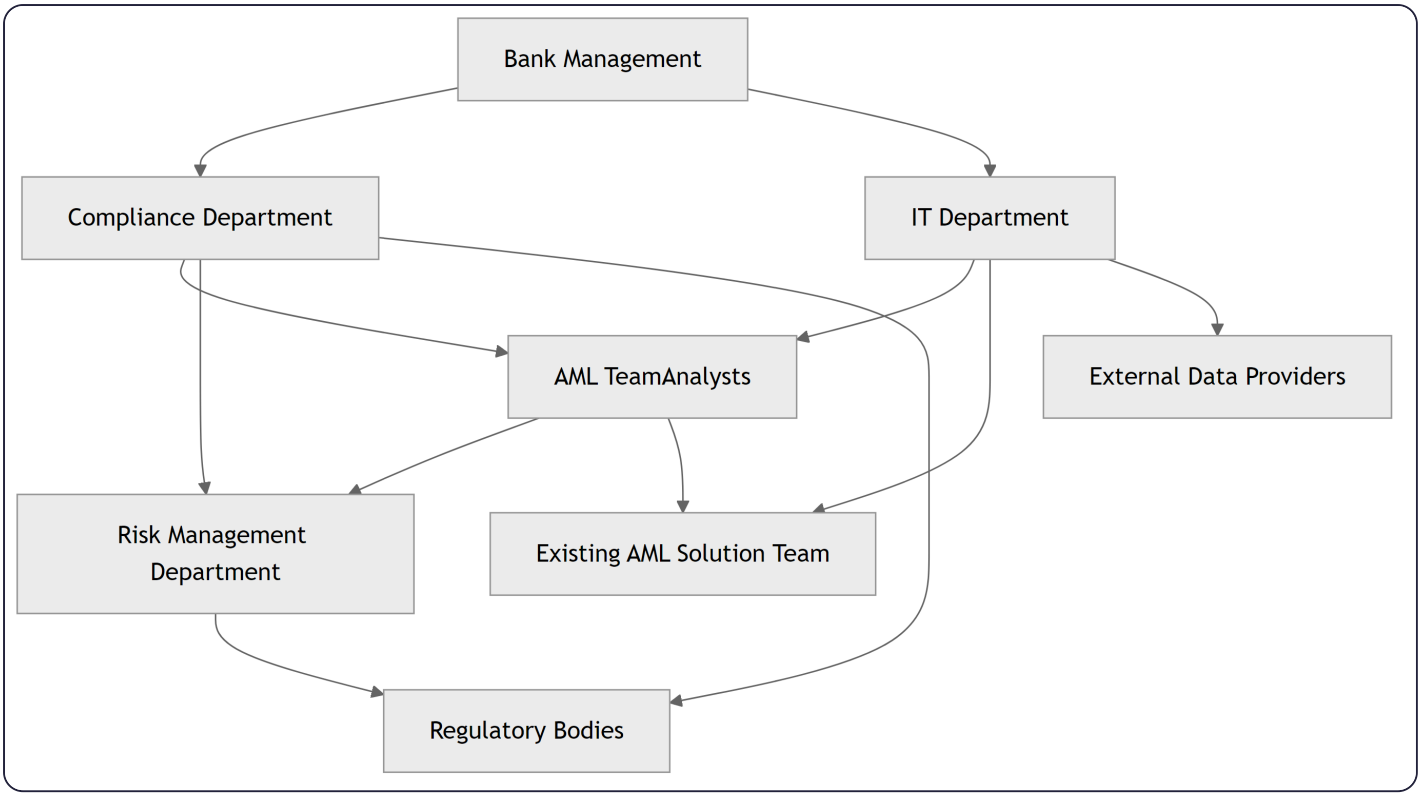
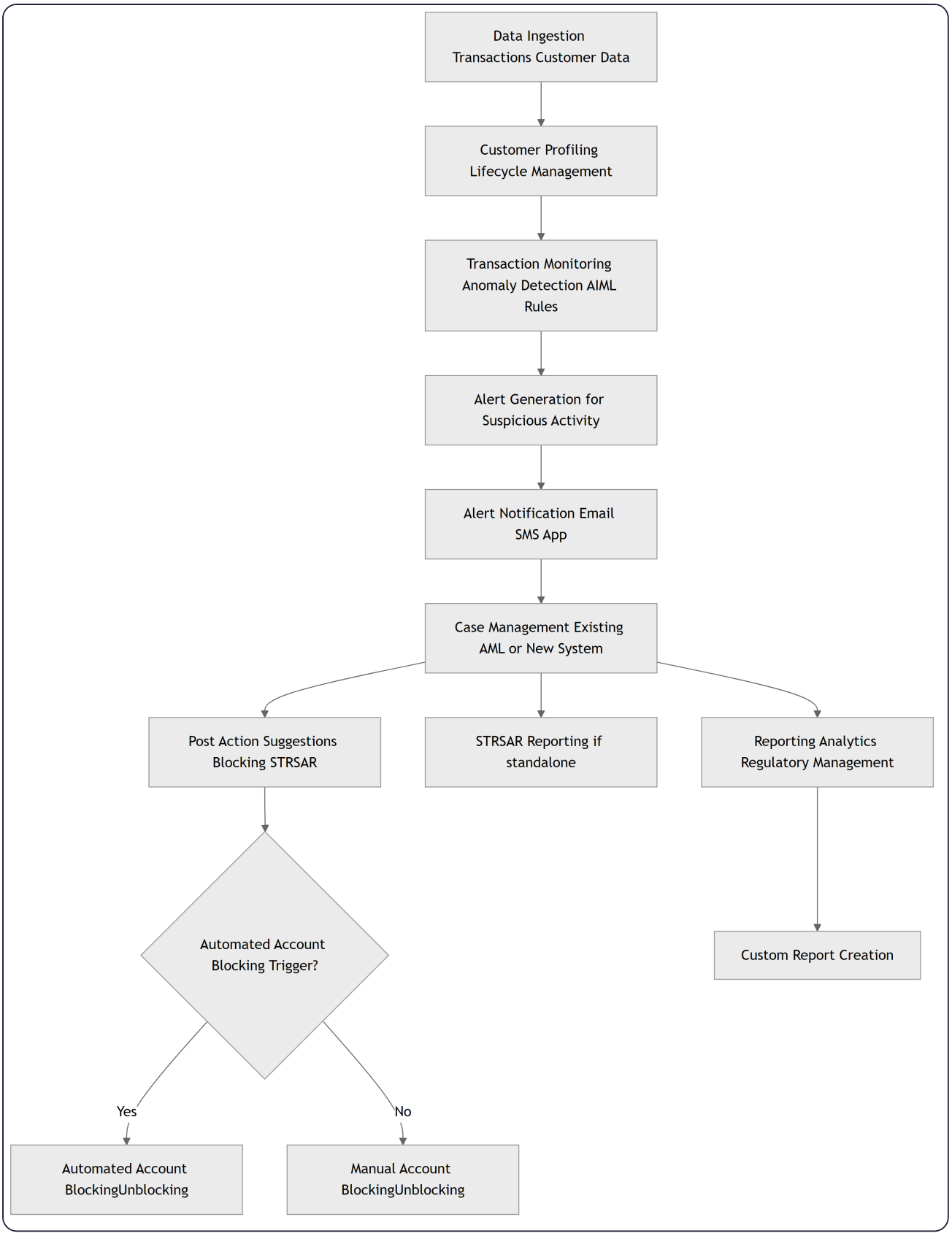
# 01. Stakeholder Map

This diagram illustrates the key stakeholders involved in the AI/ML-based AML Compliance project and their primary relationships.




# 02. Process Flow

This process flow outlines the high-level operational journey within the new AI/ML-based AML Compliance system.




# 03. Business Requirement Document (BRD)

## 3.1. Introduction and Purpose

This document outlines the business requirements for the design, development, and implementation of a comprehensive software solution to automate and streamline AI/ML-based Anti-Money Laundering (AML)

Compliance. The primary objective is to enhance the bank's ability to detect, prevent, and report suspicious financial activities, thereby mitigating financial losses and ensuring adherence to regulatory requirements. The system will primarily focus on leveraging customer profiling, transaction monitoring, related post-action (case management), and reporting functionalities, with provisions for future enhancements.

## 3.2. Project Objectives

The project aims to achieve the following key objectives:

1. **Enhanced AML and Anomaly Detection**: Significantly reduce false positives and identify suspicious transactions with higher accuracy using AI/ML algorithms.
2. **Real-time Monitoring**: Continuously monitor transactions and customer behavior for anomalies in real-time.
3. **Improved Efficiency**: Automate manual tasks associated with transaction monitoring and investigations, leading to operational cost savings and faster response times.
4. **Regulatory Compliance**: Ensure strict adherence to all relevant AML regulations, risk prevention guidelines, and data privacy standards.
5. **Comprehensive MIS & Reporting**: Provide all types of regulatory and management reports to support compliance, auditing, and strategic decision-making.

## 3.3. Business Needs

The proposed system must address the following critical business needs:

- Ability to analyze transactional data, customer behaviors, and patterns effectively.
- Accurate identification of anomalies and potential threats.
- Streamlined case management processes.
- Timely notification of relevant teams for intervention.
- Reduced risk of financial losses due to money laundering and fraudulent activities.
- Capability to adapt to evolving threats and regulatory changes.

## 3.4. High-Level Scope

The project's high-level scope encompasses the following major areas:

- **Customer Profiling & Lifecycle Management**: Develop dynamic customer profiles based on various attributes (profession, income, location, transaction patterns) and manage their lifecycle, including periodic reviews and AI-based suggestions for updates.
- **Data Collection and Analysis**: Integrate and collect data from diverse internal sources (transaction records, customer behaviors) and external sources (Blacklist, AML screening lists, PEP lists), ensuring data reliability and availability for machine learning.
- **Transaction Monitoring & Anomaly Detection**: Implement advanced AI/ML algorithms to detect atypical transaction patterns, suspicious behaviors, and automatically generate rules. This includes custom rule configuration, dynamic detection scenarios, and false positive mitigation.
- **Post Action and Case Management**: Develop capabilities for automated and manual account blocking/unblocking, post-action suggestions (e.g., communication, blacklisting), and manual case creation. The system will integrate with the bank's existing AML solution for alert management, or provide its own case management if integration is not feasible.
- **Reporting and Analytics**: Generate comprehensive regulatory and management reports, including a custom report creation feature allowing users to define new report requirements and criteria.

# 04. Functional Requirement Specification (FRS)

## 4.1. Functional Requirements

The system shall provide the following functional capabilities:

- **FR1: Customer Profiling & KYC Management**:
    - **FR1.1**: The system shall create and maintain customer profiles based on attributes such as profession, income, location, and transaction patterns.
    - **FR1.2**: The system shall support incident and trigger event-based reviews, incorporating historical data, prior involvement, and case accumulation.
    - **FR1.3**: The system shall facilitate periodic customer reviews and provide AI-based suggestions for profile updates.
    - **FR1.4**: The system shall allow for system-initiated updates to customer profiles based on detected changes in behavior or data.

- **FR2: Data Collection and Analysis**:
    - **FR2.1**: The system shall gather and integrate data from multiple internal sources (e.g., transaction records, core banking, CRM).
    - **FR2.2**: The system shall integrate with external data sources for AML screening, including Blacklists, Sanction Lists, and PEP lists.

- **FR3: Transaction Monitoring & Anomaly Detection**:
    - **FR3.1**: The system shall deploy AI and ML algorithms to identify atypical transaction patterns and suspicious behavior.
    - **FR3.2**: The system shall allow for the setting and periodic review/update of transaction limits for customers/accounts.
    - **FR3.3**: The system shall enable bank users to configure custom rules and constraints based on internal policies and monitoring needs, including:
        - Dynamic Detection Scenarios.
        - Dynamic Rule Setting.
        - Rule-based Detection Scenarios and Alert Generation.
        - System-based Case Generation.
        - False Positive Case Mitigation.
    - **FR3.4**: The system shall automatically generate new rules based on predefined patterns and AI-detected suspicious customer activity.
    - **FR3.5**: The system shall continuously adapt and improve its detection capabilities by learning from historical data, customer behavior, and ongoing monitoring results (for both AI and rule-based monitoring).
    - **FR3.6**: The system shall provide timely alerts and notifications through multiple channels (Email, SMS, App) for detected anomalies.

- **FR4: Post Action and Case Management**:
    - **FR4.1**: The system shall generate sensitivity and post-action suggestions based on detected anomalies.
    - **FR4.2**: The system shall support automated account blocking and unblocking based on predefined rules.
    - **FR4.3**: The system shall support manual account blocking and unblocking by authorized users.
    - **FR4.4**: The system shall manage customer communication related to alerts and account actions.
    - **FR4.5**: The system shall enable manual case creation by users.
    - **FR4.6**: The system shall have the capability for STR/SAR reporting, if integration with the bank's existing AML solution for case management is not feasible.
    - **FR4.7**: The system shall support post-action based blacklisting of accounts or individuals.

- **FR5: Reporting and Analytics**:
    - **FR5.1**: The system shall generate various regulatory reports as required by authorities.
    - **FR5.2**: The system shall generate management reports on detected anomalies, fraud patterns, and system performance.

    - **FR5.3**: The system shall include a custom report creation feature, allowing users to define new report templates, specify data sources, and set parameters.

## 4.2. Non-Functional Requirements (NFRs)

- **NFR1: Performance**:
    - **NFR1.1**: The system shall process transaction data and detect anomalies in near real-time, with alert generation within 5 seconds of transaction completion.
    - **NFR1.2**: The system shall be capable of handling an average daily transaction volume of [X] and peak volume of [Y] without degradation in performance.
    - **NFR1.3**: AI/ML model retraining cycles shall complete within [Z] hours.

- **NFR2: Scalability**:
    - **NFR2.1**: The system shall be scalable to accommodate future growth in transaction volumes, customer base, and data sources.
    - **NFR2.2**: The system architecture shall support horizontal scaling of its components.

- **NFR3: Security**:
    - **NFR3.1**: The system shall enforce role-based access control (RBAC) to ensure that users can only access data and functionalities relevant to their roles.
    - **NFR3.2**: All sensitive data (PII, financial data) at rest and in transit shall be encrypted.
    - **NFR3.3**: The system shall log all user actions and system events for audit purposes.
    - **NFR3.4**: The system shall be protected against common web application vulnerabilities (e.g., OWASP Top 10).

- **NFR4: Reliability and Availability**:
    - **NFR4.1**: The system shall have an uptime of at least 99.9% during business hours.
    - **NFR4.2**: The system shall have robust error handling and recovery mechanisms to ensure data integrity.

- **NFR5: Usability**:
    - **NFR5.1**: The user interface shall be intuitive and easy to navigate for Compliance Analysts and Officers.
    - **NFR5.2**: The rule configuration and custom report creation interfaces shall be user-friendly, requiring minimal technical expertise.

- **NFR6: Maintainability**:
    - **NFR6.1**: The system shall be designed with a modular architecture to facilitate future enhancements, bug fixes, and updates.
    - **NFR6.2**: Comprehensive documentation (technical and user manuals) shall be provided.

- **NFR7: Integration**:
    - **NFR7.1**: The system shall seamlessly integrate with the bank's core banking system, existing AML solution (if applicable), and CRM.
    - **NFR7.2**: The system shall support standard API interfaces for data exchange with internal and external systems.

- **NFR8: Compliance**:
    - **NFR8.1**: The system shall adhere to all relevant local and international AML/CFT regulations (e.g., FATF guidelines, local banking laws).
    - **NFR8.2**: The system shall comply with data privacy regulations (e.g., GDPR, local data protection acts) for handling customer PII.

- **NFR9: Accuracy**:
    - **NFR9.1**: The AI/ML models shall achieve an anomaly detection accuracy rate of at least [X]% with a false positive rate not exceeding [Y]%.

- **NFR9.2**: The system shall provide mechanisms for continuous feedback loop to improve model accuracy and reduce false positives.

# 05. Use Case Diagrams and Detailed Scenarios

## 5.1. Use Case 1: System Detects Unusual Transaction

**Description**: This use case describes how the AML system automatically detects an unusual transaction pattern or anomaly and generates an alert.

```
usecaseDiagram
    actor "AML System" as AMS
    actor "AI/ML Engine" as AIME
    actor "Transaction Monitoring Module" as TMM
    actor "Alert Notification Module" as ANM
    actor "Case Management System" as CMS

    AMS --> TMM
    TMM --> AIME
    AIME --> D[Detect Unusual Transaction]
    D --> E[Generate Alert]
    E --> ANM
    ANM --> F[Notify Relevant Teams]
    F --> CMS
```

**Scenario: System Detects Unusual Transaction**

**Pre-conditions**: * Transactional data is flowing into the AML system. * AI/ML models are trained and active. * Custom rules (if any) are configured and enabled.

**Main Flow**: 1. **System Receives Transaction Data**: The Transaction Monitoring Module (TMM) receives real-time transaction data from source systems. 2. **AI/ML Analysis**: The TMM feeds the transaction data to the AI/ML Engine (AIME) and evaluates against configured rules. 3. **Anomaly Detection**: The AIME identifies an unusual transaction pattern (e.g., Off-time Transaction, Unusual Volume Transaction Detection, Mule Account identification) that deviates significantly from the customer's established profile or predefined rules. 4. **Anomaly Confirmation**: The AIME confirms the anomaly based on its detection algorithms and thresholds. 5. **Alert Generation**: The TMM generates a high-priority alert for the detected unusual transaction. 6. **Alert Notification**: The Alert Notification Module (ANM) sends immediate notifications (Email, SMS, App) to the relevant AML Team/Analysts. 7. **Alert Parking in Case Management**: The alert is automatically routed and parked in the existing Case Management System (CMS) or the new system's case management module, depending on integration feasibility.

**Post-conditions**: * An alert for the suspicious transaction is generated and recorded. * Relevant AML personnel are notified. * The transaction is available for further investigation in the Case Management System.

## 5.2. Use Case 2: Compliance Analyst Configures Custom Rule

**Description**: This use case details how a Compliance Analyst defines and activates new custom rules for transaction monitoring.

```
usecaseDiagram
    actor "Compliance Analyst" as CA
```

```
    actor "Rule Configuration Module" as RCM
    actor "Rule Engine" as RE
    actor "System Audit Log" as SAL

    CA --> A[Access Rule Configuration]
    A --> B[Define New Rule Criteria]
    B --> C[Set Thresholds and Conditions]
    C --> D[Test Rule against Historical Data]
    D --> E[Validate Rule Effectiveness]
    E --> F[Activate Rule]
    F --> RE
    RE --> G[Apply Rule for Monitoring]
    G --> SAL
```

**Scenario: Compliance Analyst Configures Custom Rule**

**Pre-conditions**: * Compliance Analyst has appropriate permissions to access the Rule Configuration Module. * The system's Rule Configuration Module is accessible.

**Main Flow**: 1. **Access Rule Configuration**: The Compliance Analyst logs into the AML system and navigates to the Rule Configuration Module (RCM). 2. **Initiate New Rule Creation**: The Analyst selects the option to create a new custom rule. 3. **Define Rule Criteria**: The Analyst defines the specific criteria for the new rule (e.g., "Unusual Transaction with Small Amount in Similar Account", "One to Many and Many to One"). This includes selecting relevant data fields, operators, and values. 4. **Set Thresholds and Conditions**: The Analyst sets thresholds, frequency conditions, or other parameters relevant to the rule. 5. **Test Rule against Historical Data**: The RCM allows the Analyst to test the newly defined rule against historical transaction data to assess its potential impact (e.g., number of historical alerts it would have generated, false positive rate estimation). 6. **Validate Rule Effectiveness**: Based on test results, the Analyst fine-tunes the rule for optimal effectiveness and minimizes false positives. 7. **Activate Rule**: Once satisfied, the Analyst confirms and activates the new rule. 8. **Rule Applied**: The Rule Engine (RE) incorporates the new rule into the active monitoring processes. 9. **Audit Log**: The system records the rule creation and activation details in the System Audit Log (SAL).

**Post-conditions**: * A new custom rule is active in the system. * The system begins monitoring transactions against the new rule. * Changes are recorded for audit purposes.

## 5.3. Use Case 3: System Automatically Generates Rule

**Description**: This use case describes how the AI/ML Engine identifies recurring suspicious patterns and automatically generates and implements new monitoring rules.

```
usecaseDiagram
    actor "AML System" as AMS
    actor "AI/ML Engine" as AIME
    actor "Pattern Analysis Module" as PAM
    actor "Rule Generation Module" as RGM
    actor "Rule Engine" as RE
    actor "System Audit Log" as SAL

    AMS --> AIME
    AIME --> PAM
    PAM --> B[Identify Recurring Suspicious Pattern]
    B --> C[Propose New Rule Parameters]
    C --> RGM
    RGM --> D[Validate Proposed Rule]
    D --> E[Automatically Activate Rule]
    E --> RE
```

```
    RE --> F[Apply New Rule for Monitoring]
    F --> SAL
```

**Scenario: System Automatically Generates Rule**

**Pre-conditions**: * The AML system is continuously collecting and analyzing transaction and customer behavior data. * The AI/ML Engine is enabled for automatic rule generation.

**Main Flow**: 1. **Continuous Data Analysis**: The AI/ML Engine (AIME) continuously analyzes large volumes of historical and real-time transaction data and customer behavior patterns. 2. **Pattern Identification**: The Pattern Analysis Module (PAM) within the AIME identifies a recurring pattern of suspicious behavior across a customer base (e.g., high-value transactions to high-risk countries from various seemingly unrelated accounts). 3. **Rule Parameter Proposal**: Based on the identified pattern, the AIME proposes parameters for a new rule, including conditions, thresholds, and associated risk scores. 4. **Rule Generation**: The Rule Generation Module (RGM) receives the proposed parameters and constructs a formal rule definition. 5. **Rule Validation**: The RGM performs an automated validation of the proposed rule, potentially testing it against historical data to estimate its impact and ensure it doesn't cause excessive false positives. 6. **Automatic Rule Activation**: If the rule passes validation and meets predefined criteria for auto-activation, the system automatically activates the new rule. 7. **Rule Applied**: The Rule Engine (RE) immediately incorporates the new rule into its active monitoring processes. 8. **Audit Log**: The system logs the automatic rule generation and activation details in the System Audit Log (SAL).

**Post-conditions**: * A new, system-generated rule is active and monitoring transactions. * The system's detection capabilities are dynamically adapted to emerging risks. * The rule creation event is auditable.

## 5.4. Use Case 4: Compliance Officer Generates Regulatory Report

**Description**: This use case describes how a Compliance Officer generates various regulatory and management reports, including custom reports.

```
usecaseDiagram
    actor "Compliance Officer" as CO
    actor "Reporting Module" as RM
    actor "Data Warehouse" as DW
    actor "Report Generation Engine" as RGE

    CO --> A[Access Reporting Module]
    A --> B{Select Report Type or Custom Report}
    B -- Select Standard Report --> C[Define Report Parameters]
    B -- Create Custom Report --> D[Define Custom Report Templates]
    D --> E[Specify Data Sources and Criteria]
    E --> C
    C --> RGE
    RGE --> F[Retrieve Data from Data Warehouse]
    F --> G[Generate Report]
    G --> H[Preview Report]
    H --> I[Export/Submit Report]
```

**Scenario: Compliance Officer Generates Regulatory Report**

**Pre-conditions**: * Compliance Officer has appropriate permissions to access the Reporting Module. * Required data for reporting is available in the Data Warehouse.

**Main Flow**: 1. **Access Reporting Module**: The Compliance Officer (CO) logs into the AML system and navigates to the Reporting Module (RM). 2. **Select Report Type**: The CO chooses to generate either a standard regulatory report (e.g., STR/SAR, volume reports) or selects the "Custom Report Creation" option. 3. **Define Custom Report (if applicable)**: If creating a custom report, the CO defines a new report template

through an intuitive interface, specifying desired data elements, filters, and aggregation criteria. This involves selecting data sources and setting parameters. 4. **Define Report Parameters (for any report type)**: The CO specifies the parameters for the chosen report, such as date ranges, customer segments, or specific anomaly types. 5. **Data Retrieval**: The Report Generation Engine (RGE) retrieves the necessary data from the Data Warehouse (DW) based on the specified criteria. 6. **Generate Report**: The RGE processes the data and generates the report in the requested format. 7. **Preview Report**: The CO previews the generated report to ensure accuracy and completeness. 8. **Export/Submit Report**: The CO exports the report in a suitable format (e.g., PDF, Excel) or submits it directly to the relevant regulatory body (if integrated functionality exists).

**Post-conditions**: * The required regulatory or management report is successfully generated. * The report is available for review, export, or submission. * A new custom report template (if created) is saved for future use.

## 5.5. Use Case 5: System Initiates Account Blocking

**Description**: This use case describes how the AML system, based on confirmed high-risk anomalies or pre-defined rules, automatically triggers an account blocking action.

```
usecaseDiagram
    actor "AML System" as AMS
    actor "Case Management Module" as CMM
    actor "Post Action Suggestion Engine" as PASE
    actor "Account Blocking Module" as ABM
    actor "Core Banking System" as CBS
    actor "System Audit Log" as SAL

    AMS --> CMM
    CMM --> PASE
    PASE --> A[Confirm High Risk/Policy Violation]
    A --> B[Generate Account Blocking Suggestion]
    B --> C[Validate Auto-Blocking Rule]
    C --> ABM
    ABM --> D[Trigger Account Blocking API]
    D --> CBS
    CBS --> E[Confirm Account Blocked]
    E --> SAL
```

**Scenario: System Initiates Account Blocking**

**Pre-conditions**: * An anomaly has been detected and escalated to the Case Management Module (CMM). * The anomaly is confirmed as high-risk or a clear violation of a policy requiring immediate action. * Automated blocking rules are configured in the system. * Integration with the Core Banking System (CBS) for account actions is established.

**Main Flow**: 1. **High-Risk Confirmation**: Within the CMM, an alert or case is confirmed as high-risk, warranting immediate account action, or a pre-defined rule dictates automatic blocking based on the detected anomaly (e.g., mule account identification, rapid unjustifiable changes in activity). 2. **Post Action Suggestion**: The Post Action Suggestion Engine (PASE) generates a suggestion for account blocking based on the risk assessment and configured policies. 3. **Automated Blocking Rule Validation**: The Account Blocking Module (ABM) validates if the conditions for automated account blocking are met as per the pre-defined system rules. 4. **Trigger Account Blocking API**: If conditions are met, the ABM triggers the account blocking API call to the Core Banking System (CBS). 5. **Account Blocking in CBS**: The CBS receives the request and performs the necessary actions to block the specified account. 6. **Confirmation of Blocking**: The CBS sends a confirmation back to the AML system that the account has been successfully blocked. 7. **Action Logging**: The AML system records the automated account blocking action, including timestamps and reasons, in the System Audit Log (SAL).

**Post-conditions**: * The suspicious account is blocked in the Core Banking System. * The blocking action is logged within the AML system for audit and case management. * Further transactions on the blocked account are prevented.

# 06. Data Mapping Sheet and Data Requirements Analysis

This section outlines the key data elements required for the AI/ML AML Compliance solution, their sources, characteristics, and purpose.

| Data Element | Source System(s) | Data Type | Frequency/Freshness | Purpose for Personalization | Availability (Y/N) | PII/Sensitivity | Data Owner | Transformation/Processing | Remarks/Privacy Concerns |
|---|---|---|---|---|---|---|---|---|---|
| Customer ID | Core Banking, CRM | Alphanumeric | Real-time | Core identifier for all customer-related data. | Y | PII | Operations | Masking for non-AML access. | Essential for linking all customer data; strict access control. |
| Customer Name | Core Banking, CRM | String | Daily | Identification for case management and reporting. | Y | PII | Operations | Name standardization (e.g., case conversion). | Sensitive PII; requires secure handling. |
| Customer Profession | CRM, KYC Forms | String | On-demand/Event | Profiling for expected transaction patterns, risk assessment. | Y | PII | Compliance, Operations | Categorization into standardized professions. | Part of KYC data; useful for profiling. |
| Customer Income | CRM, KYC Forms | Numeric | On-demand/Event | Profiling for expected transaction volumes | Y | PII | Compliance, Operations | Income range categorization. | Sensitive PII; direct financial impact on profiling. |

| Data Element | Source System(s) | Data Type | Frequency/Freshness | Purpose for Personalization | Availability (Y/N) | PII/Sensitivity | Data Owner | Transformation/Processing | Remarks/Privacy Concerns |
|---|---|---|---|---|---|---|---|---|---|
| | | | | and values. | | | | | |
| Customer Location (Address) | CRM, Core Banking, KYC Forms | String | On-demand/Event | Geographic risk assessment, profiling. | Y | PII | Operations | Geocoding/Standardization for location-based analysis. | PII; used for geographic risk (e.g., sanctioned countries). |
| Transaction ID | Transaction Processing System | Alphanumeric | Real-time | Unique identifier for each transaction, audit trail. | Y | Public | IT Operations | None (Direct mapping). | Key for linking alerts to specific transactions. |
| Transaction Date/Time | Transaction Processing System | Datetime | Real-time | Time-based anomaly detection (e.g., off-time). | Y | Public | IT Operations | Timezone standardization. | Crucial for real-time monitoring and historical analysis. |
| Transaction Type | Transaction Processing System | String | Real-time | Rule configuration (e.g., cash deposit, wire transfer). | Y | Public | IT Operations | Categorization into predefined types. | Essential for rule-based detection scenarios. |
| Transaction Amount | Transaction Processing System | Numeric | Real-time | Volume-based anomaly detection, threshold violations. | Y | Public | IT Operations | Currency conversion, aggregation. | Central to financial crime detection. |
| Sender Account | Transaction | Alphanumeri | Real-time | Identification of | Y | PII (indire | IT Operati | Linking to | Essential for |

| Data Element | Source System(s) | Data Type | Frequency/Freshness | Purpose for Personalization | Availability (Y/N) | PII/Sensitivity | Data Owner | Transformation/Processing | Remarks/Privacy Concerns |
|---|---|---|---|---|---|---|---|---|---|
| ID | Processing System | c | | source for profiling & tracing. | | ct) | ons | customer profiles. | 'one-to-many' and 'mule' account detection. |
| Receiver Account ID | Transaction Processing System | Alphanumeric | Real-time | Identification of destination for profiling & tracing. | Y | PII (indirect) | IT Operations | Linking to customer profiles. | Essential for 'many-to-one' and 'mule' account detection. |
| Sender/Receiver Bank/Institution | Transaction Processing System | String | Real-time | Interbank transaction monitoring, correspondent banking risk. | Y | Public | IT Operations | Standardization of bank names. | Important for unusual country party transactions. |
| Transaction Geographic Location | Transaction Processing System (ATM/POS) | String | Real-time | Location-based anomaly detection (e.g., unusual travel). | Y | Public | IT Operations | Geocoding; association with customer's usual location. | Aids in "Unusual Geographic Location Based Transaction Detection". |
| Blacklist Status | External AML Databases | Boolean | Daily/Real-time | Screening for known problematic entities. | Y | Public | Compliance | Direct lookup; refresh periodically. | Critical for immediate identification of sanctioned entities. |

| Data Element | Source System(s) | Data Type | Frequency/Freshness | Purpose for Personalization | Availability (Y/N) | PII/Sensitivity | Data Owner | Transformation/Processing | Remarks/Privacy Concerns |
|---|---|---|---|---|---|---|---|---|---|
| PEP Status | External AML Databases | Boolean | Daily/Real-time | Screening for Politically Exposed Persons risk. | Y | Public | Compliance | Direct lookup; refresh periodically. | Regulatory requirement for enhanced due diligence. |
| Sanction List Status | External AML Databases | Boolean | Daily/Real-time | Screening for entities on global sanction lists. | Y | Public | Compliance | Direct lookup; refresh periodically. | Mandated for compliance with international sanctions. |
| Historical Case Data | Existing AML Solution, Internal CMS | Text/Structured | On-demand | Incident and trigger event-based review, case accumulation. | Y | Sensitive | Compliance | Text analysis, categorization of case types/outcomes. | Provides context for current alerts and profiling. |
| Alert History | Existing AML Solution, Internal CMS | Structured | Real-time | Learning from false positives/negatives, behavioral patterns. | Y | Sensitive | Compliance | Aggregation by customer, rule, or time. | Essential for continuous learning and false positive mitigation. |
| Account Status (Active/Blocked) | Core Banking System | String | Real-time | For effective account blocking/unblocking actions. | Y | Public | Operations | Direct mapping. | Ensures system has current state of account for post-actions. |

# 07. Functional Scope Summary (In/Out of Scope)

## 7.1. In Scope

The following functionalities are explicitly included in the initial phase of the AI/ML-based AML Compliance solution:

- **Customer Profiling & Lifecycle Management**:
    - Creation and maintenance of customer profiles (profession, income, location, transaction pattern).
    - Review mechanisms based on historical data, prior cases, and alert accumulation.
    - Periodic customer review with AI-based suggestions for profile updates.
    - System-initiated profile updates based on detected changes.

- **Data Collection and Analysis**:
    - Integration and ingestion of transactional and customer behavior data from internal bank systems.
    - Integration with designated external data sources (Blacklist, AML screening lists, PEP lists) as provided by the client.
    - Foundation for future machine learning data.

- **Transaction Monitoring & Anomaly Detection**:
    - Deployment of AI/ML algorithms for identifying atypical patterns and suspicious behavior.
    - Ability to set, review, and update transaction limits.
    - Custom Rule Configuration: Dynamic Detection Scenarios, Dynamic Rule setting, Rule-based Detection, Alert Generation, System-based Case generation, False Positive Case Mitigation.
    - Automatic Rule Generation based on AI-detected recurring suspicious patterns.
    - Continuous adaptation and learning from historical data and monitoring results.
    - Timely alert notification via Email, SMS, and App.

- **Post Action and Case Management**:
    - Generation of sensitivity and post-action suggestions.
    - Automated, rule-based, and manual account blocking and unblocking capabilities within the new system.
    - Communication features related to alerts and account actions.
    - Manual case creation.
    - STR/SAR reporting functionality (to be developed if integration with the existing AML solution for case management is not feasible).
    - Post-action based blacklisting.

- **Reporting and Analytics**:
    - Generation of all types of regulatory and management reports.
    - Custom report creation feature with an intuitive interface for users to define new report requirements.

## 7.2. Out of Scope (for initial phase)

The following functionalities are not included in the initial phase of the project:

- **Full Customer Due Diligence (CDD) Onboarding**: While customer profiling is in scope, comprehensive, end-to-end customer onboarding and initial CDD workflows are not the primary focus of this project and remain with existing systems.
- **Comprehensive Customer Interaction Management**: Direct customer communication (e.g., requesting additional documentation) outside of automated notifications/suggestions for the AML team is not handled by this system.
- **Integration with all potential external data sources**: Only the explicitly mentioned Blacklist, AML screening, and PEP lists are in scope initially. Future integration with other third-party data providers will be a separate phase.

- **Direct Law Enforcement Interaction**: The system will generate reports (STR/SAR) but will not directly manage communication channels or submissions to law enforcement agencies beyond report generation.
- **Comprehensive Fraud Detection (beyond AML)**: The system focuses on AML-related fraud and suspicious activities. Broader fraud detection (e.g., credit card fraud, identity theft outside of AML context) is not the primary focus unless it directly intersects with money laundering patterns.
- **Alert and Case Management**: Initially, the system will *park* alerts in the bank's existing AML solution for management. The development of a *full-fledged, standalone* internal case management module will only proceed if handshake/integration with the existing system proves unfeasible, becoming a conditional inclusion.

# 08. Suggested KPIs for Success Measurement

Key Performance Indicators (KPIs) to measure the success and effectiveness of the AI/ML-based AML Compliance solution:

1. **False Positive Reduction Rate**: Percentage decrease in the number of false positive alerts generated by the system compared to the previous state.
    - *Target*: X% reduction within the first 6 months.

2. **Anomaly Detection Accuracy (True Positives)**: Percentage of actual suspicious activities correctly identified by the system (reduction in false negatives).
    - *Target*: Achieve Y% detection accuracy for known anomaly types.

3. **Time to Detect Anomalies**: Average time taken from a transaction occurring to an alert being generated and available for review.
    - *Target*: Alerts generated within Z seconds for high-priority cases.

4. **Case Resolution Efficiency**: Average time taken for AML Analysts to investigate and resolve an alert/case generated by the system.
    - *Target*: A% reduction in average case resolution time.

5. **Regulatory Compliance Adherence**: Percentage of regulatory reports submitted on time and without errors, and successful audits.
    - *Target*: 100% on-time submission; Zero critical audit findings related to AML system.

6. **Operational Cost Savings**: Reduction in manual effort (FTEs) or operational expenses associated with transaction monitoring and investigation.
    - *Target*: B% cost savings in AML operations.

7. **AI Model Effectiveness**: Measured by the rate of useful auto-generated rules, and the improvement in model precision/recall over time.
    - *Target*: C% of AI-generated rules actively contributing to detection; D% improvement in model performance metrics.

8. **System Availability/Uptime**: Percentage of time the system is operational and accessible to users.
    - *Target*: 99.9% uptime during operational hours.

9. **User Satisfaction Score**: Feedback from Compliance Analysts and Officers on the system's usability, efficiency, and effectiveness.
    - *Target*: Achieve an average satisfaction score of X out of 5 in user surveys.

10. **Number of STR/SARs Filed**: Quantity of Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) filed based on system-generated alerts that lead to confirmed suspicious activity.
    - *Target*: Consistent number of valid STR/SARs indicating effective detection.