**Name-Amruta Bishwas**

**Project -Live Project Waterfall Methodology**

Que-Document 6- Please prepare a use case diagram, activity diagram and a use case specification

Document?

**Ans:**

**Use Case Diagram:**



**Activity diagram:**

1)REGISTER:



2)LOGIN AND 3) Customer due diligence

4) SAR And 5) Transaction Monitoring

**USE CASE SPECIFICATION:**

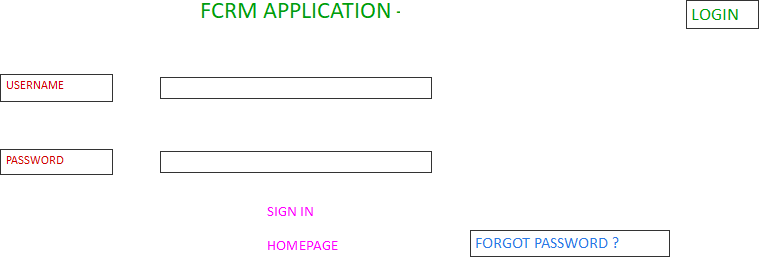
**ANS:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Use Case ID** | **Use Case Name** | **Actor(s)** | **Description** | **Preconditions** | **Postconditions** | **Flow of Events** | **Exceptions** | **Business Rules** |
| UC001 | **Transaction Monitoring** | Compliance Officer, AML Analyst | Monitors transactions for suspicious activities (e.g., structuring, layering, integration) based on pre-defined rules. | User is logged in to the FCRM system and has access to transaction data. | Suspicious activity is flagged for further review. | 1. User selects a transaction range. | False positive due to rule misconfiguration. | 1. Transactions over a threshold (e.g., $10,000) are flagged. |
| 2. System applies AML monitoring rules. | Transaction data missing or incomplete. | 2. Multiple small transactions within a short period are flagged. |
| 3. System flags suspicious transactions. |  |  |
| 4. User reviews flagged transactions. |  |  |
| UC002 | **Suspicious Activity Alert Generation** | AML Analyst, Compliance Officer | Generates alerts for suspicious activities that require investigation (e.g., money laundering or fraud indicators). | Transaction monitoring has been performed. | Alerts are created and prioritized for investigation. | 1. System flags suspicious activity. | Alert priority is incorrectly set. | Alerts are generated based on risk thresholds. |
| 2. Alert is generated and categorized (e.g., high/medium/low risk). | Failure in sending alerts. | High-risk alerts are automatically escalated. |
| 3. User receives the alert and takes action. |  |  |
| UC003 | **Customer Risk Profiling** | Compliance Officer, Risk Analyst | Creates or updates customer risk profiles based on transaction data and external data sources (e.g., PEP, sanctions). | User has customer data available for risk assessment. | Customer risk profile is updated or created. | 1. System collects customer information (e.g., KYC data, sanctions list). | Missing or outdated customer data. | Risk profiling is based on country of origin, transaction volume, and PEP status. |
| 2. System evaluates risk using predefined rules. | Inaccurate risk scoring. |
| 3. Risk score is updated. |  |
| UC004 | **Fraud Detection** | Fraud Analyst, Compliance Officer | Identifies potential fraudulent activities (e.g., account takeovers, credit card fraud, identity theft) based on transactional and behavioural patterns. | Fraud detection models are in place and data is available. | Fraudulent transactions are flagged and require investigation. | 1. System collects transaction data and user activity data. | False positive from an outdated model. | Fraudulent activities can include unusual login times, large transactions, or location anomalies. |
| 2. Machine learning models analyse patterns. | Data mismatch between channels. |
| 3. System flags suspicious behaviour. |  |
| 4. User investigates flagged cases. |  |
| UC005 | **Enhanced Due Diligence (EDD)** | AML Analyst, Compliance Officer | Performs in-depth investigation for high-risk customers flagged during transaction monitoring or customer profiling. | The customer is flagged as high-risk or is a PEP. | Detailed investigation results are recorded and documented. | 1. User reviews flagged customers. | Insufficient customer cooperation. | EDD process involves obtaining more documentation like tax returns, source of funds, or employment history. |
| 2. User requests additional verification (e.g., source of funds). | Inability to verify source of funds. |
| 3. EDD process is completed with full documentation. |  |
| UC007 | **Regulatory Reporting** | Compliance Officer | Generates reports for regulatory bodies (e.g., SAR – Suspicious Activity Reports) based on flagged activities and transactions. | Suspicious activity or high-risk transaction has been detected. | Regulatory report is generated and sent to the appropriate authorities. | 1. User generates a report based on flagged alerts. | Missing data or misreporting. | Reports must comply with local and international AML regulations (e.g., FATF, EU AMLD). |
| 2. System formats the report according to regulatory requirements. | Non-compliance with reporting standards. |
| 3. Report is sent to authorities. |  |
| UC009 | **Case Management and Investigation** | Fraud Analyst, Compliance Officer | Manages and tracks the progress of investigations into flagged transactions or high-risk customers. | Alerts or investigations are triggered and assigned. | Investigation is either closed or escalated based on findings. | 1. User opens a case for investigation. | Incomplete documentation. | Investigation case statuses: open, in progress, escalated, closed. |
| 2. Evidence and documentation are gathered. | Investigation delays. |
| 3. The investigation is completed, and a decision is made (e.g., escalate, close). |  |

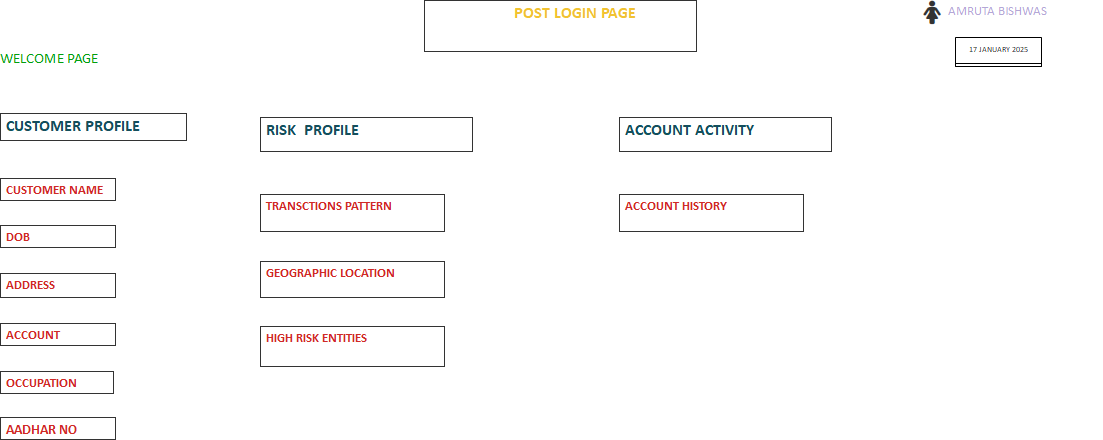
QUE) Document 7- Screens and pages?

**ANS:**

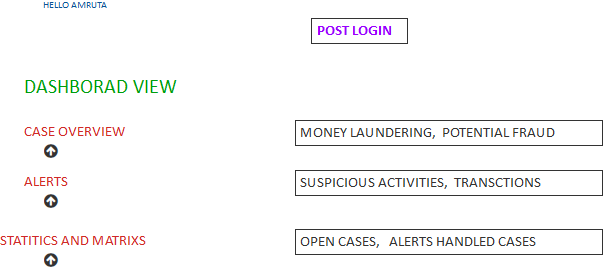
**1)LOGIN PAGE:**



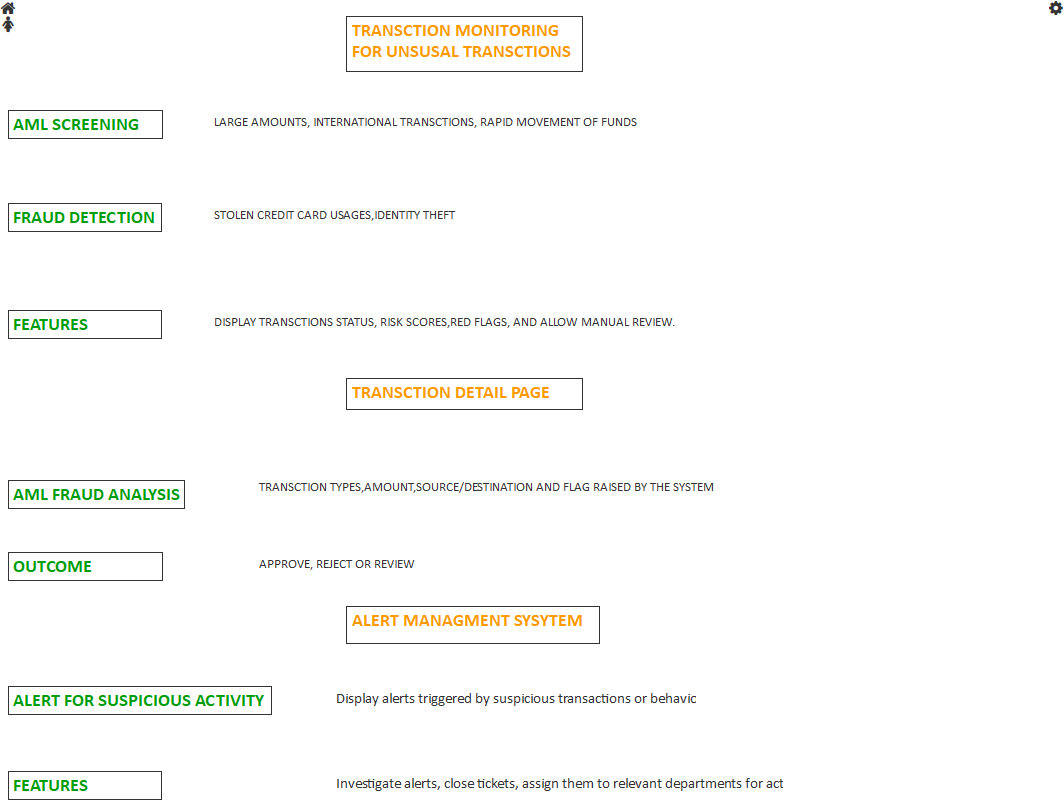
**2)WELCOME PAGE:**



**3)CASE VIEW:**



**4)TRANSCTION MONITORING:**



**5)SAR**



QUE) Document 8- Tools-Visio and Axure?

**ANS:**

In the project focused on enhancing the FCRM application for AML (Anti-Money Laundering) and fraud detection, I utilized both Visio and Axure to effectively contribute to the design and development process. Visio played a crucial role in creating detailed flowcharts, process diagrams, and data models, which helped to visualize complex workflows and system architecture. This was particularly valuable in understanding the interactions between various components of the application, such as user interfaces, databases, and the back-end systems responsible for fraud detection. On the other hand, Axure was used for wireframing and prototyping key interfaces and user experiences. By building interactive prototypes in Axure, I was able to simulate how users would interact with the enhanced system, allowing for user feedback and iteration early in the development process. These tools complemented each other, with Visio providing a strong foundation for technical design and Axure offering a hands-on approach to refining user interfaces and interactions. Together, they helped streamline communication between development teams and stakeholders, ensuring the final solution was both functional and user-friendly.

**QUE) Document 9- BA experience?**

My experience as BA in following phases:

1. Requirement gathering:

2. Requirement Analysis:

3. Design:

4. Development:

5. Testing:

6. Deployment:

**ANS:**

**My Experience as a Business Analyst in the Enhancement of FCRM Application for AML and Fraud Detection**

**1. Project Overview**

* **Project Objective:** The goal of this project was to enhance an existing FCRM application to improve the efficiency and accuracy of AML and fraud detection processes.
* **Key Stakeholders:** Risk Management Teams, Compliance Officers, IT Department, Business Operations, Regulatory Authorities.
* **Timeline:** [18MONTH]
* **Tools and Technologies:** FCRM application, MS VISIO, AUTURE].

**2. Initiation Phase: Requirement Gathering**

* **Stakeholder Interviews:** I Conducted detailed discussions with key stakeholders, including Compliance Officers, Risk Managers, and IT teams, to understand the current system’s challenges and requirements.
* **As-Is Analysis:** Analysed the current AML and fraud detection processes to identify inefficiencies and areas for improvement.
* **Business Requirements Documentation (BRD):** Compiled business requirements into a structured BRD document, which outlined the functional and non-functional requirements for the enhancement of the FCRM application.
* **Gap Analysis:** Conducted a gap analysis between the existing FCRM capabilities and the desired state based on the latest regulatory guidelines and industry best practices.

**3. Design Phase: Solution Development**

* **Functional Specifications:** Collaborated with technical teams to create functional specifications that detailed how the FCRM system should handle AML alerts, fraud detection workflows, and reporting functionalities.
* **Use Cases and User Stories:** Defined detailed use cases and user stories to describe how end users (Compliance Officers, Investigators) would interact with the enhanced system. This was key in ensuring user-centric design.
* **Data Flow Mapping:** Worked with data architects to map out data flows for AML transaction monitoring, alert generation, and escalation processes.
* **UI/UX Consultation:** Provided input into the user interface design, ensuring that the application would be intuitive and user-friendly for non-technical stakeholders.
* **Compliance and Regulatory Mapping:** Ensured that the design complied with the relevant regulatory frameworks such as FATF recommendations, local anti-money laundering laws, and fraud detection standards.

**4. Implementation Phase: Development Support**

* **Collaboration with Development Teams:** Worked closely with developers to ensure that the features being built met the requirements. This included validating design documents, discussing technical constraints, and adjusting as needed.
* **Test Case Preparation:** Assisted in preparing test cases to ensure that all AML and fraud detection features functioned correctly and adhered to regulatory requirements.
* **UAT (User Acceptance Testing):** Coordinated UAT with business users, ensuring that the new functionalities met business needs. Addressed any issues or concerns raised during testing.
* **Change Management:** Managed any changes or adjustments to the original requirements, ensuring that all changes were documented, approved, and communicated.

**5. Go-Live and Post-Implementation Support**

* **Go-Live Support:** Provided support during the deployment of the enhanced system, ensuring smooth transition and no disruption in daily operations.
* **Training & Documentation:** Developed user manuals and conducted training sessions for end-users to help them understand how to utilize the new features effectively.
* **Feedback Collection:** Collected feedback from users’ post-implementation to assess the effectiveness of the enhancements and identify any further optimization opportunities.
* **Post-Implementation Review:** Conducted a post-implementation review to evaluate project success and document lessons learned.

**6. Continuous Improvement and Monitoring**

* **Ongoing Collaboration:** Continued to work with the Risk and Compliance teams to monitor the system’s performance and make necessary adjustments based on new threats, regulatory changes, or system inefficiencies.
* **Data Analytics:** Assisted in setting up regular monitoring and reporting of suspicious activities detected by the system to ensure that the business was compliant and proactive in fraud prevention.
* **Regulatory Changes:** Ensured that any future regulatory changes were incorporated into the system by continuously liaising with legal and compliance departments.

**7. Tools and Techniques Used**

* **Business Analysis Tools:** JIRA, Confluence, Visio (for process mapping), Microsoft Excel (for data analysis), [other tools].
* **Techniques Applied:** Stakeholder analysis, process mapping, root cause analysis, SWOT analysis, and data analysis.

**Conclusion**

Through my role as a Business Analyst in the FCRM application enhancement for AML and fraud detection, I was able to contribute to the delivery of a solution that significantly improved the system’s efficiency and compliance with regulatory standards. My involvement in all phases of the project—from requirement gathering to post-implementation support—ensured that the product aligned with the business needs and provided a valuable tool for detecting financial crime.