**AGILE DOCUMENTS**

**Document 1: Definition of Done Checklist for a Fraud Management Project:**

|  |  |
| --- | --- |
| **Checklist Item** | **Description** |
| 1. Produced Code for Presumed Functionalities | All planned functionalities, as per user stories, have been implemented. |
| 1. Assumptions of User Story Met | All business and technical assumptions in the user story are validated and fulfilled. |
| 1. Project Builds Without Errors | The code compiles successfully with no errors in the build pipeline. |
| 1. Unit Tests Written and Passing | Unit tests cover the agreed minimum coverage and pass successfully. |
| 1. Project Developed on Test Environment | Development and testing performed on an environment identical to production. |
| 1. Test on Devices/Browsers Listed Passed | Feature tested on all supported devices, browsers, and platforms as listed in project assumptions. |
| 1. Feature OK-ed by UX Designer | UX design and usability approved by the UX designer |
| 1. QA Performed and Issues Resolved | QA validated the features, and all issues raised are resolved. |
| 1. Feature Tested Against Acceptance Criteria | Feature satisfies all acceptance criteria and business requirements. |
| 1. Feature OK-ed by Product Owner | The Product Owner has reviewed and approved the completed feature. |
| 1. Refactoring Completed | Code refactoring is performed to enhance maintainability and performance. |
| 1. Configuration or Build Changes Documented | Any system configuration or build changes are documented clearly. |
| 1. Documentation Updated | User guides, technical specs, and other documentation are updated as necessary. |
| 1. Peer Code Review Performed | Code reviewed by peers and approved for quality and standards. |

**Document 2- Product Vision**

|  |  |  |  |
| --- | --- | --- | --- |
| **Scrum Project**  **Name: Mastercard Developer Zone (Fraud Management)** | | | |
| **Venue: Kalpana Chawala meeting room** | | | |
| **Date: 13/12/2024** | **Start Time: 10 am** | **End Time: 12 pm** | **Duration: 2 hrs** |
| **Client: Marian Western** | | | |
| **Stakeholder List:**   1. Vijay Singh 2. Rami Lengadhare 3. Puja Sahay 4. Komal Pardeshi 5. Jayashree Gosavi | | | |
| **Scrum Team** | | | |
| **Scrum Master:** Jayesh Rajput | | | |
| **Product Owner:** Kunal Datta | | | |
| **Scrum Developer 1:** Sandeep Goyal | | | |
| **Scrum Developer 2:** Rakhi Thakare | | | |
| **Scrum Developer 3:** Neeta Singh | | | |
| **Scrum Developer 4:** Amit Verma | | | |
| **Scrum Developer 5:** Digvijay Khade | | | |
| **Scrum Developer 6:** Nikhil Sharma | | | |
| **Vision:** To create an intelligent, adaptive, and user-friendly fraud management solution that proactively detects and prevents fraudulent activities in real time, safeguarding businesses and customers while ensuring compliance with regulatory standards.   |  |  |  |  | | --- | --- | --- | --- | | **Target Group** | **Needs** | **Product** | **Value** | | **Market Segment Addressed**  **Industries:**  Financial Services (Banks, Payment Processors, FinTechs )  E-Commerce and Retail  Insurance Providers  **Market Type:**  Enterprises handling large-scale transactions or sensitive customer data.  Business operating in high-risk environments prone to fraudulent activities.  **Target Users and Customers**  **Primary User (Operational Level):**  **Fraud Analysts:** Investigating suspicious activities.  **Risk Management Teams:** Monitoring fraud trends and preventing losses.  **Compliance Officers:** Ensuring adherence to regulations like AML, PCI-DSS, GDPR.  **IT Teams:** Managing system integration and performance.  **Customers (Decision-Makers):**  C-Level Executives  Risk Managers and Directors  Business Owners  Government and Regulatory Bodies | **Problem the Product Solves**  **1. Fraud Detection and Prevention:**   * Identifies and mitigates fraudulent activities in real-time (e.g. transaction fraud, identity theft).  1. **Operational Inefficiency:**  * Reduces the time and resources spent on manual fraud detection processes.  1. **Financial Loss:**  * Minimize monetary losses caused by fraud across industries.   **Benefits Provided**   1. **Enhanced Security:**  * Provides businesses with robust fraud prevention mechanism and data.  1. **Real-Time Insights:**  * Delivers actionable alerts and insights for swift decision-making. | The product is an **intelligent fraud management system** that combines advanced analytics, machine learning, and real-time monitoring to detect, prevent and mitigate fraudulent activities across industries.  **What Makes it Desirable and Special?**   1. **Real-Time Fraud Detection:**  * Uses AL/ML algoriths to identify suspicious patterns and anomalies as they occur.  1. **Comprehensive Coverage:**  * Monitors transactions, user behaviour, and other critical data points across multiple channels (web, mobile, APIs)   **Is it Feasible to Develop the Product?**  Yes, the product is feasible to develop considering the following factors:   1. **Technological Maturity:**  * Proven technologies like AI/ML, big data analytics, and cloud computing are available to support the system.  1. **Market Demand:**  * Growing need across industries for robust fraud management solutions. | **How the Product Benefits the Company**   1. **Revenue Protection:**   Reduces finacial losses caused by fraud, ensuring profitability.   1. **Market Differentiation:**   Positions the company as a trusted provider of fraud prevention solutions, enhancing its competitive edge.  **Business Goals**   1. **Increase Market Share:**   Capture a significant portion of the fraud prevention market across industries.   1. **Revenue Growth:**   Achieve profitability through subscription-based or licensing revenue streams.   1. **Strength Brand Reputation:**   Establish the company as a trusted leader in fraud management solutions. | |  |  |  |  | | | | |

**Document 3: User stories**

|  |  |  |
| --- | --- | --- |
| **User story No:** 1 | **Tasks:**   1. Define criteria for suspicious activities. 2. Implement real-time monitoring system. 3. Test with historical data | **Priority:**  High |
| **Value Statement:**  As a user, I want to detect suspicious transactions in real-time, so that I can minimize potential losses. | | |
| **BV:** 500 | **CP:** 10 | |
| **Acceptance criteria: -** Transactions flagged for anomalies within 5 seconds.   * Alert sent to the appropriate team. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 2** | **Tasks: 1.** Design report templates.  2. Integrate with data base.  3. Ensure real time updates. | **Priority:** Medium |
| **Value Statement:** As user, I want to view detailed reports of fraudulent activities, so that I can analyze patterns | | |
| **BV:** 200 | **CP:** 10 | |
| **Acceptance criteria:** - Reports generated in under 2 minutes.   * Includes key details like time, amount, and pattern description. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 3** | **Tasks:** 1. Establish account blocking criteria.  2. Automate the blocking process.  3. Notify users of actions taken. | **Priority:** High |
| **Value Statement:** As a user, I want to block the flagged accounts automatically, so that I can prevent further fraud. | | |
| **BV:** 500 | **CP:** 10 | |
| **Acceptance criteria:**   * Accounts flagged as fraudulent are blocked instantly. * Notifications sent within 5 minutes. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 4** | **Tasks:** 1. Develop a review dashboard.  2. Implement an approval workflow.  3. Log reviewer actions. | **Priority:** Medium |
| **Value Statement:** As a user, I want to review flagged transactions manually, so that I can verify false positives. | | |
| **BV:** 200 | **CP:** 20 | |
| **Acceptance criteria:** - Reviewers can access transactions easily.   * Decisions logged with time stamps. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 5** | **Tasks:** 1. Define risk thresholds.  2. Create notifications on the system (email/SMS).  3. Test notifications for speed. | **Priority:** High |
| **Value Statement:** As a user, I want to receive alerts for high-risk transactions, so that I can act immediately. | | |
| **BV:** 500 | **CP:** 10 | |
| **Acceptance criteria:**   * Alerts received within 1 minute of detection. * Include transaction details for quick actions. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 6.** | **Tasks:** 1. Develop a whitelist feature.  2. Test with sample data.  3. Allow updates to the whitelist | **Priority:** Low |
| **Value Statement:** As a user, I want to whitelist trusted user, so I can reduce false positive. | | |
| **BV:** 100 | **CP:** 10 | |
| criteria:   * Trusted users bypass fraud checks successfully. * Whitelist updated without errors. | | |
|  | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 7** | **Tasks:** Login monitoring | **Priority:** High |
| **Value Statement:** As a user, I want unusual login patterns flagged to prevent unauthorized access. | | |
| **BV:** 500 | **CP:** 20 | |
| **Acceptance criteria:**  Alert triggered when multiple failed login attempts occur within 5 minutes | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 8** | **Tasks:** Transaction anomaly detection | **Priority:** Medium |
| **Value Statement:** As a user, I want anomalous transactions flagged to prevent financial loss. | | |
| **BV:** 200 | **CP:** 10 | |
| **Acceptance criteria:** Any transaction deviating by 30% from typical behaviour is flagged within 5 seconds. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 9** | **Tasks:** Geolocation mismatch alerts | **Priority:** High |
| **Value Statement:** As a user, I want to be notified if my account is accessed from multiple locations rapidly. | | |
| **BV:** 500 | **CP:** 20 | |
| **Acceptance criteria:** Notifications sent for logins occurring in two locations > 50 miles apart within 1 hour. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 10** | **Tasks:** Suspicious device detection | **Priority:** High |
| **Value Statement:** As a user, I want login attempts from unknown devices flagged for review. | | |
| **BV:** 500 | **CP:** 10 | |
| **Acceptance criteria:** Alert sent if a device not previously linked to the account attempts to access. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 11** | **Tasks:** Password strength check | **Priority:** High |
| **Value Statement:** As a user, I want to ensure my password meets complexity requirements to prevent breaches. | | |
| **BV:** 500 | **CP:** 10 | |
| **Acceptance criteria:** Password must be > 8 charts, including uppercase, lowercase, numbers, and symbols. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 12** | **Tasks:** Two-factor authentication | **Priority:** High |
| **Value Statement:** As a user, I want to enable 2FA to add an extra layer of security. | | |
| **BV:** 500 | **CP:** 20 | |
| **Acceptance criteria:** Users can enable 2FA, and login requires both password and OTP. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 13** | **Tasks:** Blacklist flagged IPs | **Priority:** Medium |
| **Value Statement:** As a user, I want to know if fraudulent IPs are blocked to secure my account. | | |
| **BV:** 200 | **CP:** 10 | |
| **Acceptance criteria:** All login attempts from blacklisted Ips are denied access. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 14** | **Tasks:** Real-time fraud notifications | **Priority:** High |
| **Value Statement:** As a user, I want instant alerts for suspected fraudulent activity. | | |
| **BV:** 500 | **CP:** 20 | |
| **Acceptance criteria:** Alerts sent within 10 seconds of suspicious activity detection. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 15** | **Tasks:** Account freeze feature | **Priority:** Medium |
| **Value Statement:** As a user, I want to freeze the account immediately if fraud is detected. | | |
| **BV:** 200 | **CP:** 20 | |
| **Acceptance criteria:** User can freeze their account via app or web, blocking all actions. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 16** | **Tasks:** Unusual transaction approval | **Priority:** High |
| **Value Statement:** As a user, I want to approve transactions flagged as unusual. | | |
| **BV:** 500 | **CP:** 10 | |
| **Acceptance criteria:** Notifications sent for flagged transactions with options to approve or decline. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 17** | **Tasks:** Frequent password change alert | **Priority:** Medium |
| **Value Statement:** As a user, I want alerts for frequent password changes to detect potential fraud. | | |
| **BV:** 200 | **CP:** 10 | |
| **Acceptance criteria:** Users receive alerts if more than 2 password changes occur within 24 hours. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 18** | **Tasks:** Role-based access control | **Priority:** High |
| **Value Statement:** As an admin, I want role-based permissions to limit fraud exposure. | | |
| **BV:** 500 | **CP:** 20 | |
| **Acceptance criteria:** Users only access the functionalities based on their assigned roles. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 19** | **Tasks:** Audit trail logging | **Priority:** Medium |
| **Value Statement:** As an admin, I want all activities logged for review during investigations. | | |
| **BV:** 200 | **CP:** 10 | |
| **Acceptance criteria:** Logs must capture user ID, time stamp, and action details for all activities. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 20** | **Tasks:** Data encryption | **Priority:** High |
| **Value Statement:** As a user, I want sensitive data encrypted to prevent unauthorized access. | | |
| **BV:** 500 | **CP:** 20 | |
| **Acceptance criteria:** All PII is encrypted in transit and at rest using industry-standard protocols. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 21** | **Tasks:** Fraud metrics dashboard | **Priority:** Medium |
| **Value Statement:** As a manager, I want a dashboard showing key fraud metrics to monitor trends. | | |
| **BV:** 200 | **CP:** 10 | |
| **Acceptance criteria:** The dashboard displays the number of flagged transactions. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 22** | **Tasks:** Machine learning integration | **Priority:** Low |
| **Value Statement:** As a user, I want fraud detection to improve using machine learning | | |
| **BV:** 100 | **CP:** 10 | |
| **Acceptance criteria:** ML model identifies patterns and reduces false positive by 10% | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 23** | **Tasks:** Customer reporting feature | **Priority:** Medium |
| **Value Statement:** As a user, I want to report suspected fraud for immediate investigation. | | |
| **BV:** 200 | **CP:** 20 | |
| **Acceptance criteria:** User can submit fraud reports via app or web, and receive confirmation. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 24** | **Tasks:** Automatic account lock | **Priority:** High |
| **Value Statement:** As user, I want my account locked after repeated failed access attempts. | | |
| **BV:** 500 | **CP:** 20 | |
| **Acceptance criteria:** Account locked after 5 failed login attempts within 10 minutes. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 25** | **Tasks:** Anti-phishing warnings | **Priority:** Medium |
| **Value Statement:** As a user, I want warnings for suspected phishing message. | | |
| **BV:** 200 | **CP:** 20 | |
| **Acceptance criteria:** Flagged emails or messages contain warnings and reporting options. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 26** | **Tasks:** Device fingerprinting | **Priority:** Low |
| **Value Statement:** As a user, I want my devices uniquely identified to flag unfamiliar devices. | | |
| **BV:** 100 | **CP:** 10 | |
| **Acceptance criteria:** Each device generates a unique ID; anomalies are flagged if new IDs appear. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 27** | **Tasks:** Suspicious time activity flag | **Priority:** Medium |
| **Value Statement:** As a user, I want alerts for account activity during unusual hours. | | |
| **BV:** 200 | **CP:** 20 | |
| **Acceptance criteria:** Alerts sent if transactions occur between 2 AM and 4 AM outside typical patterns. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 28** | **Tasks:** Fraud detection API | **Priority:** Low |
| **Value Statement:** As a developer, I want an API to integrate fraud detection with other systems. | | |
| **BV:** 100 | **CP:** 10 | |
| **Acceptance criteria:** API provides real-time fraud risk assessments for input transactions. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 29** | **Tasks:** High-value transactions alerts. | **Priority:** Medium |
| **Value Statement:** As a user, I want alerts for high-value transactions to confirm them. | | |
| **BV:** 200 | **CP:** 20 | |
| **Acceptance criteria:** Transactions > $ 5000 require use confirmation. | | |

|  |  |  |
| --- | --- | --- |
| **User story No: 30** | **Tasks:** Session timeout enforcement | **Priority:** High |
| **Value Statement:** As a user, I want automatic logouts after inactivity to secure my account. | | |
| **BV: 500** | **CP:** 20 | |
| **Acceptance criteria:** Sessions expire after 10 minutes of inactivity. | | |

**Document 4: Agile PO Experience**

The Product Owner plays a critical role in defining and delivering a fraud management product by blending domain expertise with market awareness. Below are the responsibilities tailored to a fraud management project:

1. Market Analysis:

* The PO conducts thorough research on **market needs and demand** for fraud detection and prevention solutions.
* The PO analyzes trends in **fraudulent activities** across industries (e.g. financial services, e-commerce, insurance).
* Study **competitive products** in the fraud management domain to identify unique selling points (USPs) and gaps.
* Assess emerging technologies like AI, machine learning, and behavioral analytics for fraud detection.
* Engage with industry experts, regulatory bodies, and stakeholders to understand **compliance requirements.**

1. **Enterprise Analysis:**

In a fraud management project, Enterprise Analysis focuses on evaluating the feasibility, value, and alignment of the product with organizational goals.

* **Due Diligence on Market Opportunities:**

The PO assesses the financial and strategic opportunity of developing a fraud management system. This involves understanding the customer base (e.g. banks, fintech, e-commerce) and determining ROI based on the reduction in fraud incidents and compliance adherence.

1. **Product Vision and Roadmap**

* **Product Vision Keeping Market Analysis in Mind:**

The vision for the fraud management system is to create a robust, AI-driven, and adaptive tool that detects and prevents fraudulent activities in real time, ensuring minimal disruption to genuine users.

* **Product Roadmap with High-Level Features and Timelines:**

The roadmap includes milestones such as integrating machine learning models, multi-channel fraud detection, and providing advanced reporting tools. Timelines account for iterative development and continuous feedback.

1. **Managing Product Features**

* **Managing Stakeholder Expectations:**

The PO works closely with stakeholders like banks, security teams, and regulatory bodies to gather requirements and address their concerns.

* **Prioritization of Epics, Stories, and Features:**

Features such as real-time anomaly detection, user behavior analysis, and customizable risk scoring are prioritized based on criticality and ROI.

1. **Managing Product Backlog:**

* **Prioritization of User Stories:**

User stories like “As a fraud analyst, I want to receive real-time alerts for suspicious activities” are ranked based on urgency and user impact.

* **Re-Prioritization Based on Stakeholder Needs:**

Adjustments are made to address emerging threats or regulatory changes. For instance, a new law requiring detailed audit trails might lead to a reprioritization of backlog items.

1. **Managing Overall Iteration Progress**

* **Sprint Progress Review:**

The PO participates in sprint reviews to assess completed work, ensuring alignment with the product vision.

* **Re-Prioritization of Sprints and Epics if Needed:**

If market demands shift, such as an uptick in fraud via mobile channels, the PO adapts the roadmap to prioritize mobile-specific features.

* **Sprint Retrospectives with Business Analyst:**

Post-sprint reviews involve discussing challenges, such as delayed feedback from fraud analysts, and finding solutions to improve future iterations.

* **From this project I have learned how to handle sprint meetings such as**

1. **Sprint Planning Meeting:**

* Collaborated with the scrum Master and Development Team to define sprint aligned with the product roadmap.
* Prioritized user stories from the product backlog based on their value and urgency, ensuring alignment with stakeholder needs.
* Clearly communicated acceptance criteria for features such as real-time fraud detection and customizable dashboards.
* Addressed any technical or functional queries from the team, ensuring the scope of work was well understood.

1. **Daily Scrum Meeting:**

* Participated as an observer to understand team progress and any roadblocks they faced, ensuring I could provide support where necessary.
* Provided clarifications on user stories to keep the team aligned with the sprint goal.
* Monitored progress on high-priority tasks like fraud alert system integration to ensure timely delivery.

1. **Sprint Review Meeting:**

* Reviewed the completed work with stakeholders, ensuring it met acceptance criteria and aligned with the fraud management vision.
* Demonstrated key features, such as machine learning-driven fraud detection, to stakeholders for feedback and validation.
* Documented feedback for refining or reprioritizing upcoming backlog items based on stockholder insights.

1. **Sprint Retrospective Meeting**

* Collaborated with the Scrum Master and team to reflect on what went well and areas for improvement.
* Discussed challenges like delays in third-party API integration for fraud detection and proposed solutions for early dependency management.
* Suggested process improvements, such as more frequent stakeholder check-ins to enhance communication and reduce rework.

1. **Backlog Refinement Meeting:**

* Engaged with the Business Analyst and team to refine and elaborate user stories, ensuring they were ready for upcoming sprints.
* Adjusted priorities based on emerging fraud trends or regulatory changes, such as the need for real-time compliance reporting.
* Also, User stories creation and what things will be included in user stories such as

**User Story Template**

1. **Story No:** Unique identifier for tracking (e.g. FMS-001)
2. **Title:** A short, descriptive title for the story.
3. **Description:** Follows the format:

* **As a** [type of user],
* **I want to [**perform an action**],**
* **So that [**achieve a goal**]**

1. **Tasks:** Key tasks needed to complete the story.
2. **Priority:** The level of importance (High, Medium, Low)
3. **Acceptance Criteria:** Clear conditions that must be met for the story to be considered done.
4. **BV (Business Value):** The value this story delivers to the business.
5. **CP (Complexity Points):** The estimated effort or complexity of the story.

Example:

1. **Story No:** FMS-001
2. **Title:** Detect fraudulent transactions in real-time
3. **Description:**

* As a fraud analyst,
* I want the system to identify and flag suspicious transactions in real-time,
* So that I can review and take necessary action promptly.

1. **Tasks:**

* Integrate a rule-based fraud detection engine.
* Configure real-time transaction monitoring.
* Send flagged transactions to the review queue.

1. **Priority:** High
2. **Acceptance Criteria:**

* Transactions exceeding the predefined thresholds are flagged automatically.
* Notifications are sent to fraud analysts within 5 seconds of detection.
* A log of flagged transactions is maintained for further review.

1. **BV:** 8
2. **CP:** 5

**Document 5: Product and sprint backlog and product and sprint burndown Charts**

**Product backlog:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **User Story ID** | **User Story** | **Tasks** | **Priority** | **BV** | **CP** | **Sprint** |
| US 001 | As a fraud analyst, I want to monitor transactions in real-time, so I can detect an opalise quickly. | Design a real-time monitoring dashboard and implement anomaly detection logic Integrate data streams for transactions. | High | 500 | 20 | Sprint 1 |
| US 002 | As a compliance, I want a report of flagged transactions, so I can meet regulatory requirements. | Define reporting templates, implement data export functionality, and add filters for flagged transactions | High | 500 | 20 | Sprint 1 |
| US 003 | As a risk manager, I want AI-powered risk scoring, so I can prioritize potential threats. | Develop risk scoring model Train and test AI algorithms Integrate scoring into dashboards. | High | 500 | 20 | Sprint 2 |
| US 004 | As a fraud analyst, I want to customize detection rules, so I can adapt to changing fraud patterns. | Create rule editor UI-Implement rule engine backend Test rule application on sample data. | Medium | 200 | 10 | Sprint 2 |
| US 005 | As an IT admin, I want to configure access controls, so only authorized user can access the system. | Design role-based access control system- Develop user authentication mechanism. Test permission | Medium | 200 | 10 | Sprint 3 |
| US 006 | As a business owner, I want a summary dashboard,, so I can track overall fraud trends at a glance. | Design dashboard layout.   * Implement trend analysis charts- Test summary report generation. | Low | 100 | 10 | Sprint 3 |

A graph showing the number of people in the same direction

Description automatically generated with medium confidence

**Sprint backlog:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **User Story ID** | **User Story** | **Tasks** | **Owner** | **Status** | **Estimated efforts** |
| US 001 | As a fraud analyst, I want to monitor transactions in real-time, so I can detect anomalies quickly. | Design a real-time monitoring dashboard to implement anomaly detection logic and integrate data streams for transactions. | Developer A | In-progress | 16 |
| US 002 | As a compliance officer, I want a report of flagged transactions, so I can meet regulatory requirements. | Define reporting templates and implement Data export functionality. | Developer B | Not started | 12 |
| US 003 | As a risk manager, I want AI-powered risk scoring, so I can prioritize potential threats. | Develop risk scoring model Train and test AI algorithms Integrate scoring into the dashboard | Data Scientist C | In progress | **20** |
| US 004 | As a fraud analyst, I want to customize detection rules, so I can adapt to changing fraud patterns. | * Create rule edit or UI-Implement rule engine backend-Test rule application on sample data. | Developer (Amit Verma) | Not Started | 15 |
| US 005 | As an IT admin, I want to configure access controls, so that only authorized users can access the system | * Design a role-based access control system Develop a user authentication mechanism. * Test permission | Developer (Kunal Datta) | Not Started | **10** |

A graph with blue squares and numbers

Description automatically generated

**Document 6: Sprint meetings**

**Meeting TypeMeeting Type 1: Sprint Planning meeting**

|  |  |
| --- | --- |
| **Date** | 1-12-2024 |
| **Time** | 10 am |
| **Location** | Pune |
| **Prepared By** | Komal Pardeshi |
| **Attendees** | Rami Lengadhare, Puja Sahay, Nikhil Sharama, Digvijay Khade |

**Agenda Topics**

|  |  |  |
| --- | --- | --- |
| Topic | Presenter | Time allotted |
| Introduction to Fraud Management | Rami Lengadhare | 10 |
| Types of Fraud | Sreelekha Ashok | 15 |
| Fraud Detection Technique | Puja Sahay | 15 |
| Case studies | Nikhil Sharma | 20 |
| Fraud Prevention Strategies | Digvijay Khade | 25 |
| Tools and Technologies in Fraud | Amruta Patil | 15 |
| Q & A Session | Sujoy Datta | 20 |

**Other Information:**

|  |  |
| --- | --- |
| **Category** | **Details** |
| **Observers** | Aarju Patel |
| Ketan Somane |
| Pratik Sawant |
| **Resources** | **Presentation Slides** |
| * Fraud Management Software (Azure) |
| * Internet Access |
| * Reference Documents (case studies) |
| **Special Notes** | * Ensure all participants have access to the necessary resources beforehand. |
| * Q & A session to be moderated by Pallavi Patil |
| * Observer to provide feedback at the end of the session. |
| * Backup of all materials to be stored on TRC for future use. |

**Meeting Type 2:** **Sprint review meeting**

|  |  |
| --- | --- |
| **Date** | 13-12-2024 |
| **Time** | 12 pm |
| **Location** | Homi Bhabha meeting room |
| **Prepared By** | Komal Pardeshi |

|  |  |  |  |
| --- | --- | --- | --- |
| **Sprint status** | **Things to demo** | **Quick updates** | **What’s next** |
| Current Sprint: Sprint 3 | Fraud detection workflow (UI/UX) | * The fraud prevention module is in final testing phase | Begin integration testing with payment gateway systems |
| Overall Status: On Track/At Track/ Delayed | * Reports generated from fraud detection module | * Stakeholder review schedule for Date | * Conduct a workshop for end users on fraud alert dashboards |
| Key Completed Tasks: - Finalized fraud detection requirements - Integrated fraud detection algorithm - Prepared user stories for fraud prevention workflows  Pending Tasks: - Test validation for fraud alerts - Stakeholder review of the case study module  Blockers:   * Delayed feedback from Nikhil Mane - Dependency on third-party fraud detection API integration | * Sample fraud case study documentation | * QA team identified and fixed [3] of bugs | * Complete documentation for fraud detection guidelines. |

**Meeting Type 3: Sprint retrospective meeting**

|  |  |
| --- | --- |
| Date | 23-12-2024 |
| Time | 10 am |
| Location | Rameswaram meeting room |
| Prepared By | Komal Pardeshi |
| Attendees | Rami Patil |
|  | Manoj Kumar |
|  | Jaykirthee Nayar |
|  | Poonam Wagh |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Agenda** | **What Went Well** | **What Didn’t Go Well** | **Questions** | **References** |
| 1. Welcome and Objectives of the Retrospective | * Fraud detection requirements were finalized ahead of schedule. | * Delays in third-party API responses affecting integration timelines. | * What steps can we take to avoid rework in the next sprint? | * Sprint Goal Document (3) |
| 1. Review of Sprint Goals | * Seamless collaboration between the development and QA teams | * Limited testing resources led to a backlog in test cases. | -How can we communicate between stakeholders and the team? | * Project Timeline and Deliverable Plan |
| 1. Discuss “What Went Well” | * Successful integration of fraud detection tools with the existing system. | * Miscommunication on fraud alert dashboard requirements causes rework. | * What additional resources or tools do we need to address current blockers? | * Issue/Bug Tracker Logs |
| 1. Discuss “What didn't Well” | Delay in third-party API responses affecting integration timelines | * Insufficient time allocated for stakeholder's training. | * Are there any process improvements to speed up API integration? | * Stakeholder Feedback from Sprint Demo |
| 1. Identify Improvement Areas | Finalized fraud detection requirements ahead of schedule. | Misalignment in understanding fraud alert dashboard requirements caused rework | What measures can be taken to prevent rework in requirements? | Stakeholder Feedback Notes from Sprint Demo |
| 1. Action Items and Next Steps | The team met 90% of the sprint goals on time, despite external challenges. | Limited test coverage for edge cases due to insufficient time and resources. | What strategies can be implemented to improve test coverage for edge cases? | Test Coverage Metrics Report |
| 1. Wrap-Up and Closing Remarks | Resolved critical issues in the fraud reporting module ahead of the deadline. | Limited focus on user training and onboarding processes. | How can we improve our testing strategy to cover all edge cases in the next sprint? | Test Reports Highlighting Gaps and Coverage |

**Meeting Type 4: Daily Stand-up meeting**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Question** | **Name/Role** |  | | | | |
| Monday | Tuesday | Wednesday | Thursday | Friday | |  |
| **What did**  **you do**  **yesterday?** | * Amruta Madale * Sumit Solankar * Nikhil Sharma | * Designed the real-time monitoring dashboard. * Started integrating transaction data streams. | * Finished integrating data streams. * Developed initial anomaly detection algorithm. | -Tested anomaly detection logic.  - Made adjustments based on the test results.  - Refined dashboard layout. | * Implemented filters for flagged transactions. * Completed export functionality for compliance reports. | * Completed rule editor UI draft.Finalized user authentication design. | |  |
| **What will**  **you do**  **today?** | * Puja Patil * Sarika Raghuvanshi * Raj Pardeshi | * Complete data stream integration. * Begin implementing anomaly detection logic. | * Test anomaly detection logic. * Refine monitoring dashboard layout. | Implement filters for flagged transactions in compliance reports. | * Start working on rule editor UI. * Draft user authentication mechanism design. | * Conduct peer reviews of implemented features. * Resolve pending bugs. | |  |
| **What (if**  **any) is**  **blocking**  **your**  **progress?** | * Sachin Raghuvanshi * Sahil Kamble * Aarju Patel | None | Delay in receiving test data from QA team. | Dependency on database configuration updates | * Pending confirmation rule editor specs. | None | |  |