**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:**

**1. Use Case Name:**

**AI-Enhanced AML & Fraud Investigation in FCRM**

**2. Use Case Description:**

The use case aims to enhance the functionality of the Fraud and Customer Risk Management (FCRM) system by integrating AI-driven tools to detect and investigate potential fraud and money laundering activities. The AI will analyse customer transactions, identify patterns of suspicious activity, and assist investigators in prioritizing cases for further review and action.

**3. Actors:**

* **Primary Actors**:
  + **FCRM System**: The core platform which processes and monitors transactions.
  + **AI Engine**: An AI tool that analyses transaction data to detect suspicious activities and provides recommendations for fraud or AML investigation.
  + **AML Investigator**: A person who investigates flagged cases and decides on further actions.
  + **Compliance Officer**: An individual responsible for ensuring the organization adheres to regulatory standards and takes necessary actions based on AML or fraud findings.
* **Secondary Actors**:
  + **External Financial Institutions/Partners**: May be consulted for cross-border transaction investigations or suspicious account links.
  + **Regulatory Authorities**: Government bodies or regulators that require reports and may conduct audits.

**4. Basic Flow:**

1. **Transaction Data Collection**: The FCRM system collects transaction data from various channels (e.g., banking systems, payment platforms, etc.).
2. **AI Processing**: The AI engine processes the collected data and identifies patterns associated with fraud and money laundering risks using machine learning algorithms.
3. **Flag Suspicious Transactions**: AI flags transactions based on predefined criteria (e.g., unusual patterns, large volume, geographic anomalies).
4. **Investigator Review**: AML investigators are notified of the flagged transactions for further analysis.
5. **Case Creation**: Investigators review transaction histories and create cases for suspicious activities.
6. **Investigation Actions**: AML investigators request additional data or transaction history, liaise with compliance officers, or contact external financial institutions as needed.
7. **Report to Regulatory Authorities**: If necessary, a report is generated for regulatory authorities or law enforcement based on investigation outcomes.
8. **Case Resolution**: Investigators decide on a course of action (e.g., closure, alert, or further investigation) and document the findings.

**5. Alternate Flow:**

* If the AI engine is unable to flag any suspicious activities, the system will continue to monitor and analyse transactions.
* If the investigator requires more information from the external institution, the system generates an automatic request for additional data.
* If the AI identifies a high-risk fraud pattern, an immediate alert is sent to the investigator for swift action, prioritizing cases based on risk level.

**6. Exceptional Flows:**

* **AI Model Error**: In case of an AI model failure (e.g., insufficient training data, or an unexpected error), a backup manual monitoring system will temporarily take over until the issue is resolved.
* **Data Inaccuracy**: If there is inaccurate or missing transaction data, the FCRM system will notify the investigator to verify the data before proceeding with investigation.

**7. Pre-Conditions:**

* The FCRM system is active and processing transaction data.
* AI engine has been trained with historical fraud and AML data.
* Investigator access rights to the system and transaction data are validated.
* Regulatory frameworks and criteria for fraud detection are defined.

**8. Post-Conditions:**

* Investigators either close or escalate cases based on AI-generated insights.
* Accurate reports and logs are generated for future audits and compliance checks.
* Suspicious activities are either cleared or flagged for legal or regulatory follow-up.

**9. Assumptions:**

* The AI system is well-trained with adequate historical data and updated periodically for new fraud or money laundering tactics.
* The investigator is trained to interpret AI-generated alerts and perform appropriate follow-up actions.
* There is sufficient collaboration with external institutions when required.

**10. Constraints:**

* The AI system may have false positives or negatives, requiring human verification.
* Limited data access or system downtime could delay investigations.
* Real-time detection might not be feasible due to resource limitations or data processing speed.

**11. Dependencies:**

* **External Data Sources**: Financial institutions or partner organizations that provide transactional data.
* **Compliance Regulations**: The FCRM system and AI must comply with local and international AML and fraud detection regulations.
* **AI Model Training**: The quality and effectiveness of fraud and AML detection are dependent on continuous AI model training with up-to-date transaction and fraud data.

**12. Inputs and Outputs:**

* **Inputs**:
  + Transaction data (from banks, payment platforms, etc.).
  + Customer profile data (account history, geographical information).
  + Historical fraud and AML data for AI training.
* **Outputs**:
  + Flagged transactions for investigator review.
  + Suspicious activity reports.
  + Alerts to investigators or compliance officers.
  + Generated reports for regulatory bodies.

**13. Business Rules:**

* The AI system will flag transactions based on pre-configured rules, such as:
  + Transactions above a certain value threshold.
  + Rapid movement of funds between different accounts, particularly across borders.
  + High-risk geographic regions associated with fraud.
  + Patterns matching known money laundering or fraud tactics.
* Investigators must prioritize flagged transactions based on risk level and adhere to a resolution timeline.
* Regulatory reporting thresholds must be met as required by local financial authorities.

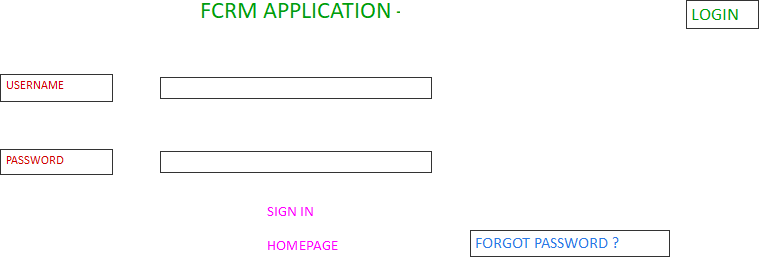
**14. Miscellaneous Information:**

* The integration of AI into FCRM is expected to improve the speed and accuracy of fraud detection, reducing false positives and identifying new fraud schemes.
* Ongoing updates and enhancements to AI models are essential to keep up with evolving fraud and money laundering methods.
* The system must comply with data privacy laws such as GDPR or CCPA when handling customer information.

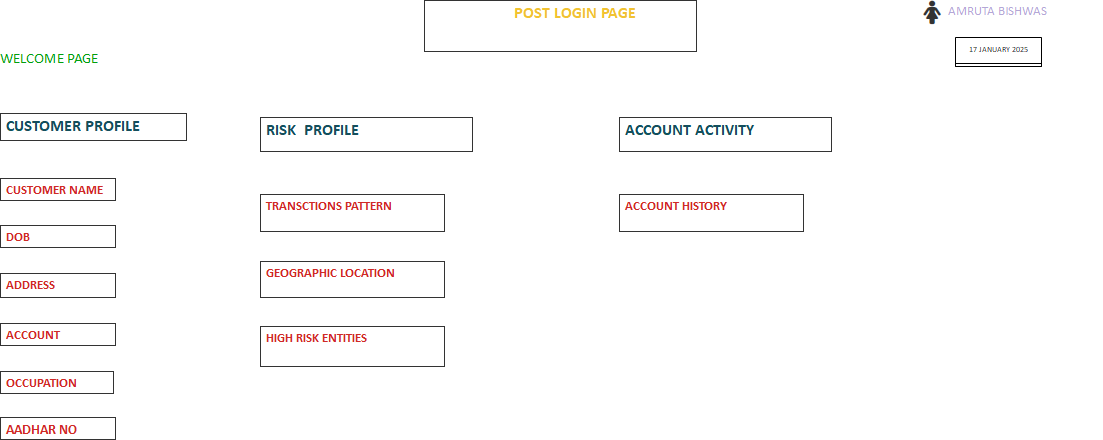
QUE) Document 7- Screens and pages?

**ANS:**

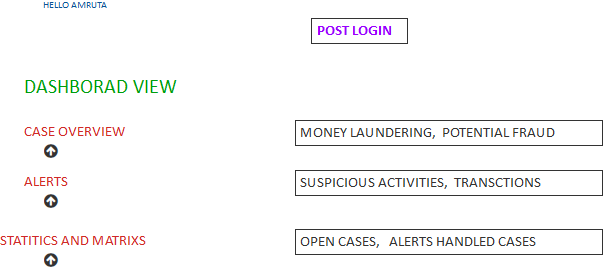
**1)LOGIN PAGE:**



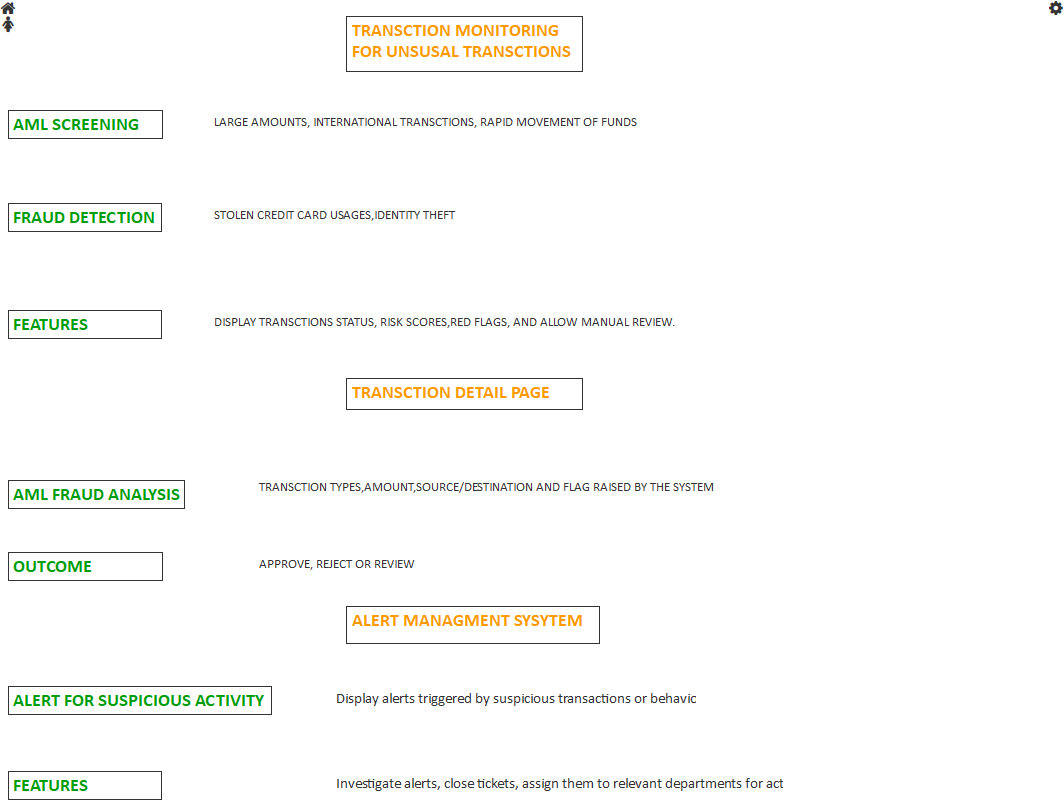
**2)WELCOME PAGE:**



**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:** [Insert timeline]
* **Tools and Technologies:** FCRM application, [insert relevant technologies], [other tools used].

**2. Initiation Phase: Requirement Gathering**

* **Stakeholder Interviews:** 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:** Analyzed 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 making adjustments 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 end product aligned with the business needs and provided a valuable tool for detecting financial crime.