Anti-Money Laundering and Counter-Terrorism Financing Policy

Updated March 2021

Table of Content

1. Introduction

Money laundering and terrorist financing have been identified as major threats to Al Khaleej Bank. Sudan, in common with many other countries, has passed legislation designed to prevent money laundering and to combat terrorism. This legislation, together with regulations, rules and industry guidance, forms the cornerstone of AML/CFT obligations for Sudanese Banks and outline the offences and penalties for failing to comply.

Al Khaleej Bank is fully committed to local and supervisory efforts to combat the spread of money laundering .The Bank is in full comply with all of the central Bank of Sudan' (CBOS) "Rules Governing Anti-Money laundering and combating Terrorist Financing as well as all CBOS circulars relating to Anti-Money laundering. The Bank will also adopt the principles drafted in international standards and Guidelines. This responsibility rests with all staff.

2. Policy Framework

Al Khaleej Bank is committed to the highest ethical standards regarding anti-money laundering (AML) and countering the financing of terrorism (CFT) consistent with the Financial Action Task Force (FATF) recommendations in its "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation". This policy aims to safeguard Al Khaleej Bank against money laundering and the financing of terrorism. The Policy outlines the principles and minimum standards of internal AML/CFT controls which should be adhered to by Al Khaleej Bank to mitigate reputational, regulatory, legal and financial loss risks. It is part of a broader set of policies aimed at ensuring that Al Khaleej Bank funds are used in line with its objective, and it lays out a set of basic principles for guidance.
Also Al Khaleej Bank implements targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. The bank comply to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.
In complying with these rules the bank issued the following policy statement

- The appointment of Money Laundering Reporting Officer (MLRO) .
- Establishing and maintaining a Risk Based Approach (RBA) towards assessing and managing the money laundering and terrorist financing risks to the Bank.
- Establishing and maintaining risk-based customer due diligence, identification, verification and know your customer (KYC) procedures, including enhanced due diligence for those customers presenting higher risk, such as Politically Exposed Persons (PEPs) and Correspondent Banking relationships.
- Establishing and maintaining risk based systems and procedures to monitor ongoing customer activity.
- Procedures for reporting suspicious activity internally and to the relevant

la
w enforcement authorities as appropriate.
- The maintenance of appropriate records for the minimum prescribed periods.
- Training and awareness for all relevant employees.
- The Head office and Branches are required to screen against Central Bank of Sudan, UN EU, and US Office of Foreign Assets Control (OFAC) sanctions lists.

3. Legal and Regulatory Framework:

This policy has been formulated according to the following:

1) Anti-Money Laundering and combating Terrorist Financing Act -2014
2) The central Bank of Sudan' (CBOS) rules governing anti-money laundering and terrorist financing.
3) The Recommendations of the Financial Action Task Force (FATF)

4. Anti-Money Laundering and Counter Financing Terrorism Unit.

The Anti-Money Laundering and Counter Financing Terrorism Unit was established in the compliance Department to assist the Bank in combating money laundering and terrorist financing. Its key responsibilities are:-

- Preventing and detecting money laundering activities.
- Ensuring compliance with the "Rules Governing Anti-Money Laundering and Combating Terrorist Financing"
- Developing internal policies and procedures to combat money laundering and terrorist financing.
- Developing and implementing money laundering awareness programs.
- Receiving, reviewing, studying, investigating and reporting all suspected cases of money laundering and terrorist financing.
- Reporting suspicious activities to the Financial Information Unit (FIU)
- Developing and implementing Anti-Money laundering training programs for all bank staff
- Reviewing and approving trade finance transactions

The Anti-Money Laundering Unit give advice in all aspects of anti-money laundering and combating terrorist financing.

5. Know Your Customer Standards

a) The objective of the KYC guidelines is to prevent Al Khaleej Bank from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures enable Al Khaleej Bank to know/understand his customers and his financial dealings better which in turn help to manage risks prudently.
b) A customer for the purpose of KYC Policy is defined as:
   - A person or entity that maintains an account and/or has a business relationship with the bank

- One on whose behalf the account is maintained (i.e., the beneficial owner)
- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors, etc as permitted under the law
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of high value demand draft as a single transaction.

6. Customer Due Diligence

The customer due diligence (CDD) measures undertaken when:

(i) Establishing business relations;

(ii) Carrying out occasional transactions: (a) above the applicable designated threshold (USD/EUR 15,000); or (b) that are wire transfers in the circumstances covered by the Interpretive Note to FATF Recommendation 16;

(iii) There is a suspicion of money laundering or terrorist financing; or

(iv) The financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The customer due diligence (CDD) measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

7. Customer Acceptance Policy (CAP)

The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed in the bank. The branches shall accept customer strictly in accordance with the said policy:

a) No account shall be opened in anonymous or fictitious name(s)
b) No business shall be conducted with non-account customers .i.e. walk in customer
c) No business shall be conducted with the bank having no physical presence in any country i.e. shell banks
d) Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc., to enable categorization of customers into low, medium and high risk.
e) The branches shall collect documents and other information from the customer depending on perceived risk.
f) The branches shall close an existing account or shall not open a new account where it is unable to apply appropriate customer due diligence measures.
g) The branches shall make necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations

The risk to the customer shall be assigned by the branches on the following basis:

i. Low Risk:

h) Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. The illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer shall be met. New accounts for low risk customers should be approved by the Branch Manager.

ii. Medium Risk:

Customers that are likely to pose a higher than average risk to the bank may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc; such as:

a) Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.
b) Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious.

New accounts for medium risk customers should be approved by the Branch Manager.

iii. High Risk (Level III):

1/ The branches apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. The examples of customers requiring higher due diligence as the following:

1) Non Resident Customers,
2) High Net worth individuals
3) Trusts, charities, NGOs and organizations receiving donations,
4) Companies having close family shareholding or beneficial ownership
5) Firms with 'sleeping partners'
6) Politically Exposed Persons (PEPs)
7) Non-face to face customers, and
8) Those with dubious reputation as per public information available, etc.
9) The persons requiring very high level of monitoring.

2/ Opening accounts for high risk customer should be approved by the Head of Compliance

3/ Opening accounts for Politically Exposed Persons (PEPs) should be approved by the GM

8. Customer Identification :

The branches need to obtain sufficient information necessary to establish, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship.

Accounts of natural persons:

For customers that are natural persons, the branches shall obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph.

- The following documents are commonly used for identity verification:

1. Identity card
2. Passport
3. Driving license
4. Diplomatic passport
5. Passport granted by foreign authorities

- The following information is necessary and essential in establishing and maintaining a customer relationship:

1. customer's name, address, personal identity number and nationality
2. information on whether the customer holds an important public position (politically exposed person, PEP) or whether he/she is a family member or a close associate of such a person
3. information on the customer's life situation, describing his/her financial status (e.g. employer, pensioner, student)
4. information on whether the customer relationship to be established is the customer's main banking customer relationship
5. information on the origins or source of funds and regular payment transfers/cash flows
6. assessment of the customer's regular payment transaction volumes

7. assessment of the customer's foreign payment transaction volumes and the grounds for such transactions

Accounts of legal persons or entities"
For customers that are legal persons or entities, the branches shall:

1. Verify the legal status of the legal person/entity through proper and relevant documents
2. Verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person
3. Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

Accounts of Politically Exposed Persons (PEPs):
Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Branches should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. ." The main due diligence measures, aimed at obtaining information and conducting monitoring and review of PEPs, laid out in the guidelines and notices of the supervisory bodies.

Correspondent Banking:

1. The bank while entering into any kind of correspondent banking arrangement shall gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country shall be of special relevance. Such relationships shall be established only with the prior approval of the Board.. The bank shall also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.
2. The Bank shall not enter into a correspondent relationship with a 'shell bank'. A Shell bank is a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group. "Shell banks" are not permitted to operate in Sudan. Bank shall also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by "shell banks".
3. The Bank shall not allow direct use of correspondent accounts by his customers to transact
   Business on their behalf i.e. do not allow Payable-through accounts.

9. Sanction policy

Al khaleej Bank is committed to complying with the sanctions laws and regulations of the United Nations (UN), the European Union (EU) and the United States (US), as well as all applicable sanctions laws and regulations in the jurisdictions in which we operate.

This policy define the minimum standards in which Al khaleej Bank and its subsidiaries must comply with to meet the above obligations. This includes:

1) Screening customers and transactions – in real time base- against the sanctions lists issued by the UN, the EU, the US (including the Office of Foreign Asset Control of the US (OFAC)) and all applicable local regulatory sanctions lists in the jurisdictions in which Al khaleej Bank and its subsidiaries operate.
2) Prohibiting or restricting business activities, personal transactions, customer relationships or facilitating transactions that:
    a. May violate the applicable sanctions laws, whether directly or indirectly.or
    b. Involve individuals, entities or vessels listed on an official sanctions list by the UN, EU, OFAC or the local regulatory sanctions list whether directly or indirectly. Or
    c. Residing in, or operating from a sanctioned country/location.or
    d. May potentially circumvent applicable sanctions laws or contravene the spirit of such sanctions laws.
3) Blocking or rejecting transactions where Al khaleej Bank is obligated to do so under the applicable sanctions laws or regulations or where the transactions are not within our risk appetite.

10. Updating and reviewing customer information.

The information and documents for customers are updated as follows:

1 / Regularly every five years as a maximum subject to reduction that period for consumers with high-risk, in such case updating and reviewing customer information shall be every year maximum.

2 / At the time of any changes or presence of suspicion concerning the customer at any stage of a deal.

3 /If there is a big change in the usual transaction pattern of the relevant customer..

4 / Considerable need, in accordance with the Bank's request for additional information from the customers

5/ the information and documents of correspondent banks are updated periodically every five years with maximum or any changes that indicate doubts about the bank at any stage of the transaction.

11. AML Compliance Officer

The bank shall appoint an AML Compliance Officer, who will be fully responsible for the bank's AML and CFT program and report to the Board of Directors or a committee thereof any material breaches of the internal AML policy and procedures and of the Regulations, codes and standards of good practice.

The Compliance Officer shall have the following responsibilities and powers:

1. The compliance officer shall exercise his powers with absolute independence to enable him to carry out his duties efficiently
2. Ensuring the Bank's compliance with the requirements of the regulations;
3. Establishing and maintaining internal AML program;
4. Establishing an audit function to test its anti-money laundering and combating the financing of terrorism procedures and systems;
5. Training employees to recognize suspicious transactions;
6. Receiving and investigating internal suspicious activity and transaction reports from staff and making reports to the FIU where appropriate;
7. Ensuring that proper AML records are kept;
8. Obtaining and updating international findings concerning countries with inadequate AML systems, laws or measures.

12. Record-keeping

Records and data should be kept as follows:

1. All records and data obtained through due diligence procedures in customer verification, including identification documents from customers and beneficiary owners, accounting files and work correspondence, for at least five years after the end of the employment relationship or the date of implementation of the transaction whichever is longer..

2. Records and data relating to domestic and international transactions, whether already implemented or that there was an attempt to implement them, for a period of at least five years from the date of the transaction or attempt to implement it.
3. Records relating to risk assessment and any associated information for a period of five years from the date of implementation or updating.
4. Internal reports of suspicious activity or investigations made by staff to the MLRO, and subsequently by the Money Laundering Reporting Officer (MLRO) to the Financial Information Unit (FIU) must be recorded on file for at least five years from the date of submission of the report, and should be kept separately from the main customer file.

5. Records of all training programs for money laundering and terrorist financing that have been carried out for a period of not less than five years. These records shall include the dates on which training was provided, the names and qualifications of the trainees and the person who carried out the training both inside and outside.

13. Suspicious Activity &Transactions Monitoring

- Suspicious transactions are financial transactions that have reasonable grounds to suspect are related to the commission of a money laundering offence. This includes transactions that which have reasonable grounds to suspect are related to the attempted commission of a money laundering offence.
- Suspicious transactions also include financial transactions that have reasonable grounds to suspect are related to the commission of a terrorist activity financing offence. This includes transactions that have reasonable grounds to suspect are related to the attempted commission of a terrorist activity financing offence.
- The suspicion is linked to the subjective and personal assessment of the person responsible for the examination of the suspicious process, based on evidence of conviction, but it does not reach the stage of final confirmation.
- It is very difficult to define what is and what is not suspicious; what may be suspicious to you may not be suspicious to your supervisor, manager of another employee. If you know your customer and understand his/her business, the transactions will follow a particular pattern. Looking at the customer's transaction records for the past six months can often reveal this. It is the transactions that do not fit into a pattern that may be suspicious to you.
- An Automated Transaction Monitoring System, which implemented by Al Khaleej Bank use profiling and/or rules-based monitoring methods.
- Profiling identifies unusual patterns of customer activity by applying statistical modelling techniques. These compare current patterns of activity to historical activity for that customer or peer group.
- Rules-based monitoring compares customer activity to fixed pre-set thresholds or patterns to determine if it is unusual.
- Transactions should be monitored based on a customer profile and specific details relating to that customer. The monitoring rules can reflect a number of factors relating to that customer (e.g. aggregate transactions, type, amount, frequency, business).
- Following are the main indicators of suspicious financial transactions:

1) Cash

- Cash transactions conducted in an unusual amount from that of usually conducted by the relevant customer.
- Transactions conducted in a relatively small amount but with high frequency.
- Transactions conducted by using several different individual names for the interest of a particular person
- The foreign currency exchange or purchase in a relatively large amount.
- The purchase of travelers checks in cash in a relatively large amount.
- The purchase of securities by cash, transfer, or checks under other person's name.

2) Economically irrational transactions

- Transactions having no conformity with the initial purpose of account opening.
- Transactions having no relationship with the business of the relevant customer.
- Transaction amount and frequency are different from that of normally conducted by the customer.

3) Fund transfers

- Fund transfers to and from high-risk offshore financial centers without any clear business purposes.
- Receipts of fund transfers in several phases and once accumulated the funds are subsequently transferred entirely to other account.
- Receipts and transfers of funds at the same or approximately the same amount and conducted in a relatively short period.
- Fund payments for export import activities without complete documents.
- Fund transfers from or to other high-risk countries.
- Fund transfers from or to other high-risk parties.
- Receipts/payments of funds made by using more than one account.
- Sends and receives a lot of fund transfers from the same recipient
- Sends fund transfers to a country other than the client's nationality
- Sends fund transfers to a group associated with terrorist activity

4) Cards:

- Information mismatch from application;
- Application information/address/customer differs from pre-screened applicant;
- Inability to verify card holder identity information;
- Primary/secondary user name appearing on applicable government watch/sanctions lists;
- Change of address to high-fraud area or to problematic jurisdiction, shortly after the card issuance
- Frequent and unusual use of the card for withdrawing cash at ATMs;
- Unusual purchase of goods or services in countries regarded by Al Khaleej Bank as posing a heightened risk for money laundering;
- Purchases at merchant on personal cards which are significantly out of pattern with historical spending behavior;

5) Behaviors of the Customer:

- Hesitant to give an explanation or details about the transaction.
- Hesitant to give information about the third party.
- Unreasonable behaviors of the relevant customer when conducting a transaction.
- Customer/prospective customer gives false information with respect to his/her identity, sources of income or businesses.
- Customer/prospective customer uses identification document that is unreliable or alleged as fake such as different signature or photo.
- Customer opens account for a short period.
- Customer is unwilling to provide right information or immediately terminating business relationship or closing his/her account at the time the officials request information with respect to his/her transaction.

14. Suspicious Activity Reporting (SAR)

1. After review, if unusual activity is identified, the responsible employee must evaluate all relevant information to determine whether the activity is really suspicious.
2. A suspicious transaction report is submitted to FIU in respect of a financial transaction that occurs or is attempted, and for which there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of a money laundering or terrorist activity financing offence.
3. The Head of Compliance is the competent person who reports suspicious cases to the FIU under Article 6 of the AML / CFT Act 2014 in accordance with the reporting format prepared by the FIU for this purpose.
4. The Bank shall not be inform the Client - in any circumstance - of the suspicious transaction or report it to the FIU. The utmost caution should be exercised in dealing with the Client.
5. The Bank must retain copies of SARs and supporting documentation for five years from the date of filing the SAR. The bank can retain copies in paper or electronic format, and must provide all documentation supporting the filing of a SAR upon request by FIU or an appropriate law enforcement or federal banking agency. "Supporting documentation" refers to all documents or records that assisted a bank in making the determination that certain activity required a SAR filing.

15. Money Laundering/Terrorist Financing Risk Assessment

The Bank applies a risk-based approach which is defined as a process encompasses the following:

1. The risk assessment of the bank business activities and clients using certain prescribed elements:
   - Different customer categories (individuals, companies, banks, cashiers, etc.)
   - Quality of products and services provided to customers
   - Service delivery channels
   - Geographical regions
2. The mitigation of risk through the implementation of controls and measures tailored to the identified risks;
3. Keeping client identification and, if required, beneficial ownership and business relationship information up to date in accordance with the assessed level of risk;and
4. The ongoing monitoring of transactions and business relationships in accordance with the assessed level of risk.

16. Employee Training Program

1. The Bank provides AML / CFT training to employees who will be dealing with customers or will be involved in any AML checking, verification or monitoring processes. The Bank may conduct its training internally or hire external third party consultants.
2. The Bank's AML training program is aimed to ensure its employees to receive

appropriate training level with regards to any possible AML/TF risks.

3. In general, the Compliance Manager is responsible for the AML / CFT training program in coordination with the Bank's Training Department
4. The Bank's AML and risk awareness training includes the following content:
    a. The Bank's commitment to the prevention, detection and reporting of ML and TF
    b. Well known or recognized typologies, especially where made available by the FATF or AML Supervisors.
    c. Those particular responsibilities of employees as identified in this AML Policy, and how employees are expected to follow the Bank's AML procedures.
    d. How to identify and report unusual activity that may be a suspicious transaction or attempted transaction.
    e. The rules that apply against unlawful disclosure of suspicious transactions
5. The Training Unit maintains a training register for each session
6. Special anti-money-laundering and terrorist financing courses will be held for new employees

17. Compliance with anti-money laundering policy

Compliance with this policy is essential in order to enable the Bank to comply with all relevant laws. All bank employees, managers and directors must be fully aware of the requirements of this policy. They must be aware of any suspicious financial transaction and immediately report it to the compliance officer.

18. AML Audit & Review

Al Khaleej Bank must conduct an ongoing testing process, including the audit, keeps the AML program current and effective against money laundering and fraudulent activities. Review of the KYC, AML, and Sanctions policy. Ascertaining whether policies, procedures and internal controls associated with KYC, AML, sanctions, laws, rules and regulations are appropriately documented, up to date and effectively communicated to the bank staff.

19. Policy amendment

This policy is amended only by the Compliance Manager if required and the amendment must be presented to the Board of Director for approval.

20. Scope of application:

This policy applies to the head office and all branches and subsidiaries.