,465.00	€ (28,599.00)	€ (247,465.00)
Sprint 6	60	380	65	360	76%	72%	€ 434,701.00	€ 65,000.00	€ 411,822.00	€ (22,879.00)	€ (346,822.00)
Sprint 7	55	435	60	420	87%	84%	€ 497,618.00	€ 55,000.00	€ 480,459.00	€ (17,159.00)	€ (425,459.00)
Sprint 8	65	500	70	490	100%	98%	€ 571,975.00	€ 70,000.00	€ 560,536.00	€ (11,440.00)	€ (490,536.00)
	500							**€ 578,000.00**			

S Curve



Other Metrics

Metric	Value	Interpretation
BAC (Budget at Completion)	€ 571,975	Total planned budget.
CV (Cost Variance)	-€ 17,464	Over budget by €17,464.
SV (Schedule Variance)	-€ 11,439	Behind schedule by €11,439.
CPI (Cost Performance Index)	0.97	€0.97 worth of work per €1 spent.
SPI (Schedule Performance)	0.98	98% of planned work completed.
EAC (Estimate at Completion)	€ 589,660	Projected total cost at completion.
ETC (Estimate to Complete)	€ 11,660	Cost to complete remaining work.
VAC (Variance at Completion)	-€ 17,685	Expected to exceed budget by €17,685.
TCPI (To-Complete Index)	-1.9	Significant effort required to meet the budget.

15.1. EVM Analysis

1. **Cost Variance (CV) Analysis:** The CV is negative for all sprints, which means that the project overshot the budget. As indicated, Sprint 5 shows a CV of -€247,465, which means strong overruns due to a higher actual cost compared to the planned budget.
2. **Schedule Variance (SV) Analysis:** The SV is negative over most sprints, meaning the project is behind schedule. In Sprint 5, the SV is -€28,599, reflecting delays in completing planned tasks within the sprint timelines. This trend needs corrective measures to avoid further delays.
3. **Planned Value (PV) vs. Earned Value (EV):** The Planned Value (PV) consistently exceeds the Earned Value (EV), demonstrating that the work completed is less than initially planned. For Sprint 8, the PV is €571,975, while the EV is €560,536, indicating that progress did not fully meet expectations.
4. **S-Curve Insights:** The S-Curve shows an increasing gap between the Planned Value (orange line) and the Earned Value (blue line), which indicates cumulative delays and cost overruns, most recognizable by Sprint 8, where the cost variance remains high.
5. **BAC (Budget at Completion):** The total planned budget is €571,975, establishing the baseline for financial performance.
6. **CV (Cost Variance)**: The project is currently over budget by €17,464, indicating potential cost control issues.
7. **SV (Schedule Variance)**: The project is behind schedule by €11,439, necessitating immediate action to recover timelines.
8. **CPI (Cost Performance Index)**: With a CPI of 0.97, the project is spending slightly more than planned for each unit of work completed.
9. **SPI (Schedule Performance Index)**: An SPI of 0.98 shows the project is progressing at 98% of the planned schedule.
10. **EAC (Estimate at Completion)**: The total estimated cost to finish the project is now €589,660, higher than the original budget.
11. **ETC (Estimate to Complete)**: The remaining cost to complete the project is €11,660, requiring careful cost management.
12. **VAC (Variance at Completion)**: The project is forecasted to exceed the budget by €17,685, highlighting the need for corrective action.
13. **TCPI (To-Complete Performance Index)**: A TCPI of -1.9 shows significant effort and efficiency improvements are required to meet the original budget.
14. **Performance Trends**: The chronic cost and schedule disparities show issues with resource estimation and implementation. Stronger resource allocation and tighter project management controls are needed to align actual performance with planned objectives in future iterations. These EVM insights highlight the need for strategic adjustments in budget management, scheduling, and overall project execution to mitigate risks and improve project outcomes.

16.Resource Planning

16.1. RACI Matrix

Task / Deliverable	Project Manager (Aditya)	Business Analyst (Kartik)	Data Scientist	Data Engineer	Software Developer	QA Engineer	Compliance Officer
Requirement Gathering	R	A	C	C	I	I	C
System Design	A	C	C	C	R	I	C
Model Development	A	C	R	C	I	I	I
Integration & Deployment	A	C	I	R	R	I	C
Testing & QA	A	C	C	I	C	R	C
Compliance Validation	C	C	I	I	C	C	R
End-User Training	A	R	I	I	C	I	C

Key Points:

1. The RACI matrix clarifies project roles for tasks and deliverables.
2. The Project Manager overlooks and approves key tasks.
3. A Business Analyst is responsible for requirement gathering and end-user training.
4. Consultation with respect to system design, model development, and integration is provided by Data Scientists and Engineers.
5. Implementation and testing are the responsibility of the Software Developer and QA Engineer.
6. Compliance validation is ensured by the Compliance Officer in support of transparency and accountability throughout the project life cycle.

16.2. Resource Planning, Acquisition and Allocation

16.2.1. Resource Planning

Personnel:

Project Manager: Oversees project execution, schedules, and stakeholder communication.
Data Scientists (2): Develop and optimize fraud detection models using machine learning.
Data Engineer: Prepares, cleans, and manages datasets for model development.
Business Analyst: Gathers requirements, conducts stakeholder analysis, and ensures business needs are met.
Software Developer: Develops backend systems, APIs, and system integrations.
QA Engineer: Conducts rigorous quality assurance, unit tests, and integration tests.

Hardware:

5 High-Performance Laptops equipped with the latest specifications to handle data processing, model training, and software development tasks.

Software:

Cloud Services: AWS for cloud computing, storage, and deployment of AI models.
Data Visualization Tools: Tableau/Power BI for creating real-time dashboards and reports.
Programming Tools: Python libraries (TensorFlow, PyTorch, Scikit-learn) and IDEs (PyCharm, VS Code) for developing and testing machine learning models.

Data:

Historical Fraud Datasets: Curated datasets of previous fraud cases for model training.
Data Cleaning Services: Services for ensuring data quality, consistency, and completeness.

Budget:

A total budget of €571,975 allocated across 8 sprints to cover all project resources, personnel, and development needs.

16.2.2. Resource Acquisition

Personnel:

Assign team members based on required skill sets, availability, and project phases to ensure tasks are distributed effectively.

Hardware:

-Procure **5 high-performance laptops** with specifications such as Intel Core i7/i9 processors, 32GB RAM, 1TB SSD, and dedicated GPUs to support machine learning tasks and data processing.

Software:

Purchase licenses for **AWS cloud services**, including EC2, S3, and SageMaker for hosting models.

Obtain licenses for **Tableau/Power BI** for data visualization.

Acquire Python libraries and tools like TensorFlow, PyTorch, Scikit-learn, and Jupyter Notebook for model development.

Data:

Acquire comprehensive **historical fraud datasets** from reliable sources to ensure the AI models are trained with diverse and accurate data.

Utilize **data cleaning services** to preprocess and enhance the datasets for optimal model performance.

16.2.3. Resource Allocation

Sprint	Deliverable	Personnel	Hardware/Software	Data
Sprint 1	Basic fraud detection system that flags suspicious transactions.	Project Manager, Data Engineer, Business Analyst	5 Laptops, AWS	Historical Fraud Dataset
Sprint 2	Enhanced fraud detection with priority-based flagging.	Project Manager, Data Scientists (2), Data Engineer	AWS, Python libraries	Cleaned Fraud Dataset
Sprint 3	Improved UI and basic reporting dashboard.	Project Manager, Software Developer, Business Analyst	Laptops, Tableau/Power BI	Processed Fraud Data
Sprint 4	Initial AI model integration for anomaly detection.	Data Scientists (2), Data Engineer, QA Engineer	AWS, Python libraries	Cleaned Fraud Dataset
Sprint 5	Continuous learning mechanism in the AI model.	Data Scientists (2), Software Developer	AWS, Python libraries	Historical & New Fraud Data
Sprint 6	Advanced fraud detection with risk scoring.	Project Manager, Data Scientists (2), QA Engineer	AWS, Python libraries, Tableau	Risk-Scored Fraud Data
Sprint 7	Real-time monitoring and alert system.	Software Developer, QA Engineer	AWS, Tableau/Power BI, Real-Time Monitoring Tools	Real-Time Fraud Data
Sprint 8	Full-featured AI-powered system with compliance.	Project Manager, Business Analyst, QA Engineer	AWS, Python libraries, Tableau, Compliance Tools	Final Fraud Dataset

16.2.4. Resource optimization

Strategy	Details
Pair Programming	Data Scientists and Software Developers collaborate to improve efficiency and code quality.
Automated Testing	Use automated unit and integration tests to streamline QA processes.
Daily Stand-Ups	Conduct daily meetings to identify blockers and adjust resource allocation promptly.
Sprint Reviews and Retrospectives	Regular reviews to gather feedback and optimize resource usage for subsequent sprints.

Activity	Details
Weekly Progress Reports	Track the progress of tasks and resource utilization.
Burndown Charts	Monitor sprint progress and identify potential scope creep.
EVM (Earned Value Management)	Track cost and schedule performance using **CPI** and **SPI** metrics.
Change Control Process	Evaluate and approve changes in resource allocation through formal change requests.

16.3. Project Communication Plan

The communication plan has the objective of ensuring that all stakeholders and team members are updated on the progress, issues, changes, and major milestones of the project. Effective communication encourages transparency, supports timely decision-making, and ensures alignment with the project's goals.

16.3.1. Stakeholder Analysis

Stakeholder	Role	Interests/Expectations	Influence	Engagement Strategy
Project Sponsor	Oversees and funds the project	Timely delivery, budget adherence, risk management	High	Regular updates, progress reports
Project Manager	Manages project execution	On-time delivery, effective resource allocation	High	Daily stand-ups, sprint reviews
Data Scientists	Develop AI fraud detection models	Accurate models, data quality, timely tasks	Medium	Daily stand-ups, Slack communication
Business Analyst	Requirements gathering	Clear requirements, changes communicated promptly	Medium	Weekly meetings, documentation updates
Software Developer	Develops system components	Clear tasks, technical support, minimal scope changes	Medium	Daily stand-ups, Jira task tracking
QA Engineer	Quality assurance and testing	Thorough testing, timely fixes	Medium	Test reports, defect tracking, Slack updates
Compliance Officer	Ensures regulatory compliance	Adherence to GDPR, PCI-DSS	High	Monthly compliance reports, meetings
End Users	System users	User-friendly system, effective training	Low	Training sessions, user manuals

The stakeholder analysis table shows key project participants, their roles, expectations, and influence. It helps in the prioritization of communication and engagement strategies. Top on the list of high-influence stakeholders—Project Sponsor and Compliance Officer—demand frequent updates, while team members benefit from daily interactions. This ensures that everyone is on the same page and works in unison at all levels.

16.3.2. Stakeholder Communication Matrix

Stakeholder	Information Needs	Frequency	Communication Method	Owner
Project Sponsor	Progress reports, risks, budget updates	Bi-weekly	Email, Progress Report, Meeting	Project Manager
Project Manager	Detailed status updates, issues, risks	Weekly	Meetings, Emails, Jira Updates	Project Team Members
Data Scientists	Task updates, data issues, model performance	Daily	Stand-ups, Slack, Emails	Project Manager
Business Analyst	Requirement updates, changes, feedback	Weekly	Meetings, Jira Comments	Project Manager
Software Developer	Technical tasks, integration issues	Daily	Stand-ups, Slack, Jira	Project Manager
QA Engineer	Test progress, defects, issues	Weekly	Test Reports, Slack	Project Manager
Compliance Officer	Compliance status, audit results	Monthly	Compliance Reports, Meetings	Project Manager
End Users	Training updates, user feedback	After key milestones	Training Sessions, User Manual	Trainers, Business Analyst

The communication matrix documents information needs, frequency, methods, and responsible owners of each stakeholder. This structured approach guarantees that communication is timely and relevant, with a reduced possibility of misunderstanding. Regular updates through emails, meetings, and task-tracking tools like Jira will keep the stakeholders informed and engaged to ensure transparency and project success.

16.3.3. Communication Methods and Tools

Method/Tool	Purpose	Frequency	Audience
Email	General updates, reports, and official notices	Weekly/Bi-weekly	All stakeholders
Jira	Task tracking, sprint planning, issue management	Daily/Continuous	Project Team
Slack	Quick communication, task clarification	Daily	Project Team
Meetings	Status updates, discussions, and decision-making	Weekly/Bi-weekly	Project Team, Sponsors, Stakeholders
Progress Reports	Detailed status updates and milestone reviews	Bi-weekly	Project Sponsor, Manager
Dashboard (Tableau/Power BI)	Visual representation of project metrics	Weekly	Project Manager, Sponsors
Training Sessions	Educate end-users on system features	After Milestones	End Users
Compliance Reports	Ensure adherence to regulations	Monthly	Compliance Officer, Sponsors

16.3.4. Meeting Schedules

Meeting Type	Participants	Frequency	Purpose
Kick-off Meeting	Project Sponsor, Project Team	Once (Start)	Introduce project, roles, objectives
Sprint Planning Meeting	Project Manager, Project Team	Bi-weekly	Plan tasks and deliverables for each sprint
Daily Stand-Up	Project Team	Daily	Discuss progress, blockers, and tasks
Sprint Review Meeting	Project Team, Stakeholders	End of Sprint	Review completed work, demo deliverables
Sprint Retrospective	Project Team	End of Sprint	Discuss lessons learned, process improvements
Progress Update Meeting	Project Sponsor, Project Manager	Bi-weekly	Review project progress, budget, and risks
Risk Review Meeting	Project Manager, Team Members	Monthly	Identify, assess, and mitigate risks
Compliance Review Meeting	Compliance Officer, Project Manager	Monthly	Ensure regulatory compliance (GDPR, PCI-DSS)

16.3.5. Escalation Plan

Issue Level	Description	Escalation Contact	Resolution Timeframe
Low	Minor issues, no immediate impact	Project Manager	Within 2 business days
Medium	Issues impacting timeline or deliverables	Project Manager, Team Lead	Within 1 business day
High	Critical issues affecting project success	Project Sponsor	Immediate (within hours)

17.Risk Management

17.1. Risk Analysis

Effective risk management for the Fraud Detection System includes identification, analysis, and mitigation of risks that might affect the project results. Using techniques such as brainstorming, expert judgment, and analysis of historical data, the risk categories have been identified to be the following ones:

1. **Technical Risks:** Issues related to model performance, data integration, and system compatibility.
2. **Schedule Risks:** Delays due to unexpected technical challenges or resource availability.
3. **Cost Risks:** Budget overruns caused by unforeseen expenses in hardware, software, or personnel.
4. **Compliance Risks:** Non-adherence to financial regulations such as GDPR and PCI-DSS.
5. **Resource Risks:** Lack of availability or loss of key personnel during critical project phases.

17.2. Risk Tolerances and Risk Thresholds

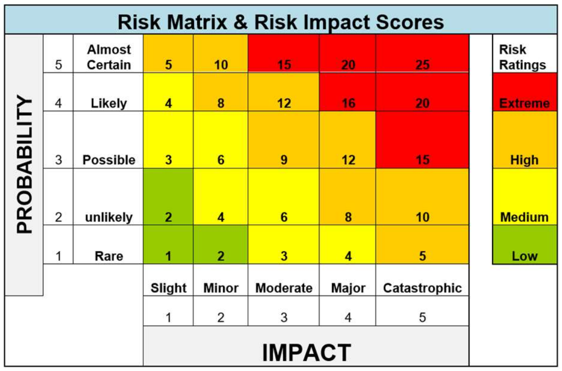
Risk Tolerance:

The project team has moderate risk tolerance in regard to technical and scheduling risks; however, low risk tolerance with respect to compliance and budgetary risks.

Threshold:

1. **Schedule Threshold:** No delay beyond 2 weeks per sprint.
2. **Cost Threshold:** Budget overruns not exceeding €20,000.
3. **Compliance Threshold:** Zero tolerance for violations of GDPR and PCI-DSS regulations.

Risk Impact Scores



Risk Matrix & Risk Impact Scores

PROBABILITY	5	Almost Certain	5	10	15	20	25	Risk Ratings
	4	Likely	4	8	12	16	20	Extreme
	3	Possible	3	6	9	12	15	High
	2	unlikely	2	4	6	8	10	Medium
	1	Rare	1	2	3	4	5	Low
			Slight	Minor	Moderate	Major	Catastrophic	
			1	2	3	4	5	
			IMPACT					

17.3. Risk Register

Ref No.	Risk Category	Risk Description (Cause and Effect)	Risk Type	P	I	Score (P × I)	Risk Response (Actions)	Owner
R1	Technical	Inconsistent data quality affects model performance	Threat	4	5	20	**Mitigate**- Implement rigorous data validation and cleaning processes	Data Scientist
R2	Technical	System integration issues with legacy infrastructure	Threat	3	4	12	**Mitigate**- Conduct early integration testing	Software Developer
R3	Schedule	Delay in acquiring historical datasets	Threat	3	4	12	**Avoid**- Establish strict SLA with data providers	Data Engineer
R4	Cost	Budget overrun due to additional hardware requirements	Threat	2	5	10	**Transfer**- Pre-approve contingency funds	Project Manager
R5	Compliance	Non-compliance with GDPR or PCI-DSS	Threat	2	5	10	**Mitigate**- Conduct regular compliance audits	Compliance Officer
R6	Resource	Loss of key personnel during critical project phases	Threat	3	4	12	**Mitigate**- Crosstrain team members	Project Manager
R7	Security	Data breach during data acquisition or processing	Threat	4	5	20	**Avoid**- Implement encryption and secure data handling procedures	Security Officer
R8	Technological	Model fails to detect new or evolving fraud patterns	Threat	3	5	15	**Mitigate**- Continuous model training and updates	Data Scientist
R9	Operational	Incorrect model predictions leading to false positives	Threat	4	4	16	**Mitigate**- Implement feedback loops for model correction	Data Analyst
R10	Environmental	Power outages affecting system availability	Threat	2	3	6	**Accept**- Use backup power solutions	IT Administrator

Accept: The risk is acknowledged, but no immediate action is taken, often due to low impact or probability.

Mitigate: Actions are taken to reduce the probability or impact of the risk.

Avoid: Steps are taken to eliminate the risk entirely, such as changing project plans or processes.

Transfer: The risk is transferred to a third party, such as through insurance or outsourcing.

17.4. Quantitative and Qualitative Risk Assessment

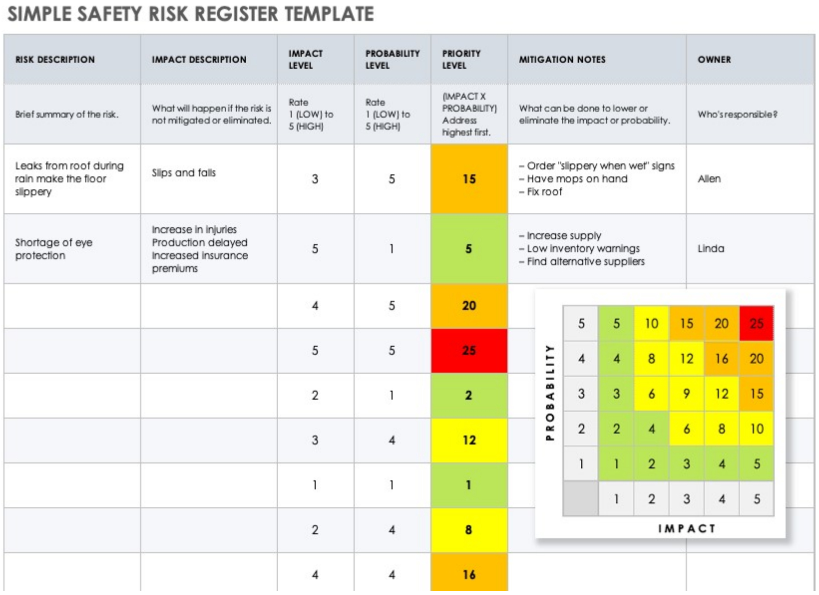
17.4.1. Quantitative Assessment:

- **Probability (P):** Rated on a scale of **1 to 5** (1 = Very Low, 5 = Very High).
- **Impact (I):** Rated on a scale of **1 to 5** (1 = Minimal Impact, 5 = Catastrophic Impact).
- **Risk Score:** Calculated as **P × I**; risks are prioritized based on this score.
  - **High Risk:** Score ≥ 15
  - **Medium Risk:** Score between 10 and 14
  - **Low Risk:** Score ≤ 9

17.4.2. Qualitative Assessment:

- **Risk Description:** Each risk is described based on potential causes and effects.
- **Risk Type:** Classified as **Threat** (negative risk).
- **Response Strategies:** Include **Mitigation, Avoidance, Transfer,** or **Acceptance**.
- **Ownership:** Clearly assigned to ensure accountability for risk management.

17.5. Risk Register template



SIMPLE SAFETY RISK REGISTER TEMPLATE

RISK DESCRIPTION	IMPACT DESCRIPTION	IMPACT LEVEL	PROBABILITY LEVEL	PRIORITY LEVEL	MITIGATION NOTES	OWNER
Brief summary of the risk.	What will happen if the risk is not mitigated or eliminated.	Rate 1 (LOW) to 5 (HIGH)	Rate 1 (LOW) to 5 (HIGH)	(IMPACT X PROBABILITY) Address highest first.	What can be done to lower or eliminate the impact or probability.	Who's responsible?
Leaks from roof during rain make the floor slippery	Slips and falls	3	5	15	– Order "slippery when wet" signs – Have mops on hand – Fix roof	Allen
Shortage of eye protection	Increase in injuries Production delayed Increased insurance premiums	5	1	5	– Increase supply – Low inventory warnings – Find alternative suppliers	Linda
		4	5	20		
		5	5	25		
		2	1	2		
		3	4	12		
		1	1	1		
		2	4	8		
		4	4	16		

PROBABILITY					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	IMPACT				

18.Stakeholder’s Definition of Done (DoD)

18.1. Definition of Done in Template form

Stakeholder	Deliverable/Task	Criteria for Completion (Definition of Done)	Approval Required	Verification Method
Project Sponsor	Final Fraud Detection System	System meets all functional requirements, compliance with regulations (GDPR, PCI-DSS), and performance benchmarks.	Yes	Formal sign-off, compliance audit
Bank Auditor	Fraud Detection Reports	Reports provide accurate, detailed, and prioritized fraud analysis for suspicious transactions.	Yes	Report validation, audit review
Data Scientist	Fraud Detection Model	Model achieves 95% accuracy, adapts to new fraud patterns, and passes all validation tests.	No	Model performance metrics
Business Analyst	Requirement Documentation	All business requirements are documented, validated, and signed off by stakeholders.	Yes	Document review, stakeholder sign-off
Software Developer	System Integration	Seamless integration with existing banking infrastructure and APIs.	No	Integration testing, QA reports
QA Engineer	System Testing and QA	All critical bugs fixed, and the system passes all regression, load, and security testing.	No	QA test results, bug reports
End-Users (Bank Staff)	User Training & Documentation	Training sessions completed, user manuals provided, and staff confident in using the system.	No	Training feedback, usability test
Compliance Officer	Compliance Validation	System complies with all legal and regulatory standards (GDPR, PCI-DSS).	Yes	Compliance audit report

- **Stakeholder:** The individual or group responsible for or impacted by the deliverable/task.
- **Deliverable/Task:** The specific output or task that needs to be completed.
- **Criteria for Completion (Definition of Done):** The measurable criteria to determine that the task or deliverable is complete.
- **Approval Required:** Indicates if formal approval is needed from the stakeholder.
- **Verification Method:** How the completion of the deliverable/task will be verified.

This template ensures transparency, accountability, and consistency of the project deliverables, thereby aiding an effective project closure process.

19.Critical Evaluation

The effort to develop the Fraud Detection System for this project was challenging, especially for us using project management tools, collaboration, and time constraints.

The biggest challenge that we faced were how to use Jira effectively for sprint planning and tracking deliverables. While Jira is a powerful tool, some getting used to was required in setting up epics, user stories, tasks, and sub-tasks.

Initially, there were a few struggles in learning how to break the project down into manageable tasks and estimate story points accurately. Some tasks proved to be much more challenging than envisioned, throwing off our timelines, so we revised our sprint goals.

The organization and supervision of sprints were not easy due to the scholarly nature of the project, further constrained by the time. That we had to coordinate was a challenge, compounded by other academic responsibilities leading to pressure.

There have been instances where the deliverables of one sprint got into those of the subsequent sprint because of our miscalculations regarding time needed for research and documentation. As such, we had to continuously reprioritize and refine the backlog to ensure that we were on track with the top-level project deadlines.

We had problems with the financial management aspect of the project. Even though the budget was a simulation, it was hard to accurately estimate costs related to software tools, human resources, and other assets, since we did not have much practical experience. For instance, estimating the costs of cloud services and data purchase required extensive research, and sometimes we found it difficult to align these estimates with the constraints of the project. This activity underscored the intricacies involved in budgetary planning and emphasized the significance of maintaining contingency reserves, even within simulated contexts.

The other challenge was collaboration and communication. This was a group effort, so the scheduling and the fair allocation of work required constant communication. There were instances where there had been a misunderstanding or delays because of not clearly spelling out the roles and responsibilities.

This became most apparent while working on detailed sections, such as the WBS and resource management plan, where making sure that our work was aligned with each other's contributions required more effort than anticipated.

We did solve these issues with the help of regular meetings and discussions, but it really underlined how essential proper communication and documentation is.

References

Books

1. **Kerzner, H. (2017).** *Project Management: A Systems Approach to Planning, Scheduling, and Controlling* (12th ed.). John Wiley & Sons.

   A comprehensive guide on project management methodologies, tools, and techniques.

2. **Schwalbe, K. (2015).** *Information Technology Project Management* (8th ed.). Cengage Learning.

   Covers IT-specific project management practices, including Agile methodologies and risk management.

3. **Lock, D. (2020).** *Project Management* (10th ed.). Routledge.

   Detailed insights into project planning, change control, and stakeholder management.

Websites

1. **Project Management Institute (PMI)**
   Project Management Framework and Best Practices.
   https://www.pmi.org

2. **Atlassian – Jira Software Guide**
   Using Jira for Sprint Planning, Backlog Management, and Agile Project Management.
   https://www.atlassian.com/software/jira

3. **Lucidchart**
   Creating Effective Work Breakdown Structures and Flowcharts.
   https://www.lucidchart.com

4. **Wrike**
   Project Risk Management Guide.
   https://www.wrike.com/project-management-guide/risk-management

5. **Smartsheet**
   Project Planning Templates and Tools for Budgeting.
   https://www.smartsheet.com

6. **MindTools**
   Tools for Communication Plans and Stakeholder Analysis.
   https://www.mindtools.com

Research Papers

7. **Turner, J. R., & Müller, R. (2005).** *The Project Manager's Leadership Style as a Success Factor on Projects.*
   Project Management Journal, 36(2), 49-61.
   https://doi.org/10.1177/875697280503600206

   - Discusses the role of leadership in project success.

8. **Sanghi, P., Panda, S. K., Pati, C., & Gantayat, P. K. (2022).** *Learning Deep Features and Classification for Fresh or Off Vegetables to Prevent Food Wastage Using Machine Learning Algorithms.*
   Smart Innovation, Systems and Technologies.
   https://doi.org/10.1007/978-981-16-6624-7_44

   - Insights into AI applications for classification and quality control.

4. **Online Tools and Templates**

   1. **GanttPro**
      Creating Gantt Charts and Managing Project Timelines.
      https://ganttpro.com

   2. **LucidSpark**
      Brainstorming and Collaborative Diagram Tools for Teams.
      https://www.lucidspark.com

Acknowledgement

We would like to express our sincere gratitude to **Professor Luciana Nascimento** for her invaluable guidance, feedback, and support throughout this project. Her expertise and encouragement were instrumental in helping us achieve the successful completion of this work.

We acknowledge the use of **ChatGPT** as a tool to better understand concepts, generate ideas, and clarify project management methodologies. Additionally, we utilized **class materials, lecture notes, PowerPoint presentations, Jira**, and **Google** for research, sprint planning, backlog management, and gathering supplementary information. These resources were used responsibly to enhance our comprehension and ensure the accuracy and completeness of our work.

We affirm that all the work presented in this project is **original**, reflecting our joint research, analysis, and effort. This project is a culmination of our teamwork, dedication, and shared commitment to delivering a high-quality outcome.