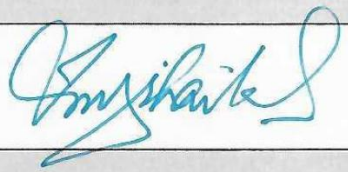
AML/CFT/CPF Program Manual

NBP KSA Branch

This document is for internal use of National Bank of Pakistan – KSA employees only. Any act of divulgence to third parties shall be viewed seriously and warrant disciplinary action.

SIGN-OFF SHEET

AML/CFT/CPF & Sanctions Program Manual		
Document Owner	Compliance Department KSA Branch	
Document Version	**4**	
Custodian	**NBP KSA Branch**	
Operating Jurisdiction	**Kingdom of Saudi Arabia**	
Last Approved	21-02-2024	
Review Frequency	Annually	
Current Approval Date	21-02-2024	
Next Review Date	21-02-2025	
Prepared by:		
Hasan Al Shehri	Country Compliance Officer	
Reviewed by:		
Imtiaz Shaikh	General Manager	
Reviewed & cleared By BCCM		
This document has been cleared/approved by the Branch Compliance Committee of Management in its 16th Branch meeting dated 21-02-2024. Please refer minutes of the meeting for committee approval and signoff.		
Approved by		
EVP/Group Head (A), Compliance Group in line with HO Global Compliance Policy, please see next sheet for sign-off		

HEAD OFFICE SIGN-OFF SHEET

REVIEWED AND CONCURRED BY IFRG

Name	Designation	Signature	Date
Moin Uddin Khan	Wing Head, Audit Inspection, Policy & Procedure Wing, IFRG, NBP, HO		20/3/2024
Syed Azhar Ali	Divisional Head, Governance & Control Div. IFRG, NBP, HO		20/3/2024.
Riaz Hussain	SEVP / Group Chief, International, Financial Institutions & Remittance Group, National Bank of Pakistan, HO, Karachi		21/3/24

REVIEWED AND CONCURRED BY COMPLIANCE GROUP

Name	Designation	Signature	Date
Sumera. Zaidi	Unit Head – International Compliance Wing (ICD), CG NBP, HO		21-03-2024
Omer Hussain	EVP – Division Head, ICD, CG NBP HO		21/3/24

APPROVED BY:

Name	Designation	Signature	Date
Muhammad Abdul Moeed	(A) GCCO/Group Chief Compliance Group, NBP, HO Karachi		21/3/24

Contents

Glossary of Terms

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CPF	Countering Proliferation Financing
CRS	Common Reporting Standard
CIF	Customer Information File
CRS	Common Reporting Standard
EDD	Enhanced Due Diligence
EU	European Union
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
KYC	Know Your Customer
NBP	National Bank of Pakistan
NGO	Non-Governmental Organization
NPO	Non-Profit Organization
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Persons
SAMA	Saudi Arabian Monetary Authority
SWIFT	Society for Worldwide Interbank Financial Telecommunications
STR	Suspicious Transaction Report
TBML	Trade Based Money Laundering
UN	United Nations
UNSC	United Nations Security Council
UBO	Ultimate Beneficial Owner

1 Definitions

- **An Occasional (Transient) Customer:** who does not have an existing business relationship with the financial institution and wishes to conduct a transaction through it.

- **Bank/Branch** shall be used intermittently to describe the branch in Riyadh, Saudi Arabia

- **Business Relationship**: The relationship of a continuous or specific nature that arises between the customer and the financial institution, related to the activities and services provided to him.

- **Beneficiary**: A natural or legal person who benefits from the business relationship with the financial institution.

- **Beneficial Owner**: A natural person who owns or exercises effective final direct or indirect control over the customer or the natural person on whose behalf the transaction is conducted or over the financial institutionor any other legal person.

- **Customer**: A person who does - or begins to do - with the financial institution any of the following actions:
  i. Arranging or conducting a transaction or business relationship or opening an account forhim.
  ii. Signing a transaction, business relationship or account.
  iii. Allocate an account under a transaction.
  iv. Transferring an account or rights or obligations under a transaction.
  v. Authorize him to conduct a transaction or control a business relationship or an account.

- **Correspondent Relationship**: It is the relationship between a correspondent financial institution and a recipient institution through an account or any other services connected to it, such as cash management, international financial transfer, check clearing, foreign exchange services, trade finance, liquidity management and short-term lending. This includes the correspondent relationship created for securities transactions or money transfers.

- **Due Diligence Measures**: The process of identifying or verifying the information of the customer or the beneficial owner, which enables the financial institution to assess the extent of its exposure to risks.

- **Enhanced Measures**: The financial institution takes additional measures when the risks of money laundering and terrorist financing are high. The additional measures include taking enhanced due diligence measures to identify and verify the customer or beneficial owner, take additional control measures and take any other measures or procedures that the financial institution determines in its policy and procedures.

- **Economic resources:** Are assets of any kind, whether tangible or intangible, movable or immovable, actualor potential, which may be used to obtain funds, goods or services, including but not limited to equipment, furniture, fittings and fixtures and other items of a fixed nature; vessels, aircraft and motor vehicles; inventories of goods; art; jewelry; gold; oil products, refined products, modular refineries and related material including chemicals and lubricants; minerals, or timber or other natural resources; arms and relatedmaterials, raw materials and components that can be used to manufacture improvised explosive devices or unconventional weapons, any types of proceeds of crime, including from the illicit cultivation, production or trafficking of narcotic drugs or their precursors; patents, trademarks, copyrights and other forms of intellectual property, internet hosting or related services.

- **Funds**: Assets, economic resources, or property of whatever value, type, or method of possession - whether material or immaterial, movable or immovable, tangible or intangible - and papers, documents, instruments, transfers and letters of credit of whatever form, whether inside or outside the Kingdom. This includes the electronic or digital systems, bank credits that indicate ownership or interest in them, as well as all types of commercial and financial papers, or any interest, profits, or other incomes resulting from these funds.

- **Family Members of the Political Person at Risk:** Any natural person associated with the political person at risk by blood or marriage ties to the second degree of kinship.

- **Monitoring Process**: Follow-up of all transactions carried out by the customers of the financial institution or the occasional beneficiary _ (transient) customer _ or the employees of the financial institution, with the aimof monitoring and detecting any abnormal transactions.

- **Person:** Includes any natural or legal person.

- **Person Close to the Political Person at Risk**: Any natural person who shares the benefit with a political person at risk through a real partnership in a legal entity or legal arrangement or has a close business relationship with him, or is a beneficial owner of a legal moral entity or legal arrangement effectively owned or controlled by a political person at risk.

- **Preventive Measures**: All measures, procedures and controls taken by the financial institution to mitigate the risks of money laundering and financing terrorism and proliferation of weapons.

- **Reliable Source**: It is the source originating information or data that the financial institution relies on to identify the customer.

- **Records**: Papers and documents, paper and electronic reports related to operations, business relationship, commercial and monetary transactions, whether local or foreign, including papers and documents obtained under enhanced / mitigated due diligence measures and any documents that contribute to the interpretation of the financial, commercial and monetary operations.

- **Suspected Transactions**: An operation for which a financial institution has reasonable grounds to suspect its connection with a money laundering crime, terrorist financing, predicate crime or crime proceeds, including an attempt to conduct the operation.

- **Simplified Measures**: The application of preventive measures in a mitigated and simplified manner consistent with money laundering and terrorist financing risks posed by the customer or the beneficial owner or the business relationship. It includes the adoption of simplified due diligence measures to identify and verify the customer, the application of a simplified method of control, and taking any measures or other simplified procedures specified by the financial institution in its policy and procedures.

- **Shell Bank**: A bank or financial institution registered or licensed in a country and that does not have a physical presence in it and not affiliated with a financial group subject to regulation and supervision.

- **The General Department of Financial Investigations**: A national center that receives reports, information and reports related to money laundering, terrorist financing crime, predicate offenses or proceeds of crime in accordance with the Anti-Money Laundering Law and its executive regulations and the Combating Terrorism Crimes and their Financing Law and its executive regulations.

- **Transaction:** Includes any disposition of funds, properties, cash or in kind proceeds including but not limited to depositing, withdrawing, transferring, selling, purchasing, loaning, committing, extending of credit, mortgaging, gifting, financing, or exchanging of funds in any currency, whether in cash or checks, payment orders, sticks, bonds or any other financial instruments; or using safe deposit boxes and any other disposition of funds.

- **The Person Who Acts on Behalf of the Customer**: The person legally authorized to carry out or initiate any of the acts that the customer may practice, such as the authorized person or the legal agent.

- **The Political Person at Risk**: The person assigned to higher public duties in the Kingdom or in a foreign country, or higher administrative positions or a position in an international organization, this includes the following positions or jobs:
  (A) Heads of state or government, senior politicians or governmental, judicial or military officials, chief executives of state-owned companies, and senior officials of political parties.
  (B) Heads and directors of international organizations, their representatives, members of the board of directors, or any similar position.

- **The Transaction**: Includes every disposal of money, property, or cash or in-kind proceeds. It includes, but is not limited to: deposit, withdrawal, transfer, sale, purchase, lending, exchange, loan or extension of a loan, mortgage, gift, financing or transfer of funds in any currency, cash or checks, or payment orders, stocks, bonds, or any other financial instruments, use of safes and other

forms of safe deposit, or any other disposal of funds.

- **The National Address**: The public residence of a natural or legal person, unless the person chooses a private address to receive notices, notifications, and the like. The address of the public or private residence - as the case may be - prepared by Saudi Post is an approved address that has all the legal effects.

- **The Third Party**: The entity that the financial institution uses to implement the due diligence measures, provided that it shall be another financial institution or any of the owners of the designated non-financial business and professions.

- **Wire Transfer**: A financial transaction conducted by a financial institution on behalf of the transferor, through which a sum of money is sent to a beneficiary in another financial institution, regardless of whether the transferor and the beneficiary are the same person.

2 Introduction

Money Laundering involves taking criminal proceeds and disguising their illegal source in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities. Simply, money laundering is the process of making dirty money looks clean. According to the Financial Action Task Force (FATF) crimes such as illegal arms sales, narcotics trafficking, smuggling and other activities of organized crime can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits, creating the incentive to "legitimize" the ill-gotten gains through money laundering. The threat of trafficking in drugs, arms, refugees, kidnapping for ransom, terrorism, etc. has spiked in recent years thereby spread black money among the various segments of the society. To curb ever-increasing risk of ML/TF/PF menace, efforts have been made by the local & international regulatory bodies to spread awareness and lay down controls' framework. Regulatory institutions have devised & enforced AML/CFT/CPF framework by means of issuing robust regulatory guidelines, independent examinations & monetary sanctions in case of breaches observed for the regulated entities/banks.

3 Scope

This Manual includes procedures have been prepared on the basis of National Bank of Pakistan Global AML /CFT Policy 2023. This Manual aims to provide procedural guidelines about the measures and obligations set out under the FATF Recommendations, SAMA's AML CFT Regulations, SBP AML/CFT/CPF & TBML Regulations as well as "Customer Due Diligence for Banks" and "Core Principles for Effective Banking Supervision" set out by Basel Committee on Banking Supervision while keeping intact the compliance of "Anti-Money Laundering Laws and Regulations."

4 Objectives

The objective of this manual is to explain possible ways of money laundering, terrorist financing, proliferation financing, trade-based money laundering through banking channel, associated risk and measures to combat them at bank level. This manual will also aid bank and its stakeholders to achieve the following purposes:

- Specifying the requirements of regulatory framework and control measures that are needed to be undertaken by the bank in various situations;
- Enable bank to ensure that only legitimate and bona fide customers are on boarded and maintaining relationship with the bank;
- Enable bank in implementing processes, controls & governance framework to effectively mitigate the ML/TF/PF & TBML risks posed by various type of customers while using products and services offered by the bank;
- Ensure that appropriate controls are in place for Customer Due Diligence / Enhanced Due

Diligence((CDD/EDD), sanctions screening, transaction monitoring, for detecting and reporting of suspicious activities, coordination & correspondence with LEAs etc. & reporting of fraud cases in accordance with applicable laws, regulations, policies & procedures;

- Necessary measures have taken by the bank to ensure that bank staff is adequately skilled, trained and with hands on experience with relevant regulatory requirements, Bank's policies & procedures.

5 Role as a Prudent Banker

The NBP Riyadh Branch is responsible to make sure that its employees are equipped, skilled and knowledgeable from relevant controls perspective. Employees should be well versed with the policies; procedures & relevant regulatory requirements & in spirit should follow the same in their day-to-day activities. Roles and responsibilities majorly comprise of the following:

- Identifying and verifying customers when establishing relationships, opening accounts, or dealing with walk-in customers;
- In line with the relevant regulatory/procedural requirements review existing customer's Information during reasonable intervals and update the same wherever necessary;
- Ensuring that information for underlying customer remain current through best effort basis;
- Ensuring that banking services are not being used by designated and proscribed individuals/entities directly or indirectly;
- Monitoring relationships on an ongoing basis & escalate or report STRs where suspicion established

6 Communications with Employees

There will be regular communication among Compliance Head / Manager Compliance and relevant staff about AML/CFT, other issues & regulatory updates, since clear communication is extremely important for establishing effective compliance culture across the bank.

7 Applicable Laws and Regulations

This manual is based on NBP's Global AML/CFT/CPF & Sanctions Policy, which is applicable to the bank along with regulations issued by Saudi Arabian Monetary Authority (SAMA) and State bank of Pakistan (SBP), some of which are mentioned below. The bank will comply with higher of the two standards.

- SAMA Anti-Money Laundering & Combating Terrorist Financing Guide
- Anti-Money Laundering Law of KSA and its Implementing Regulations
- Combating Terrorism Crimes and their Financing Law of KSA and its Executive Regulations

- Anti-Money Laundering Law
- Combating Terrorism and Financing of Terrorism Law
- Implementing Regulation to the AML Law
- Implementing Regulations of the Law of Combating Terrorist Crimes and its Financing
- Principals of Compliance with Islamic & Commercial Banks in Kingdom of Saudi Arabia
- SBP AML CFT CPF Regulations
- SBP Framework for Managing Risks of Trade Based Money Laundering and Terrorist Financing

The Bank and its employees are expected to comply with legal and regulatory requirements that are mentioned throughout this document. Failure to comply could have serious implications for the dealing officials as well as the bank.

8 KSA AML LAW Article 25

Without prejudice to any stricter sanctions and subject to the procedures provided for in other laws, if the supervisory authority finds that FIs, DNFBPs, and NPOs or any of their directors, board members, executive or supervisory management members failed to comply with any provision of this Law, its Implementing Regulation or relevant decisions or circulars, or any violation referred from other competent authority, the supervisory authority may impose one or more of the following measures:

- Issue a written warning;
- Issue an order to comply with a specific instruction;
- Issue an order to provide regular reports on the measures taken to address the identified violation;
- Impose a monetary fine of up to 5.000.000 riyals per violation;
- Ban individuals from employment within the sectors for which the supervisory authority has competences for a period to be determined by the supervisory authority;
- Restrict the powers of directors, board members, executive or supervisory management members, and controlling owners, including appointing one or more temporary controllers;
- Dismiss or replace the directors, members of the Board of Directors or of executive or supervisory management;
- Suspend, restrict or prohibit the continuation of the activity, business or profession or of certain business activities or products;
- Suspend, restrict or revoke the license

9 KSA National Risk Assessment

Saudi Arabia conducted two separate national assessments for the money laundering (ML) and terrorism financing (TF) risks. The Anti-Money Laundering Permanent Committee (AMLPC) is responsible for conducting the ML NRA and the Permanent Committee for Counter Terrorism (PCCT) for the TF NRA.

- The NRA's main objectives were to improve Saudi Arabia's AML/CFT regime by:
    - Assessing the ML/TF risk, it faces.
    - Evaluating the effectiveness of its risk mitigation strategies.
    - Prioritizing its risk mitigation activities.
    - ·Making and justifying decisions about limiting AML/CFT coverage for low-risk sectors and products.

The NRA identified threats, vulnerabilities and consequences. In addition, the regulated sectors that are FIs, DNFBPs, legal persons, and NPOs, were assessed in ML/TF risk.

9.1 Risks and General Situation

1. Saudi Arabia faces a high and diverse risk of terrorism financing, linked to terrorism committed both within Saudi Arabia, and to countries experiencing conflicts within the region. The risk of terrorism and terrorist financing within Saudi Arabia is linked to the presence of cells of Al Qaeda, ISIS, affiliates, and other groups. The number of foreign fighters is high, with estimates of over 3,000 departures between January 2000 and February 2018. Saudi Arabia also faces a high risk of terrorist acts carried out in Saudi Arabian territory. 2

2. The economy of the Kingdom is dominated by petroleum activities: Saudi Arabia is the largest exporter of petroleum, and the sector accounts for 45% of GDP. Saudi Arabia is generally seen as a conservative country and an unattractive location for laundering international proceeds because of its relatively small financial and commercial sectors, limitations on direct foreign investment and participation in the corporate sector, and restrictions on access by foreigners to the financial and nonfinancial markets. The financial sector and DNFBP sectors in Saudi Arabia are relatively small, and primarily serve domestic customers. The remittances sector is an exception: over a third of the resident population in Saudi Arabia was born outside the Kingdom, which has the second highest total outflows of remittances in the world after the US, approximately $38.8bn for the year to April 2017.

The overall proceeds of crime generated in Saudi Arabia are estimated to be approximately USD 12 - 32 billion; based on IMF and UNODC research on the proceeds of crime as a proportion of GDP. This range is consistent with Saudi Arabia’s risk profile and the Saudi NRA for ML. Saudi authorities estimate the main proceeds generating crimes in Saudi Arabia to be illicit trafficking in narcotics, corruption, and counterfeiting and piracy of products. Between 70 and 80 per cent of domestic proceeds of crime are estimated to flow out of the Kingdom, while the balance remains in the country

10 AML / CFT (Compliance) Department

10.1 Transaction Monitoring

FCM (Financial Crime Module) was implemented in NBP Riyadh in 2021 which is based on pre-set scenarios. The TMS monitors post facto transactions according to look-back period and threshold defined

on each scenario. These scenarios are based on the Banks business requirement and are approved by the Branch's Compliance Committee of Management (BCM), which is also responsible for approving modifications/fine tuning them. These scenarios and their thresholds are subject to periodic review.

10.2 Execution of Transaction Monitoring

NBP- Riyadh monitors and ensures effective Transaction Monitoring at each stage of the process chain:

The alerts are generated in 'Batch Alert Manager' on Temenos T24 module FCM on both direct customers of NBP Branch as well as external parties. Since the monitoring system will generate alerts based on triggering activity (thresholds/scenarios/look back period) CCO must consider available KYC/CDD information and other pertinent information to determine whether the activity is considered potentially unusual.

The alerts to be reviewed and cleared in accordance with standard operating procedure of transaction monitoring as per Annexure -A.

During the transaction monitoring process, the Branch staff may reach out to the CCO for guidance on, and approval to make changes to customer profiles. The CCO will review the proposed change and confirm or deny changes to customer profiles or risk ratings, which will be fully documented and uploaded to the customer profile following approval by BCCM.

10.3 Identification of Unusual Activity

i. Identification by Employees

During the course of day-to-day operations or Periodic / Trigger reviews, employees observe unusual or potentially suspicious transaction/activity. Bank has implemented appropriate training, policies, and procedures to ensure that personnel adhere to the internal processes for identification and referral of potentially suspicious activity.

ii. Law Enforcement Inquiries

These may be written requests for information issued by the regulatory and/or law enforcement authorities

to obtain the following:

- KYC Information
- Financial / Transaction Records
- Telephone and Electronic communications records

The Branch takes appropriate measures to respond to such inquiries in a timely manner and ensures the confidentiality of information requested and shared.

10.4 Resolution and Enhancement

i. STR Decision Making

After completing thorough research and analysis in case of suspicion, findings are forwarded to Country Compliance Officer who will have the authority to make the final STR filing decision.

ii. STR Completion and Filing

The Suspicious Transactions Register is required to be maintained to offer proper record of all those transactions that have been screened out as "Suspicious.". When a suspicious transaction has been identified, the matter should be dealt quickly and professionally. STRs are required to be filed electronically along with all supporting information to General Directorate of Financial Investigation Unit (FIU) by the Compliance Department on fiu@sama.gov.sa. The report shall include the following at minimum;

a) The account statement or transactions carried out under the contract for a period of six months.
b) Documents obtained to apply due diligence measures.
c) A technical report examining the account or contract subject of suspicion.

10.5 Post-STR Practices

After filing a STR, if the suspicious activity continues over a period of time, the Branch decides if the relationship has to be retained, then appropriate enhanced measures are taken to manage the risks of these accounts. These enhanced measures include subjecting the accounts to increased scrutiny, obtaining compliance and/or senior management approvals prior to executing further transactions and reviewing the risk classification and/or further business relations with the customer. Bank also takes into account any ongoing cooperation with law enforcement agencies in deriving the course of action, and ensures that their actions do not tip-off the customer.

11 SAMANET/ TANFEETH Queries

Bank will adhere to the requirements of SAMANET Queries received directly or through "Tanfeeth" Following actions will be required to be performed by compliance function on receipt of such queries;

- Screen the request against existing customer database. If there is positive or no match, respond to the query accordingly.
- In case of positive match, perform the desired action / Task in Core Banking System of the bank and respond to SAMA accordingly.

- Maintain and Update the SAMANET List as per instructions received from SAMA on daily basis
- Maintain confidentiality of the information as per SAMA requirements.

12 SSU Queries

Bank will adhere to the requirements of SSU Queries received from SAMA, according to the SSU procedures for handling SSU inquiries. Following actions are required to be performed by compliance function on receipt of such queries;

- Screen the request against existing customer database
- If there is positive or no match, respond to the query accordingly
- In case of positive match, perform the desired action directed by SSU and respond to SAMA SSU Unit
- Maintain and Update the SSU & internal lists as per instructions received from SAMA
- Maintain confidentiality of the information as per SAMA Requirements

13 Know Your Customer

The inadequacy or breaches of KYC standards can subject bank to serious customer and counterparty risks, especially reputational, operational, legal risks. It is worth noting that all these risks are interrelated.

13.1 Know Your Customer Guidelines

13.1.1.1 Customer Profiling

Customer profiling is a way to create a portrait of customers to help make risk decisions concerning our client onboarding and continuation of service. Factors such as customers' background, country of origin, public or high-profile position, linked accounts, business activities or other risk indicators are considered while profiling customers.

The main purpose of profiling is to understand customer, particularly customer's source of wealth, beneficial ownership and financial behavior in the account in order to highlight any unusual activities in his or her account/conduct.

When the branch is approached to open an account, due diligence will be carried out by asking the prospective customer to fill the Account opening form and later the account opening officer will further perform due diligence as per in line with branch procedures.

13.1.1.2 Due Diligence, Controls and Precautions

The Account Opening Officer will exercise due diligence, precautions and vigilance on KYC measures adopted to counter the money laundering risks according to the type and level of risks posed by the customer, the beneficial owner or a specific business relationship in the following cases:

- Before commencing the establishment of a new business relationship.
- Before conducting a transaction in the interest of a natural or legal person who has no business relationship, whether this transaction is carried out one time or multiple times; so that such transactions appear to be related to each other.
- When money laundering or terrorist financing is suspected.
- When doubts about the validity or adequacy of previously obtained customer' data.
- When the customer executes a transaction that is not in line with his behavior or data.

Due diligence measures shall include, at a minimum, the following:

- Identifying the identity of the customer and verify it by using documents, data or information from a reliable and independent source like government agencies according to the following:

  - **Natural person**: Obtain the person's full name, nationality, date and place of birth recorded in National Identity Card/ Iqama/ Passport, in addition to obtaining National Address of the Business / Residence, and source of income from Salary Slip/ or proof of ownership of a business, Personal Email Address (as applicable) Nationality – Resident/ Non-Resident Status, FATCA/ CRS Declaration, wherever required.

  - **Legal person:** Obtain the person's name and legal form, proof of incorporation, the powers that regulate and govern the work of the legal person or the legal arrangement, the names of all managers and senior administrators, the registered official address, the place of work if it is different, the sources of the legal person's revenue, expected monthly credit turnover (amount and No. of transactions), Normal or expected modes of transactions/ delivery channels, regulatory limits imposed such as: credit and debits/ deposit and withdrawals/ execution of financial transaction/ types of financial services allowed/ restricted (where advised)
- Identifying the identity of the person acting on behalf of the customer as mentioned above and obtain an authority from the customer determining the nature of the relationship between the person acting on behalf of the customer and the customer.
- Knowing and verifying identity of the beneficial owner
- Perform negative media search for information available through public databases, internet, etc.
- Understanding the purpose and nature of the business of the customer, geographies involved and expected type of counter-parties as applicable
- Understanding the structure of ownership and control on the legal customer.

The branch maintains necessary AML / CFT / PF controls and precautions in its Banking Activities in following manners:

- Customer Acceptance and Identification
- Risk Assessment (Client Onboarding, Periodic and Event Driven)
- On-Going Monitoring of Accounts and reporting where necessary
- Record Keeping

13.2 Type of Customers that NBP will not accept

As per Policy, NBP KSA shall not deal / accept following types of individuals/entities as a customer:

- Entities/persons appearing in UNSC/OFAC/EU/UN/ATA, SAMANET /SSU Block list and any other list recommended by SAMA or SBP.
- Customers who are nationals of or are resident in jurisdictions having country level embargoes.
- Unauthorized / Unlicensed money changers or any other illegal financial businesses including individuals known/identified as using their accounts to engage in Hundi / Hawala transactions.
- Gamblers, bookies, casinos and other businesses associated with gambling.
- Anonymous or fictitious accounts and numbered accounts
- Shell banks
- Unregistered Arms-related business
- Bearer share based entities
- Accounts where the customer is acting on behalf of another customer to open an account Where the branch is not able to satisfactorily complete required CDD measures or UBO identification
- Client or business segment black listed by the Bank or by the Regulators
- Government officials willing to open government's accounts in their personal name Institutions whose AML controls are considered inappropriate or insufficient.

13.3 Customer Identification and Verification

13.3.1 Customer Acceptance

The customer acceptance applies to all relationships regardless of which business they fall under. All businesses must adhere to following customer acceptance guidelines when establishing new relationships, without waiving statutory requirements stipulated by SAMA or other applicable regulatory requirements. NBP KSA Branch employees must verify all customers' data when entering new relationship or reviewing pre-existing relationship.

13.3.2 General requirement applicable for all relationships

Bank will accept customer on whom Bank is able to apply appropriate KYC procedures: Obtain complete information from the customer. It should be ensured that the initial forms taken by the customer are filled in completely. All photocopies submitted by the customer are verified against the relevant electronic database in KSA or overseas, in compliance with SAMA regulations or restrictions.

Staff should apply due diligence procedures for all customers, beneficial owners and actual beneficiaries. Do not accept customers' identity matched with the proscribed person list: Every new customer shall be checked against the sanctions lists and make sure the new customer's do not match with any person identified in the sanctions lists.

The Bank shall diligently (apply enhance due diligence) while accepting customers of special categories

like Charities, Politically Persons at risk, Customer from high-risk countries or customers belonging to countries where corruption/fraud level is high. The branch should use all the available information/ resources to ensure compliance with customer due diligence requirements such as documents provided by customers and information available to the public.

The Bank shall update the customer identification information periodically (based on the risk rating of each customer), and taking into consideration the event of any doubt about the identity information or alarm raised on his/her transaction activities.

In case of an account/ relationship of an entity with abbreviated name or title, bank shall satisfy themselves that the subject name/ title is in accordance with the constituent documents of the entity. Account/ relationship shall not be allowed in abbreviated name in cases where entity has its complete non-abbreviated name in their constituent document.

13.4 Identity Verification of Customer (Natural Persons & Beneficial Owners)

a. As per AML / CFT Guide issued by SAMA

To apply the risk-based approach, the bank will verify the identity of the beneficial owner or anyone controlling the business relationship. Beneficial owner(s) cannot be a legal person, but rather is a natural person who owns or controls the legal person directly or indirectly.

The bank will determine the identity of the natural person who owns or controls (25%) or more of the legal person's shares, and will verify their identity, taking into account that the natural person who owns the controlling share (25%) may not necessarily constitute the beneficial owner."

The Bank will verify identities of the customers (natural persons) and in case of legal persons, identities of their natural persons from relevant authorities or where necessary using other reliable, independent sources and retain on record copies of all reference documents used for identification and verification.

b. Negative Verification / Unverified Relationships

In case of Negative verification of identity or any other documents provided by customer becomes unverified from a reliable source, or similarly, if the physical visit report (where applicable) to open an account turns negative, the relationship will not be opened or discontinued and bank staff will immediately report the account as an Internal STR to Compliance Department.

c. Accounts with Abbreviated Name

In case of an account/relationship of legal entity with abbreviated name or title, the branch/business unit shall satisfy itself that the subject name/title is in accordance with the constituent documents of the customer entity. Any account/ relationship shall not be allowed in abbreviated name in cases where entity has its complete name (non-abbreviated) in their constituent document.

d. Accounts without Valid Identity Documents

Bank shall block all accounts without valid Identity Document (after serving one-month prior notice) for all debit transactions/withdrawals, irrespective of mode of payment, until the subject regulatory requirement is fulfilled. However, debit block from the accounts shall be removed upon submission of valid identity document and verification of the same.

e. Trade Finance Customers

Bank undertakes KYC/ CDD measures of asset side/trade finance customers in the same manner as required for deposit products as mentioned in the relevant sections of this manual and ensure monitoring of such relationships with regard to ML/TF/PF risks.

13.5 Risk Assessment

Part of the Know Your Customer / Customer due Diligence (CDD) process assesses the risk a customer poses to the bank. KYC is a continuous process not a one-time assessment of a customer. Customers are assessed in different stages of their relationship with the bank.

13.6 Account On-boarding

After the customer is passed through the Account onboarding process and when the decision is made to onboard the customer based on the review of documentation, the CDD/Risk Assessment workflow is executed for detailed risk assessment of the customer based on defined parameters.

13.7 Periodic Review

Based on the customer's risk category, the next review date is defined. If the customer poses high risk to the bank, then the customer will be reviewed more often compared to medium or low risk customers. The review period is defined later in this manual based on the ranges of the Customer Risk score. KYC also checks the behavior detection results for a customer based on the criteria defined and assesses the customers which match the criteria.

13.8 Risk Assessment Parameters

The risk assessment parameters are defined in the automated CRP (KC+) which calculates the risk, based on the following risk factors;

Risk Factor	Sub Sets
Demographic	Industry
	Target
	Segment
	Customer Status

Geographic	Nationality
	Residence
Product	Current Account
	Saving Account
Transaction Profile (SAR)	Monthly in & Out (Individual)
	Monthly in & Out (Corporate)
Over Riding Factors	High Risk Business, PEP, DNFBPs

Further details on risk scoring parameters are available in the customer risk assessment document.

14 Enhanced Due Diligence Measures

For all the customers classified as "High Risk" Following enhanced measures will be taken and business relationship:

- Bank will Obtain information about the customer's job, activity or profession and verify the validity of the information.
- Bank will Determine and identify the source of funds / income and Wealth at the beginning of the dealing and when performing transactions during the period of the dealing, and verify the validity of the data and information.
- Obtain information about the volume of the customer's assets and transactions.
- Conduct field visits and retain evidence to verify the nature of the customer's business activities.
- Obtain any additional documents or information to identify the customer.
- Obtain the approval of senior management of NBP Riyadh Branch to commence or continue the business relationship or execute the high-risk financial transaction.

15 Customer Risk Profiling

In compliance of regulatory framework with respect to risk-based approach, bank understands the risks associated with its customers, products offer, delivery channel, technologies, different categories of employees, geographies etc. While assessing customer risk, following factors can be used in the bank;

- Customer type
- Product type, industry
- Country of residence
- Age of business/vintage
- Residence status (Resident/Non-Resident)
- Business type
- Geographical Demographics (Nationality/Branch location to address transnational risk factor)
- Occupation
- Industry

Each customer should be risk rated based with the composition of aforementioned criteria. This information is used by the bank to determine the appropriate risk of the customer. Certain categories of customers may pose a perceived higher risk. Examples of such customers include politically exposed persons (PEPs),

Money or value transfer Services providers, Correspondent-banking customers, NGOs/NPOs/Trust/Societies etc.

The objective of Customer Risk Profiling is to establish a consistent, measurable, and appropriate criterion to follow for determining the risk profile of the customer and required level of due diligence for various customer types. This above shall apply to entire customer base of NBP (i.e. fresh onboarding and existing customers) broadly classified under the following categories:

a) Individuals (including Sole Proprietors, Self Employed Professionals);
b) Legal entities (including Government Institutions, Joint Stock Companies, Trusts/NGOs/NPOs etc.); and
c) Financial Institutions (including Other Banks)

The Bank uses FCCM-KYC/CDD system-based model for risk assessment, which calculates risk rating of the customer based on parameter mentioned above.

16 Enhanced Due Diligence on High-Risk Customers

16.1 Politically Exposed Persons (PEPs)

There is always a possibility, especially in countries where corruption is widespread, that PEPs abuse their public powers for their own illicit enrichment through corrupted means, receipt of bribes, embezzlement, etc.

Politically exposed persons (PEPs) generally have a higher risk of ML/TF when operating in countries characterized
by higher levels of bribery and corruption.

PEPs can pose higher money laundering, corruption and reputation risks to the Bank due to their position of political power or influence. Therefore, enhanced ongoing monitoring of business relations with the customer or beneficial owner is required when identified as PEP, close associate and family member of PEP.

1. **The Political Person at Risk**; the person assigned to higher public duties in the Kingdom or in a foreign country, or higher administrative positions or a position in an international organization, this includes the following positions or jobs;
    - Heads of state or government, senior politicians or governmental, judicial or military officials, chief executives of state-owned companies, and senior officials of political parties.
    - Heads and directors of international organizations, their representatives, members of the board of directors, or any similar position.

2. **Family Members of the Political Person at Risk:** Any natural person associated with the political person at risk by blood or marriage ties to the second degree of kinship.

   Person Close to the Political Person at Risk: Any natural person who shares the benefit with a political person at risk through a real partnership in a legal entity or legal arrangement or has a close business relationship with him, or is a beneficial owner of a legal moral entity or legal arrangement effectively owned or controlled by a political person at risk.

3. **Non-Individual PEP:** An entity is deemed to be a PEP, if the said entity is owned or controlled by an individual PEP i.e., if the individual PEP fulfills one or more of the following conditions:
   a. Has 10% or more shareholding or voting rights in the entity, as the case may be;
   b. Is an executive director or supervisory board member of the entity; or

   Exercises significant influence or control over the management affairs of the entity even in the absence of (a) or (b).

   To avoid any doubt, an entity owned by the government even with any PEP linkage (such as having an individual PEP as a director, authorized signatory etc. in the entity by virtue of his position) should not be considered as non-individual PEP.

4. **Foreign PEP and Local PEP:** There is no difference in the treatment between an individual PEP who is opening an account in a different country from where he held his office (foreign PEP) and an individual PEP who is opening an account in the same country as where he held his office (local PEP). For the purpose of the Bank's risk assessment, both foreign PEPs and local PEPs will be treated as PEPs.

   For example, if the UK Prime Minister wishes to open an account with the Bank in Singapore, he will be classified as PEP in Singapore.

5. **Declassification of PEP:** An individual PEP (Other than Politicians) will remain PEP after getting de-associated from their position as per SAMA regulations. Therefore, any such client who has previously held prominent public function but is no longer holding a prominent public function will be declassified from PEP status, if he does not engage in any public function or political activity.
   - Where a client is an immediate family member or a known close associate of a prominent public function holder, and the prominent public function holder is dead, then particular family member/known close associate may be declassified from the PEP status. De-classification procedure will require senior management approval as similar to PEP on-boarding procedure.
   - Non individual PEP will cease to be a PEP, if it is no longer owned or controlled by an individual PEP. To avoid doubt, where a client is wrongly classified as PEP due to a wrong name match and there is no prominent public function linkage, then the client must be correctly classified by removing the PEP status.
   - PEP declassification will be made by branch after taking approval from the senior management of the bank based on the recommendation of AML Manager. It must be ensuring by branch/regional management team that the reasoning of PEP declassification is true and duly verified.

6. **Adverse Media & PEP**: Adverse media or negative news is the information available in the public domain that suggests that there may be a reputation or financial crime risks in having or continuing a banking relationship with underlying individual or entity. This can include contents related to tax evasion, corruption, fraudulent activities or any such other predicate offence. When reviewing the PEP assessment form provided by the business team/branches, CG will perform following steps:
    - Conduct Accuity or Google Search against the PEP
    - Review the first 20 items of the search result.
    - In case of any potential match found, clarity should seek from concern business team/branch with endorsement from Senior Management

16.2 NGO/ NPO/ CHARITY/ TRUST ACCOUNTS

- Bank shall conduct EDD (including obtaining senior management approval) while establishing relationship/ execution of financial transaction with NGOs/ NPOs, Charities and Trusts, when the risks are higher, to ensure that these accounts are used for legitimate purposes and the transactions are commensurate with the stated objectives and purposes.
- Bank will not allow usage of personal accounts of their customers for solicitation and collection of donations/charity.

16.3 Local Money Service Business/Exchange Companies

- Money exchange companies and companies of similar nature will be treated as high-risk customer and will thus be subject to EDD.
- The background of the institution is clean (Which can be establish through open-source information like Google or with AML utility like FCM Screening).
- The directors, senior management & UBOs have good reputation–no blacklisted persons or entities are involved which may be assessed through negative lists available on intranet to ensure that these persons are not affiliated with any Designated Person/Proscribed Person

16.4 High Risk Businesses

- The Branch has a regulatory and legal obligation to conduct CDD and know its customers while understanding the nature of the business that is being conducted with the Bank and this applies to every type of a customer.
- The nature of the business that a customer expects to conduct should be ascertained at the time of account opening and later the time of periodic review. This enables the bank to judge whether the customer's transactions are in line with the recorded profile, or else unusual transactions carried out raise concern of possible suspicion that involves criminal money.

- In the DNFBP sector, real estate dealers and jewelers pose high inherent vulnerability due to their limited regulatory regime. Bank accounts of these DNFBPs may also serve as an avenue to hide funds of money launderers. The funds in their accounts may possibly come from some of their customers involved in criminal activities, therefore, the threat of such banking relationships is considered to be high.
- While opening account, branch/business units should focus on the following types of customer relationships/accounts and classify them as high risk:

    - Arms & Ammunition business (licensed only)
    - Real Estate/Vehicle/Boats/Aircraft Dealer
    - Precious Metals/Stones Dealer
    - Mining Business (Gold/Coal etc. Licensed only)
    - Lawyers, notaries, tax advisors, other independent legal professionals and accountant

16.5 Off shore corporate entities

- Offshore entities offer confidentiality to that the onshore entities cannot compete with. This available secrecy and the level of complexity is what drives much of the illegal markets offshore. Offshore companies and financial dealings in another country can be used to evade regulatory oversight or tax obligations & therefore this requires for the banks to exercise greater level of due diligence & scrutiny when establishing relationship with such entities.
- Keeping in view the complications to identify, verify and ascertaining business activity/UBO of underlying entities, these entities shall be treated as high risk. Moreover, bank shall consider to commence relationships with such entities only on case-to-case basis and shall undertake Enhance Due Diligence (EDD) measures accordingly.

16.6 High Risk Countries

High-risk jurisdictions/countries are identified with serious strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation Accordingly, in line with the UNSC Resolutions, guidelines provided by FATF, SAMA and sanctions imposed by OFAC & EU are reviewed periodically.

16.7 Approval of High-Risk Accounts

The Bank shall apply the following procedures and measures:

- Classifying all relationships, the bank makes with entities relating to countries of which warning bulletins were issued (government relationships, correspondent banks relationships, companies or individuals' commercial relationships, resident customers relationships, etc.) at risks level consistent with the nature of those businesses, relationships and the risks level of these countries.

- In case of new/existing relationship from high-risk category, the compliance department should be notified and then obtain the necessary approvals from the GM & Compliance Manager.

All High-Risk Account must be approved by GM and Compliance Manager.

16.8 Approval Matrix

Type of Risk	Recommendation	Approval
Low Risk	Operation Manager	GM
Medium Risk	Operation Manager	GM
High Risk	Operation Manager	AML/Compliance Manager & GM

Un-acceptable Risk or Sanction Element*	Refer to the CCO/AML Manager on his/her official email ID for advice

17 Periodic Review of Accounts

Following are the frequencies for updating customer data/Information for each risk category.

Risk Category	Review Periodicity
Low	After 5 years
Medium	After 3 years
High	Annually

Bank shall not allow personal accounts of individuals to be used for business purposes. In order to verify the physical existence of business, the bank shall conduct physical verification within 10 working days of the opening of account and document the results thereof on account opening form. In case of unsatisfactory verification, the branch may consider reporting it to General Department of Financial Investigation and/or may change risk profile, as appropriate.

18 Accounts Operated by Third Parties

All accounts operated by third party need to be handled very carefully. Customer shall be interviewed and reasons for such delegation of authority, full particulars of the attorney / agent and their relationship shall be conclusively established as fair and legally defendable, to the satisfaction of the bank. All the information / reasons for delegation shall be updated in the customer's profile.

19 Government Accounts

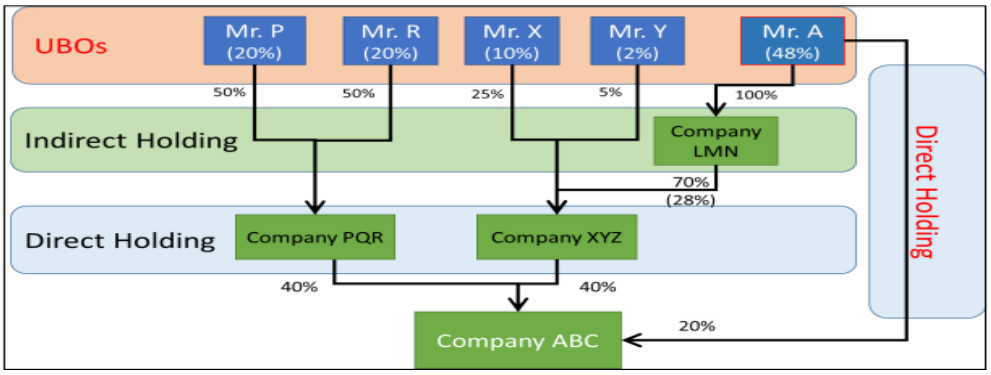
Government accounts shall not be opened in the personal names of the government official(s). The accounts shall be opened only on the production of a special resolution/authority from the concerned administrative department duly endorsed by the Ministry of Finance or Finance Department of the concerned Government.

20 Un-wrapping layers to Ultimate Beneficial Owner

Beneficial ownership identification and verification is now an essential component of the client KYC onboarding and remediation process. It is an essential element of the latest national and international AML/CFT/CPF and sanctions regulations, as well as tax compliance laws, such as FATCA and CRS.

For adopting risk-based approach to identification of UBO's either in direct / indirect ownership structure. It is responsibility of bank staff who is involved in Account opening process to identify UBO's in their ownership structure.

Below is an illustration of UBO identification concept



In above structure, the ultimate beneficial ownership is as follows:

- Mr. X 10% shareholder in ABC via company XYZ [25% of 40%],
- Mr. R 20% shareholder in Company ABC via Company PQR [50% of 40%]
- Mr. P 20% shareholder in Company ABC via Company PQR [50% of 40%]
- Mr. A is a highest shareholder with 48% (i.e. 20 % Direct in ABC + 28% via Company PQR & XYZ), hence he is an UBO.

For direct and indirect UBO, the branch must understand the ownership structure if available in complex ownership structures. There is greater risk associated with indirect ownership structure, where branch should recognize the layers of all indirect ownership and identify the UBO layers up to four and obtaining declaration from those who have 20% ownership in legal entity.

21 KYC Profile Update at the time of Dormant Account's Activation

Dormant or in-operative means the account in which no transaction has been taken place from last one year. For customers whose accounts are either dormant or inoperative and of account holder's ID is not available in bank's records, the bank may allow credit entries in such accounts without changing the status of such accounts. However, debit transactions/withdrawals shall not be allowed until the account holder produces an attested copy of his/her ID, if already not available and fulfills all other formalities for updating the KYC/CDD/EDD before activation of the account. However, transactions e.g. debit under the recovery of loans and markup etc. or any permissible bank charges, government duties or levies and instructions Issued under any law or from the court will not be subject to debit or withdrawal restriction. Branch may use

Government database(s) for activation of dormant account by customers. All inoperative/dormant accounts will be made operative after updating customer profile in core banking application and KYC/CDD/EDD forms in hard/digital form.

22 Prohibition on Use of Personal Account for Business Purposes

Branch shall not allow personal accounts of individuals to be used for business purposes except proprietorships, small businesses and professions where constituent documents are not available and the branch is satisfied with KYC profile of the account holder, purpose of relationship and expected turnover of the account keeping in view financial status & nature of business of that customer. 1st Line internal controls team will monitor all such relationships.

The Branch Manager and Branch Operations Manager primarily need to ensure due compliance in this regard while monitoring transactions conducted of such customers. In order to verify the physical existence of business or self-employment status, business unit/branches will conduct physical verification prior opening of account. In case of unsatisfactory verification, the branch should share their findings with AML staff for appropriate measures that include reporting of STR.

23 Employee Due Diligence

The bank shall develop and implement appropriate screening procedures to ensure high standards and integrity at the time of hiring all employees, whether contractual or permanent or hired through outsourcing. In this respect, HR shall inter alia invariably ensure that:

a. All employees are screened against lists of designated and proscribed individuals, on an ongoing basis, and maintain proper record of screening. Accordingly, employees shall become disqualified if they are designated/ proscribed or associated directly or indirectly with DPs/ PPs.
b. No employee is or has been convicted/ involved in any fraud/ forgery, financial crime etc.
c. No employee is or has been associated with any illegal activity concerning banking business, foreign exchange business, financial dealing and other business or employment.
d. Bank will comply with SAMA NOC required for senior management appointments.

24 Occasional Customers / Walk-In Customers

The branch does not provide any service to occasional customers/Walk-in customers. Changes to this will require update of this document.

25 Wire Transfer/Fund Transfer

The Bank does, before executing a wire transfer, obtain record the following minimum information about the originator and the beneficiary:

Originator information shall include:

- The full name of the originator;
- The originator account number where such an account is used to process the transaction or in the absence of an account number, a unique transaction number that permits traceability of the transaction; and
- The originator's address, or customer identification, or date and place of birth.
- Originator's applicable identity document number

Beneficiary information shall include:

- The full name of the beneficiary; and
- The beneficiary account number where such an account is used to process the transaction or in the absence of an account number, a unique transaction number that permits traceability of the transaction. Determine the purpose of the wire transfer and the relationship of the transferor to the beneficiary.
- The Cross- Border wire transfer shall include required and verified originator information and required beneficiary information with each wire transfer as mentioned above. However, the bank will make the required and verified originator and required beneficiary information available within three business days upon receiving a request for such information from the financial institution ultimately receiving the wire transfer or a competent authority
- For cross-border wire transfers, where the bank is processing the transactions as an intermediary bank, element of the payment chain shall ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it, and shall keep all wire transfer information including originator and beneficiary information available at the bank.
- The Bank shall complete a declaration from the customer before executing a wire transfer that includes his knowledge and familiarity that the Kingdom's regulations prohibit the transfer of funds if the remitter does not know the beneficiary (or without a legal relationship with the beneficiary or without a legitimate purpose.
- Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to several beneficiaries, the ordering financial institution shall include in the batch file the required and verified originator information; the required beneficiary information that is fully traceable within the beneficiary country; and the originator's account number of unique transaction reference number.
- The bank while receiving wire transfers from outside the Kingdom shall analyze them to;
- Identify wire transfers that lack the required information regarding the remitter or the beneficiary.
- Reject or suspend a wire transfer if it lacks the required information about the remitter or the beneficiary.
- Restricting or terminating the business relationship with the correspondent bank's if they consistently
- fail to provide the missing information.
- In the event that the identity of the beneficiary was not previously verified, the recipient financial institution shall verify his identity and keep this data as described in the section of record keeping.

The bank will not execute a wire transfer outside the Kingdom in any currency for charitable purposes, regardless of the source of funds or the beneficiary.

The bank will not receive a wire transfer from outside the Kingdom to a beneficiary in a financial institution outside the Kingdom if the wire transfer is in a currency other than the Saudi riyal (in which case purpose of the wire transfer will be described in a clear and detailed manner).

26 Correspondent Banking

In addition to the enhanced due diligence measures (as deemed necessary by the bank), Bank shall take the following measures for providing correspondent banking services:

(a) Assess the suitability of the respondent bank by taking the following steps:

(i) Gather adequate information about the respondent bank to understand fully the nature of the respondent bank's business, including the following, where available or applicable;

- Correspondent Bank's Know Your Customer (KYC) policy
- Information about the respondent bank's management and ownership
- Major business activities & customer types served
- Their geographical presence/jurisdiction (country) of correspondence
- Money Laundering prevention and detection measures/AML/CFT/CPF Regulations in place
- Condition of the bank regulations and supervision in the correspondent's country
- The purpose of the account or service
- Undertaking that correspondent banking services will not be used for payable through accounts
- Confirmation that the correspondent bank does not allow its accounts to be used by a shell bank
- Negative news searches should not reveal material negative information that is less than 3 years old. Branch can ask the applicant bank for an explanation of any negative news it determines is material

(ii) Determine from any available sources the reputation of the respondent bank and, as far as practicable, the quality of supervision over the respondent bank, including where possible whether it has been the subject of money laundering or financing of terrorism investigation or regulatory action; and
(iii) Assess the respondent bank in the context of sanctions/embargoes and Advisories about risks.
(iv) Evaluate the internal policies, controls and procedures for mitigating risks that the correspondent financial institution implements to combat money laundering and terrorist financing by preparing a questionnaire that includes the basic AML / CFT/CPF requirements and assessing whether measures are efficient or not.
(v) The Bank shall clearly understand the responsibilities of each party in the correspondent relationship from the perspective of AML / CFT/CPF.

(b) Obtain approval of senior management and Head Office, before establishing new correspondent banking relationship.

i. Where the cross-border banking services involve a payable-through account, the correspondent bank shall be satisfied that -
   - the respondent bank has performed appropriate CDD measures at least equivalent to those specified in of SAMA & SBP AML/CFT/CPF regulations on the third party having direct access to the payable-through account; and
   - the respondent bank is able to perform ongoing monitoring of its business relations with that third party and is willing and able to provide customer identification information to the correspondent bank upon request.

ii. Bank shall pay special attention when establishing or continuing correspondent relationship with banks/ financial institutions which are located in jurisdictions that have been identified or called for by FATF for inadequate and poor AML/CFT/CPF standards in the fight against money laundering and financing of terrorism.

iii. Bank shall NOT enter into or continue correspondent banking relations with a shell bank and shall take appropriate measures when establishing correspondent banking relations, to satisfy them that their respondent banks do not permit their accounts to be used by shell banks.

iv. The steps mentioned above and the approval for of On-Boarding any Correspondent is subject to clearance and approval from Head Office. (NBP-Pakistan).

27 Sanction Screening

Sanctions screening is one of the primary controls used by Bank to comply with applicable sanctions laws and regulations.

Sanctions screening involves screening parties based on their names and other associated information against applicable sanctions watch lists, as well as any internal lists maintained by NBP KSA Branch.

In addition to real-time-transaction screening and periodic name screening of customers, vendors, trade documents, and employees. NBP KSA Branch conducts screening on parties identified in the ownership structure, beneficiaries, Ultimate Beneficial Ownerships ("UBOs"), related/ controlling parties, authorized signers, associated parties, when necessary, prior to opening the customer's account. This total layer of screening provides a control to ensure that no required party's information is omitted from the process.

The Compliance Team is responsible for establishing and communicating screening requirements to ensure consistency in NBP KSA Branch's sanctions screening process and satisfies regulator expectations.

Since 2021, NBP KSA has put in function an “automated” screening system as its primary transaction and person/entity screening system “sanctions screening system.” All transactions that go through NBP KSA are screened through the sanction screening system.

NBP KSA subscribes to an external database DOW JONES for its primary sanction screening system. Transactions are also screened against Private Local Lists, that includes SSU, etc.

Requirements

The following are subject to screening:

Customers:
All NBP KSA Branch customers and related parties whose information is collected as part of the Know Your Customer ("KYC") Program (e.g. beneficial owners, authorized signers, connected parties, principal directors, senior management, and associated third parties) are screened prior to account opening. This screening also applies new account parties being added to existing accounts. The customers and any beneficial owners are screened against all new or any updated designations to the database as soon as reasonably practicable.

Employees:
All NBP KSA Branch employees, including contractors, are screened before their employment start dates and periodically thereafter.

Vendors:
All vendors, agents, service providers, and any third parties that conduct business or operational activities on behalf of NBP KSA Branch are required to be screened prior to entering into a contract with NBP KSA Branch and also periodically thereafter.

In the case management tool of the SSS, alerts will be generated which will require a 4-eye review.

- The first level review of alerts will be reviewed by L1,
- The second level will be dispositioned by L2

Each level will be required to add value added analysis, including uploading documents, images, etc., if necessary, of each match reviewed that should clearly indicate why the match is a false-positive or full match.

Most alerts will generate matches against multiple words/names and negative lists such that there will be more than one match per alert. In order to review such alerts effectively, the process below will be followed. Alerts will show which name(s)/word(s) generated matches and their percentage matching probability (maximum 100%).

i. Reviewers will search those words/names that generated exact name matches irrespective of the matching probability percentage and those that have a partial name matching probability percentage of 90% and where all the words/names match in any order (e.g.: first - last or last – first, etc.)
ii. In case the reviewer assesses a match to be exact, he/she is required to give a recommendation on next steps; e.g.: • reject payment.
iii. block payment
iv. release as a partial name match
v. even if it is a full name match (e.g.: negative news), there are no restrictions or sanctions that prevent it from being processed.
vi. In order to do this, the reviewer will read the actual sanction or negative news in detail that applies to the matched words and may also need to search other open-source databases, depending on the nature of the match.

vii. Screen-prints of such searches will be uploaded to the alert.

For negative news matches, the reviewer has to ensure the source of the news is reputable, such as a major news source (e.g.: CNN, BBC, New York Times, Bloomberg, etc.). Next, the negative news should impact either the customer's or his/her close associates' ethical or financial choices made to determine next steps, as shown above.

27.1 Real-Time Transaction Screening

NBP KSA Branch utilizes a sanction screening system to screen inbound and outbound payment transactions. Parties and narrative fields of the payments are screened against the applicable sanctions lists. Transactions involving potential matches or confirmed hits against sanctions lists cannot be amended, altered, returned, or cancelled but must be reviewed and dispositioned following the Four-Eye Principle.

27.2 Validation of Sanctions Screening List Updates

Each time sanctions lists change; the entire database is replaced by an updated database. The Compliance function will be notified of this via email by the data provider/IT department, which will contain a summary of the changes, e.g.: new names added, deleted or modified, immediately following upload of the updated database into the SSS. Since this usually happens overnight, the test should be conducted the following business day. In order to ensure the latest database has been uploaded to the SSS, the Compliance function will validate this by following the procedures below.

Compliance function is required to test that the revised dataset has been updated in the SSS. They will do the following to comply with this requirement:

1. From the notification email, select one name/word Create a reasonable sample for testing from the vendor's email of new to additions, deletions and, or modifications for testing.

2. In the single word/name lookup utility of the SSS, enter each name and capture a screenshot of the search result take a screenshot of each search result and document whether each test failed or was a success.

3. Save screenshots in a MS Word document, a sample of which is in **Annexure II**.

a. If the name/word that was added to the updated database is detected in the search, take a screenshot as shown in Appendix 2 and move to test a name/word deleted from the updated database.

b. If not, re-test it immediately and save both failed result screenshots in Annexure II.

i. Immediately notify the IT department of the search failure with instructions to alert the vendor to upload the database again.

ii. Notify the Operations Manager and GM, providing the name/word that is missing.

4. Operation Manager will be responsible to ensure that the name/word not in the updated database is screened manually against all incoming and outgoing payments/messages and other financial transactions.

5. If the name/word deleted from the updated database does not produce a match, follow step #3a above.

6. If it detected in the search result, review the list from which it was removed and compare it to the list the name/word that was detected in the SS system.

a. If the list names are different, document this in Annexure II below the screenshot and declare the test as successful and move to the next test.

b. If the list names from which the name/word was deleted is the same as that shown in the search result, notify the IT department to notify the vendor.

7. If the name/word modified in the updated database matches the search result, follow step #3a above and mark the test as successful.

8. If not, notify the IT department to notify the vendor to provide a fresh list.

9. After the vendor provides the updated database again, re-start the testing from #2 above.

10. For deleted and modified name/word that resulted in a failed test, if the vendor advises that the deleted and/or modified name/word was an error, select another name/word from the respective list, if any, and re-start testing from #2 above.

11. For each update to the database, a separate test results document must be created.

12. Within each test result document, each failed and successful search results must be documented as shown in Appendix 2.

13. All tests must be 100% successful before testing can be deemed to be completed.

14. Retain an electronic record of each search.

15. Report statistics of this in each BCCM, e.g.: number of changes to each sanction list during the period, number of tests performed to ensure all updates were successfully uploaded to the SSS, delays in conducting testing along with reasons

29. Trade Based Money Laundering

Trade Based Money Laundering (TBML) is defined as the process of disguising the proceeds of crime and moving value through the use of trade financing in an attempt to legitimize their illicit origin.

In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. With additional scrutiny on remittances (and other cash payments) making it difficult to explain movement of large amounts without a valid purpose, TBML has become one of the primary methods for criminals to move illegal money.

Traditionally, in the past regulatory expectation / requirement is to Identify & report suspicious activity. However, with respect to latest regulatory expectation is to protect the financial system from the treat of financial crime by seeking to prevent it, thereby strengthening financial sector integrity and contributing to safety and security. Due to this reason Trade based Money Laundering is becoming an increasing area of focus by the regulators around the world. The Bank is required to enhance their capacity to process foreign trade transactions with extreme care and diligence.

Trade-based money laundering involves using of the following techniques to disguise the illicit origin of money:

- Over invoicing
- Under invoicing
- Multiple invoicing
- Over-shipping or short-shipping
- Falsely described goods and services
- Phantom shipment. etc.

Following are few of the Scenarios against which Bank staff shall stay vigilant:

- In Most of the illegally transferred funds, applicants and beneficiaries are connected party and have some common interest between them.
- If any trade transaction is inconsistent with the customer's existing line of business that may have ill- motive to transact against criminal proceeds or may simply move money rather than goods through accommodation of bill etc.

Under Invoicing

The act of stating price on an invoice as being less than the price actually paid. The exporter submits a deflated invoice to the importer, shipping goods with greater value and transferring that value to the importer. Importer is also able to pay less customs duty/tax by under invoicing.

Over invoicing (against market price)

The exporter submits an inflated invoice to the importer, generating a payment that exceeds the value of the shipped goods. Greater value is transferred from the importer to the exporter.

There are no goods (Phantom Shipment)

In this circumstance, the beneficiary or applicant can refuse to provide document against shipment of goods (possible phantom shipping or multiple invoicing). For Example: LC or bank guarantee purportedly covers the movement of goods but fails to call for presentation of transport documents. LC covers steel shipment but allows a forwarders cargo receipt (FCR).

27.3 Controls

- Maintaining a close relationship with customers.
- Reporting to the General Department of Financial Investigation if it comes to the bank knowledge that

the exporter is directly or indirectly connected with or has any financial or other interest in the buyer/consignee abroad that may have led to TBML.

- If necessary, discreet inquiry about the bonafide and credentials of the charter party is made in case the shipment is proposed to be made against a charter party Bill of Lading.
- Finding out any blatant or obvious pricing irregularities inconsistencies of the goods being shipped.
- Verifying that both the exporter and importer are bonafide businessmen of the goods concerned, the exporting country is the usual exporter of the goods concerned.
- Understanding the current trading profile of the customer and its future plans on an ongoing basis.
- Ascertaining which trade products are suitable and which trade products are vulnerable for a particular trade customer at the outset of a trade relationship.

28 New Products and Services AML / CFT / PF Risk Assessment

Bank shall ensure that whenever a new product / service is being launched AML / CFT / PF risk assessment will be performed in the following manner:

Risk Area Description	Risk emanating from different products
Criteria	The bank has a formal procedure of vetting the new product and review of existingproducts to assess the AML/CFT/CPF Risks.
Inherent Risk	Low/Medium/High
Control	AML/Compliance Department shall review each new product or an amendment to the existing product and to ensure a standard control mechanism. Compliance department shall check whether the new product / service or amendment in existing product / service complies with all the regulatory requirements & detailed analysis shall be done to assess whether AML / CFTcontrols are in place against all the information and / or transactions that could pass through that product / service as the case maybe Moreover, since the bank offers most of the conventional products over risk profileis also quite low, due to absence of high-risk products like Credit Cards etc. are not offered by the bank.

29 Regulatory Reporting

Branch will comply with local and international reporting requirements, such as FATCA, CRS, etc. These will be managed by the relevant department of the branch, but monitored for timely submission by the BCCM.

STRs and other Compliance/AML/CFT related reporting, such as SSU, Fraud, etc. will be filed by the AML/relevant department and whose data (e.g.: number of reports received/processed, etc.) will be reported to the BCCM to the extent allowed by local law.

30 Record Keeping

To comply with AML/CFT/CPF Regulations issued by SAMA & SBP, Bank shall maintain all necessary records on transactions, both domestic and international, including the results of any analysis undertaken (e.g., inquiries to establish the background and purpose of complex, unusual large transactions) for a minimum period of ten years from termination of customer relationship.

The records shall be sufficient to permit reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any account involved in the transactions so as to provide, when necessary, evidence for prosecution of criminal activity. The transactions records may be maintained in paper or electronic form or on microfilm, provided it is admissible as evidence in a court of law.

- The records of identification data obtained through CDD process like copies of identification documents, account opening forms, CIF, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a minimum period of ten years after the business relationship is ended. The identification records may be maintained in document as originals or copies subject to bank's attestation.

- The Bank shall, however, retain those records for longer period where transactions, customers or accounts involve litigation or it is required by court or other competent authority.

31 Staff AML/CFT/CPF Training

The Bank has a continuous training program for all employees to inform them of the regulations, instructions and developments related to the field of AML/CFT/CPF, in order to increase the efficiency of the employees in recognizing these operations and their patterns and how to counter them in a manner that achieves a degree of familiarity and knowledge to play an effective role in reducing the occurrence of these crimes and combating them.

The bank has allocated sufficient budget to train senior management and employees to achieve efficiency in AML/CFT/CPF. The training is inspired by realistic experiences and include the internal controls of the Bank and the new developments and methods in the relevant money laundering and terrorist financing operations.

The following shall be taken into account in the provided training program:

- Train and educate all current and new employees before starting their works on the importance of AML/ CFT/CPF policies and procedures. As well as, this training shall be re-introduced continuously to ensure that employees are reminded of their responsibilities and are constantly informed of updates and developments in this regard.

- Provide more comprehensive and detailed training for the personnel responsible for implementing due diligence measures, consistent with the risks to which the financial institution is exposed.
- Provide specialized and adequate training in the field of AML/CFT/CPF for the officers of AML/CFT/CPF compliance and the personnel of independent audit.
- Educate all employees, Senior Management of the Branch of their responsibilities, personal duties and the penalties they may face if they fail to comply with the relevant requirements, as stipulated in the Anti-Money Laundering Law, the Combating Terrorist Crimes and their Financing, the executive regulations and instructions issued by the Authority and the relevant authorities.
- Training must be provided by those certified by SAMA and must comply with its rules, eg: in-person, classroom or online training, etc.
- In addition, nominated staff, including all employees in Compliance, are required to pass the online trainings set up by HO Compliance Group.

32 Whistle Blow

Whistle-Blowing (WB) covers reporting of incidents of misconduct, involving or affecting an organization to enable the organization to take appropriate action. It is a window to obtain feedback on issues bordering on both corporate governance as well as reputational risk related issues, escalated to the highest levels of the Bank.

32.1 Who Can Speak-Up/Blow the Whistle?

Any individual, institution and an employee of the Bank, who has observed reportable misconduct shall report his / her concerns to the designated officials within the Bank. This gives assurance that employees, stakeholders, or any member of the public can raise legitimate concerns, without fear of reprisals, provided they are made in good faith. All staff should ensure that they take steps to disclose any wrongdoings or malpractices of which they become aware as non-action/ concealment will be deemed as complicity.

32.2 What Constitutes Malpractice or Misconduct?

A genuine concern should be reported if there are reasonable grounds for believing that anything including but not limited to the following have been committed:

- Illegal or Unlawful Conduct
- Financial Misconduct
- Unethical & Non-Financial Misconduct
- Wasteful Misconduct
- Harassment

All whistle Blow cases will be handled by Whistle Blow Unit at Head office and the branch Compliance department. Whistle blow against any official of the bank can be reported to the Compliance Manager, who

should notify Head Office about the complaint, but must investigate it in line with the bank's policy. Whistle blow complaints will be reported to the branch compliance committee to the extent allowable by local laws.

Annexure-A

Standard Operating Procedure
Transaction Monitoring – NBP KSA Branch

Contents

1. Introduction

NBP Riyadh Branch implemented FCM (Financial Crime Mitigation) which is a part of T24 in 2021 which is based on pre-set scenarios. These scenarios are based on the Banks business requirement and are approved by the branch ‘s compliance committee, which is also responsible for approving modifications/fine tuning to them. These scenarios and their thresholds are subject to periodic review.

2. Scope

This document describes procedural guideline for management of alerts generated by FCM. It includes the scenarios and thresholds currently activated and describes the lookback period to be followed for certain scenarios by the Level 1 Analyst and Level 2 Approver. It also defines criteria for prioritizing, selecting and reviewing the alerts on the basis of level of risk associated with the Customer / Account.

This document is prepared by the KSA CCO in coordination with the International Compliance Division of the Compliance Group at Head Office. This document is subject to review at least annually.,

3. Financial Crime Functionality Overview

There are currently four modules available within the FCM product family that are in use by the branch.

- Suspicious Activity Prevention
- Profile
- Screen
- Know Customer+

FCM applies scenarios against customer and transactional data from the Core Banking System (CBS) to automatically identify potentially suspicious behavior. A seamless workflow enables the investigative process to proceed with increased effectiveness and efficiency.

4. Alert Management

The branch has developed scenarios to detect the following:

- Large or complex transactions with no visible/apparent economic or lawful purpose.
- Aggregated frequent and small transactions.
- Unusual patterns of physical cash deposits or withdrawals, which are large when aggregated over a period of time.
- Significant deviations from past account activity (or inactivity).
- Transaction activities with nexus to higher risk countries or geographies.

- Detection of activities or behaviors consistent with certain predicate offences (e.g. possible tax evasion or avoidance, corruption nexus, or terrorism financing).
- Hidden relationships between customers or accounts evident through funds flows.

In FCM, presently there are 14 active scenarios against on which TMS alerts are generated. NBP Riyadh has opted and implemented relevant scenarios considering risk exposure prone to the branch. Transactions are monitored through these rules against the respective threshold sets/values and look back period to ensure reasonable risk coverage. Alert Rules which are currently configured in the FCM are listed below:

4.1. Implemented Scenarios

S. No.	Rule Name	Rule Description	Frequency
1	Rapid Debits	Number of debits over 1 day > Number of debits over the last 30 days	Monthly
2	Rapid Credits	Number of credits over 1 day > Number of credits over the last 30 days	Monthly
3	Rapid high credits	Number of Credits over 7 days > 10 Cumulated Credits over 7 days > 20,000 SAR	Weekly
4	Rapid high cash withdrawals	Number of debits over 7 days > 10 Cumulated debits over 7 days > 10,000 SAR	Weekly
5	Smurfing	Maximum single Credit in one day < 10,000 SAR, but Cumulated Credits over 1 day > 10,000 SAR. Number of Credit over 1 days > 2	Daily
6	Unusual values	Cumulated transactions over 30 days > 200% average Cumulated transactions over 6 months	6 Monthly
7	High value balance	Cumulated credits over 6 Months > 300% Cumulated debits over 6 Months	6 Monthly

8	Unusual frequencies of transactions	Number of transactions over 1 day > number of transactions over 60 days	2 Monthly
9	Regulatory threshold	Single transaction > 20,000 SAR	Daily
10	Structuring	Transaction amount < 18,000 SAR And Transaction amount > 16,000 SAR	Daily
11	Debit exceed credits	Cumulated Debits over 5 days > 5,000 SAR; Cumulated Debits over 5 days > 300% Cumulated Credits over 3 months	3 Monthly
12	Deviation from history	Cumulated transaction amount over the last 30 days > 150% of the monthly cumulated Transaction amount over the last 6 months	6 Monthly
13	Odd transactions	Number of transactions over the last 30 days > 150% of the monthly average of Transactions over the last 6 months	6 Monthly
14	Monthly Remittances	Sum of Remittances amount over a month > 5000 SAR and Sum of Remittances transaction over a month > 5	Monthly

5. Escalation Matrix - TAT (Turn-around time)

- Turnaround time for review & closure of an alert is 30 business days from the date of alert creation by L1 and L2.
- L1 has to commence review of alerts within 3 days of generation. The remaining 27 business days can be used to determine the final disposition of an alert.
- Initial TAT for RFIs is 5 working days.
    - In case of a delay in the response, follow-up will be sent the next working day.
    - If a response is not received by EoD on the 7th working day, the matter will be escalated to Branch GM.
    - If a response is not received on the 9th working day, an escalation will be sent to all, including IFRG and Compliance Groups in Head Office
    - If no response is received, the RFI will continue to be escalated to all the above every 2 working days thereafter until either the information is provided or the alert is dispositioned.

    - L1 will escalate the lack of response as a potentially suspicious matter by documenting the potential risks in the alert to L2.
- Alerts that are not dispositioned within the deadline will be reported to the Branch Compliance Committee of Management (BCCM) along with a reason.

6. Alert Aging

The reports for aging of alerts from the time an alert is created till it is closed is available in FCM, which is sent daily to the Compliance Manager and Compliance Group in Head Office (for oversight). This report does not contain any details about the alerted transaction, for e.g.: customer name, etc.

7. Guidelines for Reviewing Alerts

Alerts generated through FCM are reviewed and closed through four eye principle on the basis of analysis conducted by the Compliance Officer/MLRO. Rights of each user level are:

- Level 1 - Analyst (View and Open) and
- Level 2 - Reviewer (View, Open, Close and file STR/SAR).

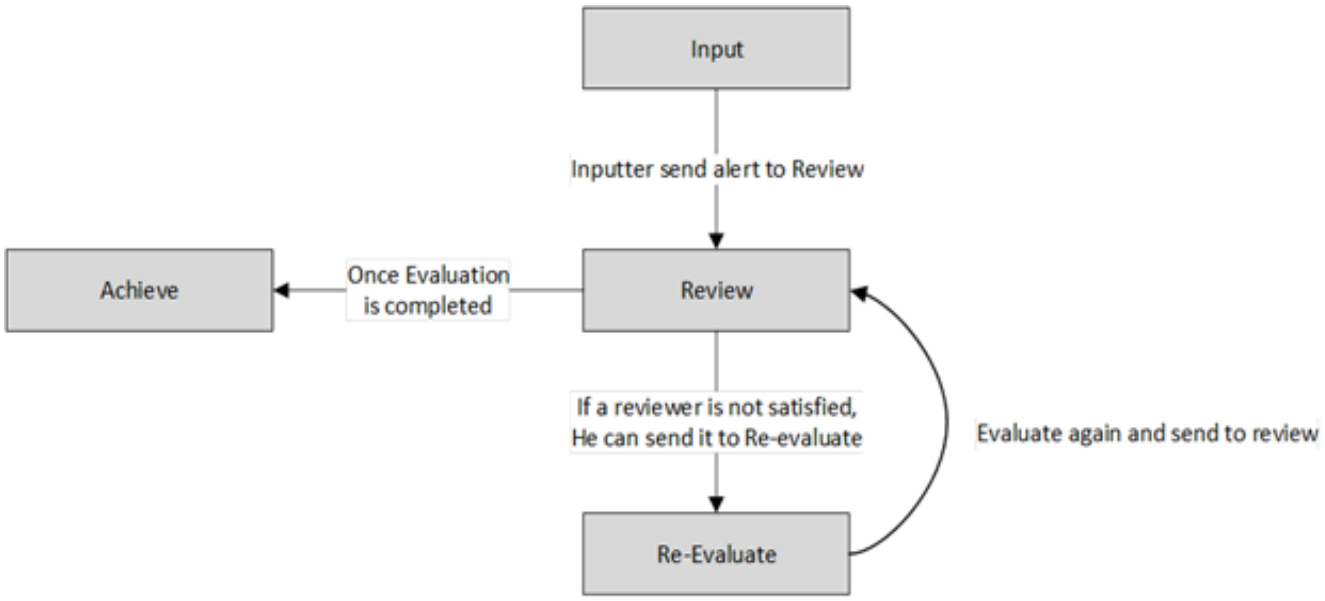
1. Analysis on the alerted transactions to be initiated by the Analyst.
2. If clarification is required to disposition an alert, L1 should issue a Request for Information (RFI) to the branch Operations Manager only if the information requested is not accessible to L1 or L2. RFIs should contain the alerted transaction(s) and a list of information/documents requested.
3. If L1 has reservations with the response to the RFI, it should be brought in the knowledge of the Compliance Manager for further consultation and opinion on the alert under review.
4. When an alert requires further investigation, either issue an amendment to the initial RFI or send another RFI following step 2 above. Refer to the 'Alert Disposition Process' for guidance.
5. Once the reply is received from the respective branch the same will be evaluated and scrutinized.
6. In case of 'Out of Character Transactions/Unusual Transactions' Appendix – 1 (AML Red Flags) is identified, L1 will refer the same to the L2 for guidance.
7. L2 will ensure compliance of the guidelines for reviewing alerts.
8. All closures irrespective of the scenarios to be handled by L2.

8. Manual Escalations of Suspicious Behavior to Compliance

- Where a suspicion is raised by the Branch, they will report the instance to the Compliance Manager.
- Where a suspicion is raised related to the account opening documents, L1/L2 will raise a RFI to Operations.

Workflow of alert review is:

Input ⇨ Review ⇨ Re-evaluate ⇨ Final Disposition



9. Alert Disposition Process

The following general guidelines may be considered by the analyst during alert disposition process:

- Analysis of transactions/transactional pattern as to whether they are consistent and aligned with customer's profile, personal/business activity, source of funds/income/wealth and/or any relevant information available in the bank's record
- Status/Type/Nature of account along with intended purpose of account
- Do the scenarios that trigger alerts seem unusual based on the type and volume of customer's business
- Nature of business along with factors like size, volume, major flow of funds, seasonal fluctuations (peak or low), linked entities, other business dynamics etc.
- Counterparties analysis where deemed necessary and where specific alert rule requires the analysis for e.g. Rule "International Transactions"
- Customer relationship/account history in light of recurring alerts generation and business feedback thereof
- Is the flow of cross border transactions justified?
- In individual/self-employed/sole proprietor etc. accounts, especially customer's age is one of the important factor that should be considered while reviewing alerts and transactional pattern of accounts.

- Special attention should be paid to those alerts where customer is young & account activity is high or not aligning with the customer's profile
- Web searches including google searches for negative news/information from a reputed source may be useful for alert review process, local authorities' published records & name screening (where deemed necessary)
- Age of account or length of relationship with the bank: the shorter the age, the more vigilant the analyst should be
- Various demographical factors related to customer/account like high-risk jurisdictions/territories, countries of special concern identified by the FATF, cash intensive businesses, high risk businesses like real estate dealer, jewelers, students, housewives, minors, PEPs, NGO/NPO, trust, charity, associations, societies, etc., should pay special attention due to their inherent risk posed while reviewing alerts.
- Money flows / multiple wire transfers received by Beneficiaries or sent by Originators that do not fit common remittance patterns.

While disposing/closing the alerts in FCM, following are the guidelines that may refer by reviewer during the alert life cycle:

- Every alert closed in the system should include an appropriate disposition comment by the analyst / reviewer;
- Disposition comments may encompass details like customer information, source of funds, purpose of account/transaction, and analysis on the basis of which alert is reviewed or closed;
- Based on the investigation findings, make informed decisions regarding the disposition of each alert. If suspicious activity is determined, escalate the case for further action, such as filing a Suspicious Transaction Report (STR) by escalating to the CCO, which may lead to a recommendation for account closure or customer relationship termination.

Analyst may attach/refer KYC/CDD/EDD documents, documentary evidence/proof of transaction that obtained during the course of review.

9.1. Guiding Rules for Review, Analysis & Investigations of Alerts or Cases

Mandatory Step	Description
1	**Customer Profile:** • Review current CIF to understand the customer's disclosed economic profile/ financial worth. During this, following e-KYC information are a must to be reviewed & analyzed: • Purpose of Account • Customer type • Product Type • Channels used • Turnovers (i.e., Monthly Credit T/O, Annual A/C T/O) • Major Counter parties' / Geographic locations • PEP Status • UBO (Ultimate Beneficial Owners) • Last KYC Review Data & Reviewed changes (as applicable) • Review SS Cards uploaded on System in order to know if there is any mandate holder in the account • Review AODs (account opening documents) * • Customer Profile (to check No. of accounts tagged with customer ID). If more than 1, merge the activity of both accounts to determine if there are indicia of suspicion. **Information for Legal Persons/ Legal Arrangements:** • Nature of business, geographies involved and expected type of counter-parties, line(s) of business • Does purpose of account or align with type of transaction.
2	**Transaction Analysis:** • Review relevant transactions that generated the alerts. • Cash, remittances, IBFT, frequent transfers, frequent credits need to be focused and require necessary evidence which supports those transactions from the concerned Branch. • Review past transactions of a reasonable period** and establish trend to analyze the transactional pattern • Check statistical history and current volume/ turnovers.

	• Identify counter parties & geographic locations of major transactions carried out during last 1** Year • Determine the relationship between the main entity and counter-parties to the transaction. • Check & compare the identified major counter parties with information provided in CIF, if it is not mentioned, Analyst should raise the concern to Operations for the necessary update. • Transactions analyzed in context of the alert must be annotated.
3	**For alerts requiring further investigation - Public Domain Search against suspected parties:** • Perform Public domain searches through Google to identify adverse information about the entity [pertaining to Sanctions, Fraud, ABC, Corruption, PEP or any other Adverse Media News, (if any) • Capture the results in form of screen shots and make part of the analysis / uploaded the same in the SAS for Audit Trail Purpose.
4	**Conclusion:** • Articulate proper justification of the alert/ case closure in the closing comments. • In case of AML query, analyses of the response / supporting documents received and should also be annotated in the closing comments. • Further, complete analysis of the transactional activity along with, print screen of current KYC Form, Public Domain/ NSS search results, email trail (as applicable) should be attached in the FCM alerts for Audit Trail Purpose.

***** Mandatory where Account Opening Documents are available on DMS portal

**Period for transactional review may be decreased depending over the transactional volume of the account but not lower that the appended horizon:

10.Reporting of STR to FIU

A Case may be escalated for STR filing in the following circumstances:

- Where negative information from a reliable source has been obtained on the parties that relates to customer's activity processed through their account(s) or negative financial news of a business customer.
- Where the activity in question does not appear to be in line with the parties' business/functions.
- Where customer does not respond or delays responding to a RFI by Compliance.
- Where the party's account with the Branch was closed under suspicious circumstances

Appendix – 1 "Red Flags"

Red Flags

Red Flags Related to Client Onboarding / Periodic Review

- An account in which several individuals hold signature authority and the individuals do not apparently have any family/business relationship or any economic connect;
- An account opened by a person/entity that has the same addresses or contact numbers as of other person/entity without any apparent economic reason or rationale;
- A person/entity maintaining an account apparently associated with a terrorist organization or having similar ideology as of a terrorist organization;
- Accounts of person/entity that belong to or are associated with person/entity of high−risk jurisdictions or to countries of specific concern;
- Any type of irregularity noticed during the identification and verification process while opening the account which could not be adequately justified by the individual/entity or by the available circumstances;
- Names identified in adverse media / Law enforcement agency / FIA Redbook etc. published online.

Red Flags Related to Monitoring of Transactions

- A dormant account suddenly receives a huge deposit or series of deposits followed by cash withdrawals or through any other transaction mode made on regular basis till the funds in the account are reduced to a nominal balance;
- Multiple cash deposits of small amounts in different accounts maintained by the same person/entity in different branches in a single day or a short span of time;
- Cash withdrawals of small amounts made on a regular basis from the account of a person/entity from different geographical locations, which does not commensurate with the stated profile of such person/entity;
- The individual conducts a transaction via using a credit instrument or any other negotiable/non−negotiable instrument with a high−risk jurisdiction or a country of specific concern;
- Cash withdrawals or transactions (including financial and non−financial transactions) using the ATMs located in the areas of conflicts &/or high−risk jurisdictions;
- The person/entity conducts transactions for the sale/purchase of virtual currency directly or through a virtual currency intermediary that allows for increased anonymity;
- Person/Entity suddenly receives funds from foreign jurisdictions in different accounts maintained in a bank;
- Upon inquiry for justification of inconsistent transactions conducted in the account, apparently vague

explanations are provided and no supportive documentary evidence is presented;
- Accounts observed where customer has paid minimal / nil amount of tax determined from FBR's online published Tax directory, which contradicts with the heavy account activity/profile of the customer;
- Customers are apparently involved in Bitcoin / Virtual Currency Transactions, which is not a legal tender in Pakistan.

Red Flags Related to Wire Transfers/Sanctioned & Proliferation Financing Risk

- Large number of wire transfers made by a person in small amounts in an apparent effort to avoid identification/triggering requirement;
- An incoming wire transfer where the originator information is either not available or a very
- limited information is available of the originator;
- Wire transfers by an individual or entity to/from the high−risk jurisdictions or to countries of
- specific concern including but not limited to countries designated by national/international authorities or countries included in FATF's list of high−risk/sanctioned jurisdictions;
- Person sending/receiving wire transfers frequently have variations of addresses or contact
- numbers while conducting transactions most of the times;
- Transactions conducted with shell companies &/or through shell banks located in tax havens or
- offshore jurisdictions;
- Person/Entity receiving or sending funds through wire transfers to the parties which are not
- related to its line of business;
- A wire transfer received from a foreign jurisdiction in which the name of the originator
- apparently seems similar to the name an entity/person designated under UNSCRs 1267, 1373 & other relevant UNSCRs and/or entity/person proscribed under the domestic laws like 1st, 2nd & 4th schedules of ATA, 1997 or as declared by any relevant authority.

Red Flags Related to TF risk & NGOs/NPOs/Charity/Trust etc.

- Transactions conducted in the accounts of NGOs/NPOs for which there is no apparent economic or plausible reason and the transactions apparently do not match with the regular business activities of the organization;
- Use of the accounts of NGOs/NPOs to collect funds for immediate transfer to a small number of
- foreign/domestic beneficiaries;
- Movement of funds to/from the areas of frequent military and terrorism activities by
- NGOs/NPOs;
- Wire transfers conducted in the account of NGOs/NPOs to/from the high−risk jurisdictions or to
- countries of specific concern;
- NGOs/NPOs involved in charity related activities in the areas of conflict or high−risk jurisdictions;

- High volume of cash−based activity noticed in the account of NGOs/NPOs without any economic
- or plausible reason.

Red Flags Related to TBML:

- Obvious over or under/over pricing of goods (significant discrepancies appear between the value of the goods reported on the invoice/EIF/MIF, EFE/MFE, Advance Payment Voucher and the
- known fair market value of the goods).
- The description of goods on the Goods Declaration Form/Transport documents significantly varies from the description declared on EIF/MIF, EFE/MEF or underlying contract.
- Significant variation is found between the description of the goods on the bill of lading and the in− voice.
- There are indications that the descriptions of the goods are disguised.
- The tenor of the transaction does not commensurate with the nature of the underlying goods − for example perishable goods are traded on terms involving lengthy usage period.
- Documents such as a letter of credit is received through unverified channels such as unauthenticated SWIFT message.
- The type of goods being shipped appears to be inconsistent with the exporter's or importer's regular business activities.
- The size of the shipment does not commensurate with the size of the exporter's or importer's regular business activities.
- The packaging of goods is inconsistent with the commodity or shipping method.
- The goods are transshipped through one or more countries/jurisdictions for no apparent economic or logistical reason.
- The country from which goods are being shipped is designated as "high risk" for money laundering activities.
- The transaction involves the receipt of payments from third parties that have no apparent connection with the transaction.
- The method of payment apparently does not commensurate with the risk characteristics of the transaction e.g. the remittance of funds in advance payment for a shipment from a new supplier in a high−risk country.
- The transactions involving consecutive trade discount offered by exporters to the same importer.
- The transaction involves repeatedly amended or frequently extended letters of credit.
- An exporter receives advance payment(s) but does not make shipment(s) there against.
- An Importer remits advance payment(s) but does not receive shipment(s) there against.
- The transaction appears to involve use of front or shell companies for the purpose of hiding the true

parties involved.

- The transaction involves import/export of dual use goods.
- The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- Where important details are missing on commercial invoice(s) or mentioned vaguely.
- Where some of the shipping documents are provided in photocopies instead of original against the regularity instructions or against normal business scenarios.
- Where goods declaration in commercial invoice(s) are not proper, incomplete or otherwise not mentioned at all to conceal the facts.
- Receipt of proceeds from non−cooperative countries as per FATF list against the shipment made to a third country.
- Where export proceeds are received from unrelated/third party with differing nature of business from that of exporter.

Annexure II

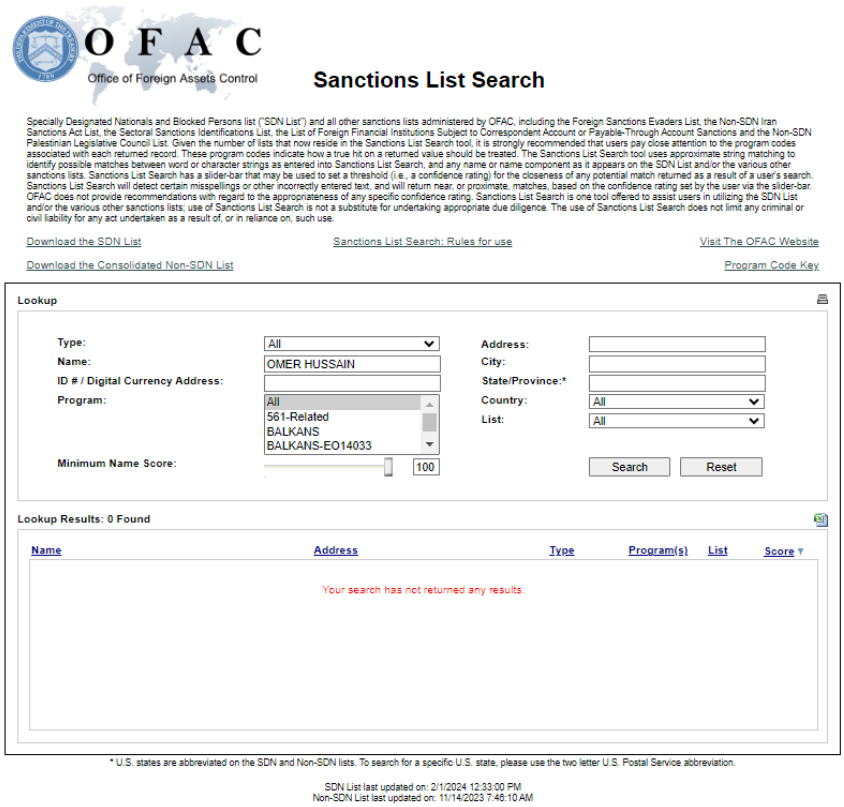
Validation Testing of Sanctions Screening List Database Update

Database Update Date: Testing Date:

Testing of name/word Added to database, if any

Name/Word Tested: Omer Hussain Test Result: Successful / Failed

[THIS IS A SAMPLE SCREENSHOT – ADD SCREENSHOT OF SS SYSTEM]



*** Sample reasons for successful/failed tests, if required:**

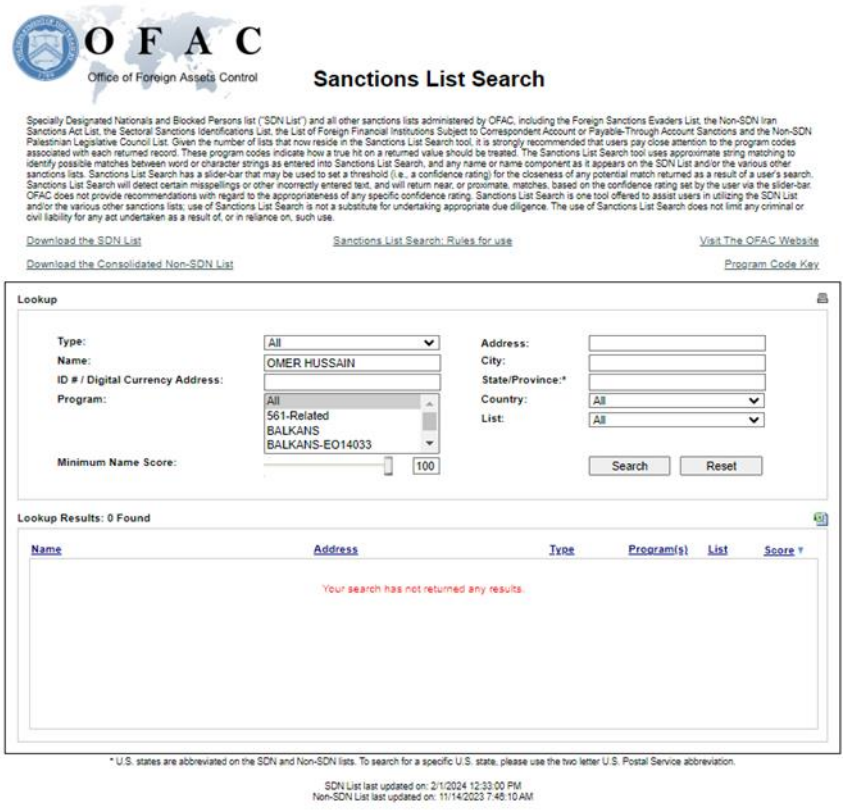
[for failed tests]

- Name/word added to the updated database was not detected. Vendor has been informed. Retest will occur after fresh database is uploaded to the SS system whose results will be documented in this file.

Testing of name/word Deleted from the updated database, if any

Name/Word Tested: Omer Hussain Test Result*: Successful / Failed

[THIS IS A SAMPLE SCREENSHOT – ADD SCREENSHOT OF SS SYSTEM]



*** Sample reasons for successful/failed tests, if required:**

[for successful tests]

- Deleted name/word in the updated database was included in more than 1 list, which is why it continued to generate alerts.

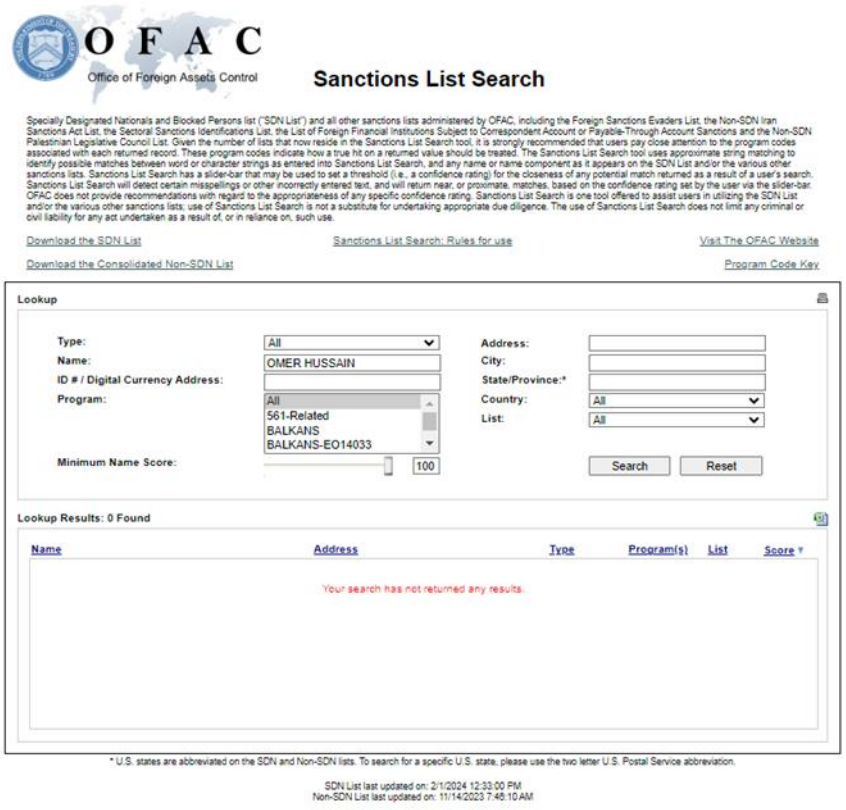
[for failed tests]

- The same name/word that was reported to be deleted by the list owner in the updated database continued to product matches of the same list. Matter has been referred to the vendor.
    - If the vendor provides an updated database, retesting will take place and will be contained in this document.
    - If vendor indicates that the deletion was incorrectly reported, another deleted and/or modified name, if any, will be tested, whose result will be included in this file.

Testing of name/word Modified in the updated database, if any

Name/Word Tested: Omer Hussain Test Result*: Successful / Failed

[THIS IS A SAMPLE SCREENSHOT – ADD SCREENSHOT OF SS SYSTEM]



*** Sample reasons for successful/failed tests, if required:**

[for failed tests]

- Modified name/word continued to generate matches to the original name/word, not the modified name/word. Vendor has been notified.
    - If the vendor provides an updated database, retesting will take place and will be contained in this document.
    - If vendor indicates that the deletion was incorrectly reported, another modified name, if any, will be tested, whose result will be included in this file.