

# Business Requirement Specification

Integrated AML, Trade Compliance &  
Fraud Risk Management Platform

## Contents

1. Executive Overview .....	3
2. Business Objectives .....	3
3. Scope of the Project .....	3
4. Business Projections .....	3
5. Functional Requirement Details .....	4
6. Acceptance Criteria .....	18
7. Workflow requirement .....	18
8. AI/ML Model Governance Framework .....	19
9. Hardware Requirements & Related Cost Finalizations .....	19
10. Business Continuity Plan .....	19
11. System Integration .....	20
12. Stakeholders .....	20
13. Appendix – 1 .....	20

## 1. Executive Overview

This document defines the business requirements for implementing a single, integrated, AI-driven AML, Trade Compliance, and Fraud Risk Management platform for The City Bank PLC. The platform will provide end-to-end financial crime risk coverage across all channels and departments with role-based access control.

## 2. Business Objectives

- Establish a single enterprise platform for AML, TBML, SWIFT monitoring, and Fraud Risk Management
- Enhance regulatory compliance with Bangladesh Bank, BFIU, FATF, PCI DSS, ISO standards
- Enable real-time risk detection and proactive intervention
- Reduce false positives and operational overhead through AI/ML

## 3. Scope of the Project

- AML/CFT Screening & Monitoring
- Transaction Monitoring (CASA, Cards, Digital, Payments)
- Trade-Based Money Laundering (TBML) Monitoring
- SWIFT Message Screening
- Fraud Risk Management (All Channels)
- Centralized Case Management
- Regulatory Reporting (STR/SAR, ISS, MIS)
- Role-Based Access Control (RBAC)
- Integration with all core and digital banking systems

## 4. Business Projections

The implementation of the AI-Driven AML & Fraud Risk Management Ecosystem is expected to deliver measurable operational, financial, regulatory, and risk-reduction benefits immediately after deployment.

### Strategic Objectives

- Establish a **single source of truth** for AML, Trade Compliance, and Fraud Risk Management
- Enable **real-time, proactive detection** of money laundering, TBML, and fraud risks
- Reduce **false positives** through AI-driven risk scoring and continuous learning
- Improve **regulatory compliance, audit readiness, and reporting accuracy**
- Enhance **cross-department collaboration** with standardized workflows
- Build a **future-ready, scalable platform** for new products and channels

### Business Outcomes

- Faster alert resolution and investigation turnaround
- Reduced regulatory and operational risk
- Improved customer trust and digital security
- Lower operational cost through automation.

## 5. Functional Requirement Details

Money Laundering & Terrorist Financing Prevention Division		
1. Screening and Risk Assessment		
FR Code	Functionality	Details
AML 1.1	<b>Sanction Screening with near real time updated Sanction List</b>	<p>The system shall accept and process all commonly used data formats, including but not limited to: PDF, DOCX, CSV, XLSX, TXT, XML, URLs, Images (e.g., JPEG, PNG)</p> <p>Cross-Referencing Against Sanction Sources</p> <p>The system shall be capable of cross-referencing input data with internal, external, and global sanction lists, including but not limited to:</p> <ul style="list-style-type: none"> <li>• United Nations (UN) Sanctions List</li> <li>• Office of Foreign Assets Control (OFAC) List</li> <li>• European Union (EU) Sanctions List</li> <li>• United Kingdom (UK) Sanctions List</li> <li>• High-Risk Jurisdiction country lists</li> <li>• Dow Jones sanction list</li> <li>• Local regulatory sanction lists</li> <li>• Any additional sanction datasets required in the future</li> </ul> <p>Sanction List Update Frequency</p> <p>The system shall ensure sanction lists are updated in near real-time to maintain accuracy and compliance.</p>
AML 1.2	<b>Foreign Language &amp; Script Handling</b>	<p>The system shall:</p> <ol style="list-style-type: none"> <li>1. <b>Support multilingual screening</b> by automatically detecting and translating foreign-language characters, ensuring that potential matches are identified even when customer information and sanction list entries use different languages or scripts.</li> <li>2. <b>Handle alternate spellings and name variations</b>, attempting multiple possible spellings or transliterations to improve match accuracy.</li> <li>3. <b>Allow screening at all required stages</b>, including: <ul style="list-style-type: none"> <li>○ Pre-onboarding</li> <li>○ Periodic reviews</li> <li>○ Ad-hoc or event-driven screenings</li> </ul> </li> <li>4. <b>Continuously update sanction lists</b> and, upon receiving any update or newly added name, system will screen the new entries against the existing customer database to identify potential matches.</li> </ol>
AML 1.3	<b>Adverse Media News Screening</b>	<p>Inputs to the System:</p> <ul style="list-style-type: none"> <li>• All commonly used data formats</li> <li>• The system will be integrated with external data source to identify Adverse news on potential/ existing customer.</li> </ul> <p>The system shall perform adverse media screening during:</p> <ul style="list-style-type: none"> <li>• Customer Onboarding</li> <li>• Periodic customer reviews / KYC refresh cycles</li> </ul>

		Automated alerts shall be generated for any detected adverse news. Also generate MIS for adverse news monitoring.
AML 1.4	<b>Photo matching functionality</b>	The system shall provide an AI-based photo matching functionality to compare images of applicants (borrower, guarantor, introducer, etc.) against internal and external databases with confidence level in %
AML 1.5	<b>PEP/IP Screening</b>	<ul style="list-style-type: none"> <li>The system will have the capability to integrate with external data source to identify potential PEP/ IP.</li> <li>Automated screening of PEP/ IP during on boarding and periodic review.</li> </ul>
AML 1.6	<b>Internal Negative/Blacklisted/ Adverse News on Customer Screening</b>	<ul style="list-style-type: none"> <li>Internal negative/blacklisted customer screening automatically. Also generate MIS for adverse news monitoring.</li> </ul>
AML 1.7	<b>MIS on Sanction Screening Result</b>	<p>The system must generate comprehensive MIS reports related to sanction screening activities. These reports should include:</p> <ul style="list-style-type: none"> <li><b>Summary of all screening results</b>, including matches, non-matches, and exceptions.</li> <li><b>Detailed analysis of false positives</b>, highlighting reasons for false alerts, patterns, and recommendations for tuning the screening parameters.</li> <li><b>Trend and performance metrics</b>, such as volume of screenings, hit rates, false-positive rates, and resolution timelines.</li> <li><b>Exportable and filterable report formats</b> (e.g., Excel, CSV) for management review and regulatory reporting.</li> </ul>

**Note:**

- The System should be able to read and translate multi-language input and cross-match with the data.
- All updates to the sanction lists must be logged for auditing purposes. The system must maintain version control for each list to track changes over time.

**2. Transaction Monitoring and Reporting (from CASA & CC)**

FR Code	Functionality	Details
AML 2.1	<b>Real-Time AML Surveillance</b>	The system must monitor financial transactions in real-time (Event-driven) across all channels, including Core Banking, Internet, Mobile, Card, and Remittance, to detect suspicious patterns, layering, structuring, and unusual activity.
AML 2.2	<b>Data Ingestion and Integration</b>	The solution must allow data ingestion and exchange with KYC/CDD systems, core banking, CRM, and external intelligence sources through RESTful APIs.
AML 2.3	<b>Dynamic data analysis</b>	Based on each customer's verified income documents and other key risk indicators—such as profession, source of funds, geographic exposure, transactional behaviour, and quality of submitted documents—a dynamic, risk-based transaction limit will be set within regulatory thresholds. This approach ensures that transaction capacity aligns with the customer's true financial standing and risk profile.

		For example, factors like internal credit rating, historical transaction pattern, product type, account tenure, cross-bank fund transfers, payment limits, and digital channel usage can be used to automatically adjust and monitor permissible limits, enhancing both compliance and control.
AML 2.4	<b>Rule based Detection Scenario and Alert Generation</b>	Specific transaction threshold will generate alerts when activities deviate from expected behaviour. These alerts will be treated as potential risk events and prioritized based on severity.
AML 2.5	<b>False positive case mitigation</b>	With AI and parameter-based analytics, the system will intelligently identify and suppress false positives, allowing investigators to focus on truly suspicious cases.
AML 2.6	<b>Potential STR/SAR cases identification</b>	The solution will automatically identify confirmed suspicious cases and prepare the required STR/SAR formats for regulatory submission, ensuring accuracy and timeliness.
AML 2.7	<b>Maintain STR database</b>	The system shall keep a full STR database with clear lifecycle status, enable branch-to-HO reconciliation, and allow SOL/branch-wise STR status reporting.
AML 2.8	<b>Alert on STR account transaction</b>	If huge transactions occur in identified STR/SAR accounts or previously frozen accounts after unfreeze, the system shall trigger alerts, pop-ups, or SMS notifications to AML teams and branches for further EDD.
AML 2.9	<b>Hybrid approach on Alert Management</b>	Each issue shall be subject to a three-tier referral framework. Alerts shall be distributed between branch operations and central AML teams following a hybrid case management approach. The system shall ensure that alerts are handled based on their category, origin, and risk severity, enabling efficient and coordinated resolution.
AML 2.10	<b>Communication</b>	Based on the post actions, relevant stakeholder communication shall be generated by the system. If needed customer communication can be initiated from the system.
<b>3. STR/SAR Identification and Processing</b>		
<b>FR Code</b>	<b>Functionality</b>	<b>Details</b>
<b>AML 3.1</b>	<b>Potential STR/SAR cases identification</b>	The solution will automatically identify confirmed suspicious cases and prepare the required STR/SAR formats for regulatory submission, ensuring accuracy and timeliness.
<b>AML 3.2</b>	<b>STR-SAR workflow</b>	It will feature an integrated workflow covering initiation, review, approval, and XML file preparation for regulatory submission. Branches and divisions shall also be able to raise STR/SARs directly to the ML & TFP Division through a single platform.
<b>AML 3.3</b>	<b>STR database</b>	The system will automatically update the MIS upon submission, maintain complete case lifecycle records with audit trails, and support real-time tracking for timely follow-up.  The system will allow branch-to-HO reconciliation, and allow SOL/branch-wise STR status reporting.
<b>4. Freeze and Unfreeze Management</b>		

FR Code	Functionality	Details
AML 4.1	Freeze/Unfreeze Functions	<ul style="list-style-type: none"> <li>The system will be able to auto detect (upon having the necessary criteria input from AML team) the suspected accounts to be freeze as per the internal process of City Bank.</li> <li>The Freeze accounts are received from City Bank's internal investigation.</li> <li>A centralized Freeze &amp; Unfreeze dashboard shall display details like data like Active freezes, Expiry dates, Linked accounts, Override and update options etc.</li> <li>The system shall integrate with Core Banking and related systems.</li> <li>The system shall also identify and display accounts where unusually large transactions occur when an account transitions from unfreeze to freeze.</li> <li>Automated reports shall be generated for supervisors and regulators.</li> </ul>

#### 5. Detection and Risk Management Technology

FR Code	Functionality	Details
AML 5.1	AI/ML-Based Detection Models	The system should apply <b>supervised and unsupervised machine-learning models</b> to identify anomalies and hidden patterns not captured by static rules. It should utilize machine learning and advanced analytics to identify suspicious transaction patterns and evolving typologies of money laundering.
AML 5.2	Dynamic Risk Scoring	The solution must continuously evaluate customer and transaction risk using behavioural, geographic, and entity-based parameters (such as KYC, occupation, volume, velocity, and counterparties). This capability ensures compliance with AML/CFT requirements.
AML 5.3	Event-Driven Risk Recalculation	The system must automatically recalculate customer risk ratings in an event-driven manner based on predefined triggers.
AML 5.4	Entity Resolution & Graph Analytics	The platform should correlate related entities (accounts, devices, merchants, IPs) using <b>graph-based intelligence</b> to uncover collusion, mule networks, layering, or circular money flows.
AML 5.5	Nominee and Beneficiary Relationship Detection	<p>The system also should detect:</p> <ul style="list-style-type: none"> <li>One customer acting as nominee for multiple accounts</li> <li>Same beneficiary linked with multiple accounts</li> </ul>
AML 5.6	Explainable AI (XAI)	<p>The system must provide full transparency for all alerts and risk scores generated by its AML models. For each flagged transaction or entity, the system must present <b>explainable reasoning</b>, including contributing features and their impact on the final risk score, to support compliance and audit review.</p> <p>The explanation should be <b>detailed enough to justify model decisions</b> to regulators and facilitate manual investigation. All explanations and model decisions must be logged and retrievable for regulatory inspection, ensuring compliance with applicable AML regulations.</p>
AML 5.7	Continuous Learning and Feedback Loop	<p><b>Analyst Feedback Integration</b></p> <ul style="list-style-type: none"> <li>The system <b>must allow analysts to provide feedback</b> on each alert, including marking it as true positive, false positive, or other relevant categories.</li> </ul>

		<b>Model Retraining and Adaptation</b> <ul style="list-style-type: none"> <li>Feedback provided by analysts <b>will be used to retrain and refine the AML models</b>, improving accuracy over time and <b>reducing false positives</b>.</li> <li>The system should support <b>periodic or on-demand retraining</b> while maintaining auditability of changes to the model.</li> </ul> <b>Audit and Traceability</b> <ul style="list-style-type: none"> <li>All feedback and subsequent model updates <b>must be logged</b>, ensuring a <b>full audit trail</b> for compliance and regulatory review.</li> </ul>
<b>6. Search Engine</b>		
<b>AML 4.1 Input Mechanism</b>		
<b>FR Code</b>	<b>Functionality</b>	<b>Details</b>
AML 4.1.1	<b>Manual Input</b>	The system should be able to take input from the following: Excel, CSV, PDF, Images, URL, TXT, XML, Adverse News Monitoring Report
AML 4.1.2	<b>Language Translation and Multi-language Support</b>	The sanction lists provided by the bank may contain names and details in multiple languages, depending on the country of origin and the issuing sanctioning body. The system must have the capability to match that.
<b>4.2 Search Criteria</b>		
AML 4.2.1	<b>Customer Search</b>	<p>By keying the following information, system will identify the customer:</p> <ul style="list-style-type: none"> <li>Identification Number</li> <li>Date of Birth</li> <li>Mobile Number</li> <li>Email Address</li> <li>Customer Name (Full Name, First Name, Last Name, etc.)</li> <li>Communication Address (Partial or Full Address)</li> <li>Father's Name</li> <li>Mother's Name</li> <li>Profession</li> <li>Spouse's Name</li> </ul> <p>There can be a single information. If the input is more than one, the name will be constant the other input value will be considered as "OR".</p>
AML 4.2.2	<b>Exact Match (100%)</b>	<p>For numeric or unique identifier fields (e.g., Identification Number, Mobile Number), the system shall return results only when there is an exact match.</p> <p>No partial matching or approximations shall be applied for these fields when Exact Match mode is selected.</p>
AML 4.2.3	<b>Partial Match (Configurable 0-100%)</b>	<p>The system shall allow searches based on partial matching of input values.</p> <p>The degree of match shall be configurable as a percentage (0–100%), enabling flexibility to account for spelling errors, typos, or minor variations in input data.</p> <p>Users shall have the ability to adjust the matching threshold</p>



		according to their search requirements.
AML 4.2.4	<b>Probable Matching Rule for qualitative information</b>	<p>For qualitative data fields (e.g., names, addresses), the system shall implement <b>probable matching techniques</b>, including but not limited to:</p> <ul style="list-style-type: none"> <li>• <b>Fuzzy Matching</b></li> <li>• <b>Phonetic Matching</b></li> </ul> <p>These rules shall help identify records that are similar in sound or spelling even if not identical.</p> <p><b>Examples:</b></p> <ul style="list-style-type: none"> <li>• “Noor Rohoman” and “Nor Rahman” may be identified as similar despite different spellings.</li> <li>• Searching for “Sefat” may also return “Shifat”, “Sifat”, or “Seefat” when other variables are considered.</li> </ul>
<b>4.3 Search Output</b>		
AML 4.3.1	<b>Basic Customer Information:</b>	<p>If true match found, following information should be illustrated:</p> <ul style="list-style-type: none"> <li>- Basic Customer Information</li> <li>- Account Information</li> <li>- Transactional Data</li> </ul>
AML 4.3.2	<b>Flexibility in Search Query Input/output</b>	The system shall return relevant and meaningful results regardless of how many fields are populated, ensuring that searches are flexible and user-friendly while maintaining accuracy in matching and reporting potential AML risks.
<b>7. Case Management and Operations</b>		
FR Code	Functionality	Details
AML 5.1	<b>Intelligent Case Management</b>	The system should automatically generate AML alerts and rank them by severity. It must also provide smart case management features, support automated alert triage, and enable smooth workflow collaboration between compliance officers and investigators.
AML 5.2	<b>Case Management Functions</b>	The integrated case management system should enable real-time case creation for identified money laundering patterns and it should support multiple work queues to manage different compliance activities such as <b>staff compliance</b> and <b>KYC compliance</b> .
AML 5.3	<b>Alert Prioritization</b>	Alerts must be prioritized based on set parameters and defined rules.
<b>8. Reporting, Audit Trail and Regulatory Compliance</b>		
FR Code	Functionality	Details
AML 6.1	<b>Freeze &amp; Unfreeze Database</b>	A dashboard should display all active freezes, their expiry dates, and any linked accounts, with easy options to update or override instructions. The system should integrate seamlessly with core banking and other required systems, and automatically generate reports for supervisors and regulators.
AML 6.2	<b>Report on Locker list</b>	The system should provide a report that allows AMLD to check whether a customer holds a locker with the Bank by searching using any available customer identifier, such as National ID, Mobile Number, or Account Number.
AML 6.3	<b>AML Training MIS</b>	Regulatory authorities require the bank to ensure that all employees receive training on Anti-Money Laundering (AML) and related compliance topics, and to periodically report on these trainings. To meet this requirement, the bank AML team needs a training management system.

		<p>The training management system will be fully automated and integrated with HRMS and People HR. It will record invitations (individual or group), cancellations, and attendance automatically. It will also generate absentee and eligible participant lists, ensuring accurate tracking. Through HRMS integration, the system will pull data like designation, role, and compliance needs for training need assessments, while training plans and schedules are synced with HR's calendar and leave data for better coordination.</p>
AML 6.4	<b>Self-Assessment Report</b>	<p>The proposed system will be a web-based platform with an intuitive dashboard and automatic reminders. Branch AML teams will have branch-specific access, allowing them to view and manage only their assigned cases through the dashboard.</p> <p>Data can be pulled directly from existing systems or uploaded via Excel for greater flexibility and accuracy. Role-based access control will ensure secure data entry and management, while comprehensive data security and a full audit trail will maintain transparency.</p> <p>The system will also auto-generate half-yearly reports with trend analysis and send email alerts for any issues that remain unresolved or fall below the required standard.</p>
AML 6.5	<b>Automated Transaction Monitoring and Database</b>	<p>The system will include a centralized MIS that automatically captures all flagged accounts and related details, making it easy to track and monitor them.</p> <p>It will support real-time, event-driven updates, allowing branches and divisions to log actions and feedback as they happen.</p> <p>Each flagged account will maintain a complete history of actions and feedback, ensuring clear accountability for all activities.</p> <p>An integrated audit trail will provide full transparency, supporting compliance reviews, regulatory reporting, and internal oversight.</p>
AML 6.6	<b>ISS Report</b>	<p>The system should automatically generate the ISS report in the required regulatory format. It will extract data directly from source systems and organize it according to regulatory guidelines. The report will be produced in Excel, making it easy to review, analyze, and submit. This automation should reduce manual effort, increase accuracy and efficiency, minimize errors, and ensure timely, regulator-ready reporting.</p>
AML 6.7	<b>TP reporting</b>	<p>Monthly TP update and review status reports shall be generated as per schedule.</p> <p>The system shall calculate the number of TP reviews required and completed per branch.</p>
AML 6.8	<b>Holistic AML report</b>	<p>The proposed system will provide a comprehensive, centralized MIS offering a consolidated view of all account-related information. It will include intelligence-driven fields such as STR/SAR status, BFIU inquiry flags, TP breach percentages, and account freeze history. By integrating these data points, the MIS will present a holistic account view, enhancing transparency, supporting regulatory compliance, and enabling the ML &amp; TFP Division to make faster, more informed decisions.</p>

AML 6.9	<b>Regulatory Adherence</b>	The solution must ensure full compliance with Bangladesh Bank AML/CFT Guidelines, FATF Recommendations, and global AML/CFT regulations. It must also support localization to meet Bangladesh Bank AML/CFT and FATF reporting standards.
AML 6.10	<b>Regulatory Reporting Automation</b>	<b>The system should</b> generate STR/SAR drafts, regulatory reports, and periodic AML summaries. Ensures data accuracy through standardized templates and automated validation checks.
<b>Trade Service Division</b>		
<b>FR Code</b>	<b>Functionality</b>	<b>Details</b>
TSD 1.1	<b>Sanction Screening</b>	<p>a. <b>Goal:</b> Prevent transactions with sanctioned/black listed entities and to identify high risk entities/ persons/ PEPs/ countries/ jurisdictions/adverse media news for EDD.</p> <p>b. <b>Source Data:</b></p> <ul style="list-style-type: none"> <li>• Paid Data Base like: World check, Lloyd's list</li> <li>• Open Source data like OFAC/</li> <li>• BFIU/local list</li> <li>• Banks own black/high alert list</li> <li>• Sanctioning authority website like: OFAC, EU, UN, HMT/HK/Switzerland sanction List</li> <li>• Adverse Media News etc.</li> <li>• PEP list</li> <li>• FATF Country list based on risk like black list, grey list, non-member etc.</li> <li>• Open source like: knowyourcountry.com</li> </ul> <p>c. <b>Approach:</b></p> <ul style="list-style-type: none"> <li>• Manual and automated screening against applicable lists like OFAC, UN, EU, and local lists.</li> <li>• Bidirectional Integration with processing module (City IMPEX/Ababil)</li> <li>• Screen counterparties, vessels, ports, and countries.</li> <li>• Use in pre/post transaction monitoring tools.</li> <li>• Issue resolution through 3 level review/referral system.</li> <li>• Report, case Management, SAR/STR.</li> </ul>
TSD 1.2	<b>SWIFT Message Screening</b>	<p>a. <b>Goal:</b> Detect suspicious patterns in financial messaging.</p> <p>b. <b>Source:</b> Database mentioned in this document.</p> <p>c. <b>Approach:</b></p> <ul style="list-style-type: none"> <li>• Parse incoming and outgoing Swift messages</li> <li>• Bidirectional Integration with trade module, middleware like XMM, CBS and other system like e-deal, LWF etc. sending and receiving SWIFT messages</li> <li>• Use list and probable hit based on international standards (source similar as 1)</li> <li>• Use keyword and pattern matching to detect red flags (e.g., unusual terms, routing).</li> <li>• Use of A.I and M.L.</li> <li>• Use in pre/post transaction monitoring tools.</li> <li>• Issue resolution through 3 level review/referral system.</li> <li>• Report, case Management, SAR/STR.</li> </ul>
TSD 1.3	<b>Price Verification</b>	<p>a. <b>Goal:</b> Detect over/under-invoicing by analyzing historical price, current market price etc.</p>

		<p>b. <b>Source Data:</b></p> <ul style="list-style-type: none"> <li>• Data base of own bank transactions: City IMPEX, Ababil, BB-OIMS, BB-OEMS.</li> <li>• Data of other bank transactions: BFIU has plan to share, may be incorporated once available.</li> <li>• Subscribed data base: currently GTT, Lloyd's List if can be purchased or solution provide may offer internationally recognized database.</li> <li>• Customs database when accessible/</li> <li>• Open source price data: Index prices and global specialized websites.</li> </ul> <p>c. <b>Approach:</b></p> <ul style="list-style-type: none"> <li>• Include HS code/Country of origin/country of Import/country of export-based price ranges.</li> <li>• Use source data to set benchmark prices/base prices.</li> <li>• Apply machine learning to flag anomalies based on historical pricing patterns.</li> <li>• Provide the result to user/system (Manual search report, API)</li> <li>• Use of AI and Machine Learning for detection based on name.</li> <li>• Use in pre/post transaction monitoring tools.</li> <li>• Issue resolution through 3 level review/referral system.</li> <li>• Report, case Management, SAR/STR.</li> </ul>
TSD 1.4	<b>Dual-Use Goods Detection</b>	<p>a. <b>Goal:</b> Identify goods that can be used for both civilian and military purposes.</p> <p>b. <b>Source:</b></p> <ul style="list-style-type: none"> <li>• Open sources like: EU or US export control lists.</li> <li>• Purchased database.</li> </ul> <p>c. <b>Approach:</b></p> <ul style="list-style-type: none"> <li>• Maintain a list of dual-use items, H.S code wise, country wise.</li> <li>• Flag transactions involving these items for enhanced due diligence.</li> <li>• Results to be included in price verification report (Manual search, API)</li> <li>• Use of A.I and M.L for detection based on name.</li> <li>• Use in pre/post transaction monitoring tools.</li> <li>• Report, case Management, SAR/STR.</li> <li>• Issue resolution through 3 level review/referral system.</li> </ul>
TSD 1.5	<b>Restricted and Banned items</b>	<p>a. <b>Goal:</b> Identify goods that are restricted for certain purpose, or Banned for import/export.</p> <p>b. <b>Source:</b></p> <ul style="list-style-type: none"> <li>• Regulatory documents like IPO, Export Order</li> <li>• Any other country/region specific lists.</li> </ul> <p>c. <b>Approach:</b></p> <ul style="list-style-type: none"> <li>• List of restricted items, banned items based on H.S code, Name, sector, industry etc.</li> <li>• Flag transactions involving restricted items for Enhanced Due Diligence.</li> <li>• Results to be included in price verification report (Manual search, API)</li> <li>• Use of A.I and M.L for detection based on name.</li> <li>• Use in pre/post transaction monitoring tools.</li> </ul>

		<ul style="list-style-type: none"> <li>• Report, case Management, SAR/STR.</li> <li>• Issue resolution through 3 level review/referral system</li> </ul>
TSD 1.6	<b>Pre-Transaction Monitoring</b>	<p>a. <b>Goal:</b> Risk assessment before transaction execution.</p> <p>b. <b>Source Data:</b> trade module, middleware, CBS and proposed database</p> <p>c. <b>Approach:</b></p> <ul style="list-style-type: none"> <li>• AI enabled documents checker</li> <li>• Rule-based and AI-driven risk scoring.</li> <li>• Rule based monitoring.</li> <li>• Report, case Management, SAR/STR.</li> <li>• Issue resolution through 3 level review/referral system.</li> </ul>
TSD 1.7	<b>Post-Transaction Monitoring</b>	<p>a. <b>Goal:</b></p> <ul style="list-style-type: none"> <li>• Detect laundering after transaction completion.</li> <li>• Issue resolution through 3 level review/referral system.</li> <li>• STR/SAR reporting.</li> </ul> <p>b. <b>Sources of Data:</b></p> <ul style="list-style-type: none"> <li>• Credit report data: read the report and store data automatically to defined fields</li> <li>• Customer/counter party/country/jurisdiction data: From trade modules.</li> <li>• Transaction data: systematic storing and retrieval from trade module.</li> </ul> <p>c. <b>Approach:</b></p> <ul style="list-style-type: none"> <li>• Set rules to identify deviations/high risk issues that might be linked with TBML</li> <li>• Generate alert.</li> <li>• Manage Alerts</li> <li>• Implement 3 level review system</li> <li>• Generate STR/SAR and report to central bank/BFIU.</li> </ul>
TSD 1.8	<b>Compliance With BFIU Trade Monitoring Indicators</b>	<p><b>a. Goal:</b> Ensure that all trade transactions are monitored in alignment with the BFIU-suggested Trade-Based Money Laundering (TBML) Indicators included in <b>Appendix–1: BFIU TBML Checklist (Trade Monitoring Indicators)</b>. At a minimum, the system must:</p> <ul style="list-style-type: none"> <li>• Enable automated or semi-automated evaluation of each checklist item.</li> <li>• Support monitoring at the stage(s) specified in the checklist (Pre-Transaction, Post-Transaction, or Both).</li> <li>• Capture, store, and track checklist outcomes as part of the trade monitoring workflow.</li> <li>• Trigger alerts whenever any BFIU-recommended indicator is breached.</li> <li>• Maintain full audit trails for all checklist-based assessments.</li> </ul> <p><b>b. Outcome:</b> A standardized, regulator-aligned TBML monitoring framework ensuring compliance with BFIU guidelines through structured, consistent, and auditable trade-risk assessments.</p>
<b>Central Reconciliation and Swift Services</b>		

FR Code	Functionality	Details
CRSS 1.1	<b>SWIFT Message Screening for Inward &amp; Outward Messages</b>	<p>The system should screen all inward and outward SWIFT messages.</p> <p>The solution shall provide a <b>department- or stakeholder-based list</b> of all SWIFT messages that are pending action.</p> <p><b>Unmatched SWIFT messages</b> should be automatically routed to the respective stakeholders based on message type.</p> <p>CRSS should be able to manually forward <b>unmatched SWIFT messages that fail to auto-route</b>, to the respective stakeholders, as well as close those items with comments.</p> <p>All SWIFT messages should be <b>automatically passed to the middleware (XMM/CS)</b> as appropriate, regardless of the AML status.</p> <p>There should be a <b>reporting facility</b> for SWIFT items which fail in the XMM/CS system.</p> <p>There should be horizontal (<i>among team members</i>) and vertical (<i>other stakeholders</i>) <b>escalation facility</b>.</p> <p>CRSS should have the ability to <b>generate reports</b> for Pending, Closed, Escalated, Rejected, and Authorized items based on periodic intervals.</p> <p>There should be a facility for <b>items requiring authorization</b> to appear in a common tray under the same department (stakeholder).</p> <p>There should be a <b>super user (e.g., Admin user within the department/stakeholder)</b> who can re-escalate items if the assigned escalated user is unavailable.</p> <p>A <b>maker-checker mechanism</b> should be available for every action requiring manual judgment.</p> <p>There should be a <b>dashboard</b> for items pending processing.</p> <p>There should be an <b>Exception management facility</b>. AML Division will be able to set Exception Rules in the system.</p>

Fraud Risk Management		
Functional Requirements		
FR Code	Functionality	Details
FRM 1.1	<b>Real-Time Monitoring</b>	Process and score all transactions instantly across all channels to enable immediate decision making. Near-real-time monitoring for

		batch transactions (BEFTN/settlements)
FRM 1.2	<b>Alert Generation</b>	Create alerts based on configurable risk thresholds, rules and AI/ML-based anomaly detection models.
FRM 1.3	<b>Risk Scoring</b>	Assign dynamic and contextual risk scores using behavioral analytics, device reputation, geolocation and transaction pattern deviations
FRM 1.4	<b>Case Management</b>	Manage alerts and investigations through a centralized dashboard, supporting escalation, status tracking, analyst feedback and case linking.
FRM 1.5	<b>Behavioral Profiling</b>	Build and continuously update adaptive behavioral profiles including geographical presence of customers, merchants, accounts and devices, leveraging machine learning (ML).
FRM 1.6	<b>Device Fingerprinting</b>	Identify and track unique device signatures, detect cloned or spoofed devices, rooted, jail-broken and correlate with fraud history.
FRM 1.7	<b>Integration</b>	Ensure API-driven interoperability with core banking, card management, Citytouch, Neo Bank (Cityblink), CRM and other digital platforms, using secure and standardized communication protocols.
FRM 1.8	<b>Reporting &amp; Analytics</b>	Generate fraud summary reports, loss dashboards, analyst productivity reports and fraud trend analytics, with drill-down and export capabilities for management and regulatory review.
FRM 1.9	<b>Rule performance report</b>	Have the capacity to generate and download effective rule performance report.
FRM 1.10	<b>Capacity to adapt complex rule</b>	Have the capacity to generate alert and scoring the weightage when breaches multiple rule from a specific transaction/timeframe.
FRM 1.11	<b>User Roles &amp; Security</b>	Enforce role-based access control (RBAC), maker-checker mechanisms and multi-factor authentication (MFA) for all user activities within the system.
FRM 1.12	<b>Notifications</b>	Send automated notifications or escalations to fraud analysts, management and relevant stakeholders via SMS, email or system dashboard alerts.
FRM 1.13	<b>Model Management</b>	Enable configuration, testing and deployment of AI/ML models and detection rules within a controlled environment, including version control and performance tracking.
FRM 1.14	<b>Data Retention &amp; Audit Trails</b>	Maintain comprehensive audit logs of all transactions, alerts and analyst actions for forensic investigation and compliance.
FRM 1.15	<b>Performance &amp; Scalability</b>	Support high transaction volumes with horizontal scalability and 24x7 high availability architecture, ensuring no data loss or downtime.
FRM 1.16	<b>Workflow Automation</b>	Automate alert prioritization, case assignment and escalation based on defined business rules and service-level targets (SLAs).
FRM 1.17	<b>System Health Monitoring</b>	Include tools for monitoring system uptime, latency and rule performance, with proactive alerts for operational issues.
FRM 1.18	<b>Data Security &amp; Privacy</b>	Implement encryption (data-at-rest and in-transit), tokenization, and anonymization per PCI DSS, ISO 27001 and GDPR-equivalent standards.
FRM 1.19	<b>Global Standards Alignment</b>	Conform to international best practices, including Basel Committee's Principles for Sound Management of Operational Risk, FATF Recommendation and ISO 22301 for business continuity.

Non-Functional Requirements		
FR Code	Features	Details
FRM 2.1	<b>Performance</b>	<ul style="list-style-type: none"> <li>Support a minimum throughput of 2,000 transactions per second (TPS) across channels.</li> <li>Maintain end-to-end processing latency of under 100 milliseconds for real-time scoring and decision making.</li> <li>Ensure optimized rule execution and parallel processing for large data volumes.</li> </ul>
FRM 2.2	<b>Availability</b>	<ul style="list-style-type: none"> <li>Achieve a minimum system uptime of 99.99% through redundant architecture and automatic failover.</li> <li>Ensure active-active replication between primary and Disaster Recovery (DR) sites with Recovery Time Objective (RTO) ≤ 15 minutes and Recovery Point Objective (RPO) = 0.</li> <li>Provide built-in health monitoring and alerting for system and network failures.</li> </ul>
FRM 2.3	<b>Security</b>	<ul style="list-style-type: none"> <li>Encrypt data in transit and data at rest.</li> <li>Implement multi-factor authentication (MFA), least-privilege access and role-based access control (RBAC).</li> <li>Ensure compliance with PCI DSS, ISO 27001 and NIST Cybersecurity Framework.</li> <li>Regularly perform vulnerability assessments, penetration testing, and patch management.</li> </ul>
FRM 2.4	<b>Scalability</b>	<ul style="list-style-type: none"> <li>Support horizontal and vertical scalability to handle future channel expansion and up to 2x transaction volume growth without performance degradation.</li> <li>Enable dynamic rule deployment and scaling of processing nodes without downtime.</li> </ul>
FRM 2.5	<b>Compliance</b>	<ul style="list-style-type: none"> <li>Ensure full compliance with: <ul style="list-style-type: none"> <li>➤ BB regulatory compliance</li> <li>➤ Data Protection Act 2019 (Bangladesh)</li> <li>➤ PCI-DSS and ISO 20022 for secure financial messaging</li> <li>➤ FATF Recommendation 15 for technology risk</li> </ul> </li> <li>Provide automated regulatory reporting and secure data retention as per local and global requirements.</li> </ul>
FRM 2.6	<b>Auditability</b>	<ul style="list-style-type: none"> <li>Maintain immutable audit logs for all transactions, alerts, configuration changes, and user activities.</li> <li>Integrate with City Bank's SIEM (Security Information and Event Management) solution for centralized log collection and real-time security analytics.</li> <li>Support forensic investigation and evidence export capabilities with digital signature validation.</li> </ul>
FRM 2.7	<b>Maintainability</b>	<ul style="list-style-type: none"> <li>Support automated deployment, version control, and system updates without service interruption.</li> <li>Provide comprehensive documentation, admin tools, and monitoring interfaces for operational teams.</li> </ul>
FRM 2.8	<b>Data Retention and Archiving</b>	<ul style="list-style-type: none"> <li>Retain historical transaction and alert data for at least 7 years, in line with regulatory and audit requirements.</li> </ul>



		<ul style="list-style-type: none"> <li>• Support tiered storage for active, historical, and archived data with fast retrieval options.</li> </ul>
FRM 2.9	<b>Interoperability</b>	<ul style="list-style-type: none"> <li>• Ensure compatibility with existing and future City Bank IT infrastructure, including middleware, CRM, card systems, and analytics platforms.</li> <li>• Support open standards and API-based architecture for easy integration with third-party or regulatory systems.</li> </ul>
FRM 2.10	<b>Dynamic Resource Scaling</b>	<ul style="list-style-type: none"> <li>• Ensure the system can automatically scale resources up or down in response to real-time transaction demand and system utilization metrics.</li> </ul>

**Note:** The platform must support bi-directional intelligence sharing between AML and Fraud modules with a unified risk view.

## 6. Acceptance Criteria

The system will be accepted upon successful verification that the following criteria are met:

### 5.1 Functional Acceptance

100% successful UAT of all the requirements mentioned in Functional Requirements Details.

### 5.2 Performance Acceptance

- Support **minimum 2,000 TPS** with <100ms latency.
- End-to-end processing (data ingestion → scoring → alert creation) within 1–5 minutes depending on batch or real-time.
- Auto-scaling in cloud mode to handle peak load.
- Must support linear scalability as transaction volume increases (≥50% annual growth).
- Achieve 99.99% system uptime during UAT stress testing.

### 5.3 Integration Acceptance

Bidirectional and Seamless API integration with Finacle, Ababil, Tranzware, City IMPEX, CityTouch, CityFast, CityBlink, LOS, DOB, CRM, and all listed systems in Section 8.

Also may need bulk upload and update functionality for power user.

Successful data ingestion from all required channels (CASA, card, trade, digital) with no data mismatch.

### 5.4 Role-Based Access Control (RBAC)

The system shall implement **fine-grained RBAC**, ensuring users can only access data and functions relevant to their role and department. RBAC Principles:

- Least-privilege access
- Maker–Checker enforcement
- Department-level data segregation
- Central override by authorized Head Office users

### 5.5 Reporting & Audit Acceptance

- STR/SAR XML generation must match regulator specification.
- ISS report must be generated accurately and automatically.
- MIS data must match original transaction data with <0.1% variance.

## 7. Workflow requirement

The proposed system will follow a hybrid workflow, integrating both bottom-up and top-down approaches. The specific workflow details will be determined through discussions with the vendor to ensure alignment with business requirements.

## 8. AI/ML Model Governance Framework

The solution must support a formal AI/ML model governance framework, including model lifecycle management, versioning, validation, approval workflow, and auditability.

The solution should support explainability, bias monitoring, and human-override controls in line with Responsible AI principles.

## 9. Hardware Requirements & Related Cost Finalizations

Hardware requirement & related Cost finalization for the proposed AI Gen system will be determined on post discussion with the vendor.

## 10. Business Continuity Plan

The proposed AML & Fraud Management System is a mission-critical platform supporting compliance, fraud prevention, and regulatory reporting. To ensure uninterrupted operations, the following Business Continuity Plan (BCP) will apply:

### 9.1 System Availability

- The platform must maintain **99.99% uptime** as required in the Non-Functional Requirements.
- Real-time scoring, screening, and alerting will continue without interruption across channels.

### 9.2 Disaster Recovery (DR) Readiness

- DR site must maintain an **RTO ≤ 15 minutes** and **RPO = 0**, consistent with system requirements
- Active-active replication of:
  - Transaction data
  - Sanction/PEP/adverse media updates
  - Alerts and case management information
  - Audit logs and system configuration

### 9.3 Failover Mechanisms

- Automatic failover between primary and DR sites with no data loss.
- Continuous monitoring of node health, latency, and storage capacity.

### 9.4 Continuity for Critical Functions

The following functions must remain operational even during disruptions:

- Real-time fraud detection and risk scoring
- AML sanction/PEP screening
- Regulatory reporting (STR/SAR generation, ISS reporting)
- Freeze/Unfreeze operations
- Case management workflows

### 9.5 Backup & Data Retention

- Automated daily backups for all transaction, screening, and alert data.
- The system must retain all AML, Fraud, Transaction Monitoring, Screening, Case Management, and Regulatory Reporting data for a minimum of 7 years in the production environment.
- Data must remain fully searchable, retrievable, and accessible for investigation, regulatory inspection, and audit purposes throughout the retention period.
- Archiving of Older Data: Any data older than 7 years must be automatically archived in compliance with Bangladesh Bank and global AML/CFT data retention guidelines.
- The archived data must:
  - Be securely encrypted (at rest & in transit)

- Remain immutable (non-editable)
- Support retrieval within an acceptable SLA for regulator queries
- Be stored in a cost-optimized tier (e.g., WORM storage, secure archival systems)

### **9.6 Cybersecurity & Incident Response**

- Align with Bangladesh Bank ICT Security Guidelines, BFIU AML/CFT compliance requirements and bank's internal cybersecurity policies, IT security standards, access control requirements, and secure coding guidelines.

### **9.7 Periodic Testing**

- Annual DR drill as per ICT policy.
- Semi-annual failover test for AML & Fraud monitoring modules.
- Quarterly verification of blacklist syncing, model updates, and audit logs.

## **11. System Integration**

The system must support bidirectional integration with the bank's key software platforms, including:

- Finacle
- Ababil NG
- Tranzware
- Agent Banking System (ABS)
- Liability Workflow (LWF)
- Digital Onboarding (DOB)
- Loan Originating System (LOS)
- CityFast
- NRB Software
- City IMPEX (CS) – Trade System
- City Blink – Digital Banking

In addition to the above mentioned software, system should be flexible to integrate with other software/applications/tools if required.

## **12. Stakeholders**

- AML & MLTFP Division
- Fraud Risk Management Division
- Trade Services Division
- Branch Operations
- Central Reconciliation & SWIFT Services
- IT, Information Security, Senior Management

## **13. Appendix – 1**

BFIU Trade-Based Money Laundering (TBML) Checklist — Trade Monitoring Indicators

<b>Problem Indicator/Scenario Name</b>	<b>Probable Solution/Conditions/Logic/Parameters in System</b>	<b>Proposed Solution/Remarks by "The City Bank PLC"</b>	<b>Monitoring type (Pre/post/Both)</b>
Over/under invoicing	Variation of quoted price with standard price by certain % fixed based on LC value/item value	Based on LC value, system needs to compare the proposed/executed transaction Unit Price with Base/standard price and raise alert if exceed the base price over a certain %.	Both
Shifting or changing of import/export items/goods	Difference of imported/exported items with last one year historical items	Based on H.S code and item Generic name, system will check whether current month items include any item that is not covered in last 12 month items. System will also allow user to search manually or through integration whether item in a particular transactions were listed in last one year transaction of the same customer	Post-must Pre-Feasibility test One off-checking required
Change of beneficiaries	Change of beneficiaries by amendment at any stage of transaction	System will check whether Beneficiary of transaction changed from last value and trigger alert	Post
Presenting/ negotiating bank differs with payment receiving bank	Presenting/ negotiating bank differs with payment bank	Compare the payment receiving bank with presenting/negotiating bank.	Post pre-transaction will be done by transaction module

Trade with high risk/trade heaven countries at any stage of transaction	Trade with high risk countries at any stage of transaction	Will upload and update current list of High Risk/tax heaven countries/jurisdiction through Sanctions screening platform or in CBS/Trade System to generate system alert during transaction. (Monitoring based on country of counter party according to FATF list. a. Comprehensive Sanction b. High risk- call for action. c. Sectoral sanction d. Grey list- Selected country/Jurisdiction) System will compare the list and alert.	Post Pre- as part of sanction screening, both field level and SWIFT Message detail level
Frequent amendments in L/C	Alert if the no. of amendment exceeds a certain threshold like 5/7/10. Threshold will be decided based on transaction type	Compare the no. of amendment with threshold and raise alert.	Post pre-transaction will be done by transaction module
Address of beneficiaries and document presenters differs	Difference of beneficiaries and document presenters' country / address	Compare the country and address of the LC level beneficiary and bill level presenter address and country	Post pre-transaction to be done by transaction module
Transaction Volume follow up (Significant growth (above a threshold ) in a particular month compared to last one-year average for a customer)		System will check current month transaction volume with last one year average and raise alert if exceed a certain threshold	Post

Transaction Profile Violation (review based on frequency/recurrence and percentage on different parameters like country, item, value and volume of transactions. )	Compare transactions with Trade transaction profile and alert for deviations. For numerical values, alert only if the deviation is above a certain % above/threshold applied	Compare transactions with Trade transaction profile and alert for deviations. For numerical values, alert only if the deviation is above a certain % above/threshold applied	Post
Price Variance of the Products	1. A certain % high or low from last 6-month average unit price for a particular customer 2. A certain % high or low from last 6-month average unit price from the own database of Different Customers	Compare the unit price deviation mentioned in point 1 and 2 , raise alert.	Both
Dual Use Goods and Restricted items		Check the proposed product (H.s code/name/both) in DUG and restricted items and raise alert	Both
Payment to Third country other than the exporter/importer's country.		Compare the exporter country and payment receiving country & raise alert.	Post Pre- should be done in transaction module
TTP Violation report- numerical values	If actual transaction exceeds TTP in a particular month above a certain threshold like 50%, 100%	Raise the alert based on TTP data, actual volume and threshold value.	Post
TTP Violation: non-numerical values	Compare the item, country of Import, country of Export and other non-numerical items of TTP with actual transactions and raise alert	Show alert item wise, automated/manual test creation	Post
Alert for Restricted goods by the current Import policy.	Compare the item with restricted items list (h.s code/name)	Check the list and alert	Option 1: both option 2: Post, pre: transaction

			module
If the commission (bank) of a trade transaction exceeds threshold (4%), an alert will be generated.	Compare bank commission with invoice value		Post
If freight charges for an LC exceeds a certain threshold (5%), an alert will be generated.	Compare freight charge with Lc value over a threshold like 25%	Raise alert and create case	Option 1: both option 2: Post, pre: transaction module
If the destination/origin country, is situated in a land locked county an alert should be generated for further assessment of full voyage of the vessel.	In case of sea shipment: Compare the port of loading (Import), port of discharge (Export) country with land locked country list.	Raise alert, case creation and manual case creation	Option 1: both option 2: Post, pre: transaction module
If LC is overdrawn up to a certain threshold (10%), an alert will be generated		Compare Documents value and LC available value for presentation	Post
If LC is opened in round figures up to 5 digits, an alert will be generated	If LC value is rounded up to 5 digit ,	Taise alert	Option 1: both option 2: Post, pre: transaction module
If Bill of lading is future dated or within 10 days from present date, an alert will be generated	List all bill of lading with future date	List & raise alert, automated and manual case	Post Pre-transaction is subject to integration can be restricted in transaction module



In case of Import LC, if port of loading doesn't match with the country from which goods are being imported, then it will give an alert	Port of Loading country and country of origin, beneficiary country different	As it is usual practice, raise alert only above a threshold like USD0.5 Mn	post
The volume of purchases and/or imports grossly exceeds the expected sales amount.		Recommended as credit monitoring alert	
A single bank account is used by multiple businesses.	Customer ID and Operative A/C mismatch	Compare the operative account used with the customer ID of the transaction	Post
The exporter doesn't receive money from the buyer, but from someone else who pays on behalf of the buyer.	Ordering Customer is not buyer	Comparing , raising alert: automated and manual	
Funds are received/transferred for import/export, and the ordering customer/beneficiary is an MSB.	Ordering Customer/beneficiary is MSB	List matching and alert, automated and manual	Post
Media reports that the account holder is linked to a known terrorist organization or engaged in terrorist activities.	Adverse news checking as part of sanction screening. Customer level check and transaction level alert	Automated as well as manual test cases.	
Beneficial owner of the account is not properly identified		Recommended for General Banking	

Light Displacement Tonnage and Deadweight Tonnage certificate of the vessels which indicates weight of the loaded goods and miss-matching with BL.		Manual Test cases	Both
Custom Procedure Codes (CPC) miss-matching with Bill of Entry.		Manual Test cases	Post
Any involvement of Frustrated Cargo/Container Issues are raised and try to get custom clearance.		Manual Test cases	Both
Any Advance ruling issues are raised and settled from ruling authority.		Manual Test case	both
Required Credit report of the seller with PI \$30000 and with Indent \$40000 are not collected.	Check the availability of credit report of the beneficiary for LCs above threshold	Raise alert and test case, automated & Manual	post
There are discrepancies between the description of goods or commodity in the invoice and the actual goods shipped.		Manual test case	
There is a lack of appropriate documentation to support transactions.		Manual test case	Both

Imported Goods or items originates from a country where there is limited production or no sources at all.	based on the item.	Raise alert based on country of Origin and product	Post
Using offshore account to settle import payment .		No data currently, will study feasibility in transaction module	
Unusual HS Code of the imported Goods.	identification of new H.S code not in our transaction database for last one year	Raise alert	Post
Incoterms DDP, CIF and CIP used in case of Private party.	For private sector importers, if the mentioned Incoterms are used	If customer Segment is Private and incoterms is one or combination of these , raise alert	Option 1.: both Option 2: post, pre-transaction to be done through transaction module
In Vessel Tracking/Container Tracking any discrepancies/sign like spoofing, Loitering and stripping.		Identify and raise alert based on pre-defined pattern	
Exports proceed Repatriation time frame expired.		Agreed to the proposed Scenario	
Invoice splitting/ multiple invoicing.		the scenario is recommended for multiple invoice import only. However, clarification is required to understand "Splitting Invoicing".	

In case of import via land port multiple land port mentioned.		The scenario is not applicable in the system as it is pre-checking requirement.	
Goods import through Israeli flag bearing vessel.		Vessel Tracking gives red flags while taking report manually from the portal ( Lloyd's ) . No system alert is possible.	
Import from which country that has attributed sanction by different stakeholder or organization.		Santions screening solution with data source can be integrated with CBS to give real time alert.	
Import from a country that is involve with war.		Vessel Tracking gives red flags while taking report manually from the portal ( Lloyd's ) . No system alert is possible.	
inconsistent staff count and trading volume	Credit report details comparison with transaction volume, relationship to be provided	Compare and raise alert	Post
Relationship with PEP/IP	PEP/IP list scanning for new, existing customer s and transaction	If there is possible match, raise alert with details, case creation	Post: for all Pre-Onboarding and new transaction
Frequently Changing ownership or signatories		recommended as part of General banking and credit monitoring	
Invoice showing significant amount of misc charges e.g. handling charges	If miscellaneous charges are higher than a certain % above invoice value	Raise alert, case creation and manual case creation	Post
Transshipment through a country for no apparent	If the container is routed through unusual route or no. of transshipment country above a	Alert based on logic as well as manual case creation	Both

reason	certain no.		
Vessel/Container number cannot be tracked through web search		For integrated vessel tracking, system based alert and for manual checking manual case creation	Both
not clearly mentioning multiple HS Code, COO and product specification in PI in case of spare parts import		Data based comparison not feasible. However an item may be kept for case creation and review	Both
Price mentioned in KG whereas in open source prices are mentioned in pieces or in sets or in dozens	First Schedule Unit and actual unit comparison.	For LC above a certain amount like 0.5 Mn , list , review and case creation.	Post
Price determination in case of capital machinery		List the LCs opened for capital machineries above a certain value like USD 1Mn and provide facilities to review , comment, case creation	Post
Refund manipulation	Beneficiary and refund initiator different for same LC/TT	Compare the both and raise alert	post
LC or TT Value below the range for which Credit report is required	LC value and credit report requirement minimum value comparison	If LC value with close to Credit report requirement minimum value Like (USD20000) by a certain % like 10 % , i.e: 18001 to 199999: raise an alert	Post
Same address of Beneficiary/ Applicant , Drawer/Drawee, Related		Compare the address of Applicant/beneficiaries and raise alert if address is same,	Both

parties/other address inconsistencies		certain % match	
Misrepresentation of quantity or type of goods imported or exported	quantity declared during opening of LC differs with quantity in commercial invoice more than (10%) and/or type of goods imported or exported differs (HS Code different in shipping documents for LC)	Compare the H.S code/item wise quantity in commercial invoice with that in LC, and raise alert if exceeds threshold like 10%	post
The Bill of lading describes containerized cargo but without container numbers or with sequential container numbers		This data not available, only manual case creation may be accommodated.	Post
Alternation of PI Information after remitting advance TT or issuing DA/DP Number		Only for case creation.	post
During Settlement , obtaining huge amount of discount on bill value from beneficiary	Get the discount amount, place a threshold (% of bill value) and compare	Raise an alert if exceeds threshold (%)	option 1. Both Option 2: Post transaction, Pre-transaction to be done in transaction module.
Different HS code found in the Bill of Entry as compared to the respective commercial invoice	Comparison between the H.S codes as per Bill of Entry (available in BB OIMS) with H.S code reported under the LC	Raise alert if there is mismatch, i.e: Bill of Entry has a H.S code not reported under LC	Post