

Rastriya Banijya Bank Limited

AML/CFT Policy
2074

Contents

Chapter 1

General Background.....	3
1.1 Introduction, Short Title, and Commencement.....	3
1.2 Definitions of Terms	3
1.3 Objectives of the AML/CFT Policy	7
1.4 Scope and Availability	8
1.5 Money laundering and Financing of terrorism.....	8
1.5.1 Money Laundering Process.....	8
1.5.2 Risk of Money Laundering And Terrorist Financing.....	8

Chapter 2

Legal and Regulatory Obligations and International Standards.....	10
2.1 Legal and Regulatory Obligations	10

Chapter 3

Know your Customer (KYC)/ Customer Due Diligence (CDD)	11
3.1 Purpose of KYC/CDD.....	11
3.2 KYC Policy Elements	11
3.3 Types of CDD	12
3.4 Beneficial Ownership.....	12
3.5 PEPs	12
3.6 KYC Review and Update.....	13

Chapter 4

Risk Based Approach.....	14
4.1 ML/TF risks	14
4.2 Sanctions risks.....	14
4.3 Customer risks.....	14
4.4 Customer risk rating.....	15

Chapter 5

Account and Transaction Monitoring and Reporting.....	16
5.1 Monitoring.....	16
5.2. Reporting.....	16
5.3. Record keeping.....	17

Chapter 6

Governance and Internal Controls for AML/CFT.....	18
6.1. Roles and Responsibilities	18

Chapter 7

Compliance Management.....	22
7.1. Implementation Strategies.....	22
7.2. Action Plan and compliance.....	22
7.3. Training & Awareness	23

Chapter 8

Miscellaneous.....	24
8.1. Amendment to the policy	24
8.2. Interpretation	24
8.3. AML/CFT Procedure	24
8.4. Action.....	24
8.5. Repeal and Saving.....	24

Chapter 6

Governance and Internal Controls for AML/CFT.....	18
6.1. Roles and Responsibilities	18

Chapter 7

Compliance Management.....	22
7.1. Implementation Strategies.....	22
7.2. Action Plan and compliance.....	22
7.3. Training & Awareness	23

Chapter 8

Miscellaneous.....	24
8.1. Amendment to the policy	24
8.2. Interpretation.....	24
8.3. AML/CFT Procedure	24
8.4. Action.....	24
8.5. Repeal and Saving.....	24

Chapter 1

General Background

1.1 Introduction, Short Title, and Commencement

Money laundering is the process by which illegal funds and assets are converted into legitimate funds and assets. Such funds are generated through illegal or criminal sources. Terrorism Financing is an act of supporting terrorist, terrorist group or terrorist conduct financially and with any other type of contribution. For any financial institution, there is a risk of its products and services being used to launder money and finance terrorism. Wealth collected through various predicate offences is brought into financial system with the intention of disguising the source of wealth.

AML/CFT is a strategic mechanism to ensure transparency and stability in financial system and broader economy. Its contribution to control financial crime is developing incredibly in the world. The role of banks and financial institution in this regard is substantially increasing as the foundation of the AML/CFT system.

In order to prevent the Bank from being used for money laundering and financing of terrorism, the Board of Directors of Rastriya Banijya Bank Limited (hereinafter referred to as the "Board") has approved this policy as provided by Section 133(2) of the Banks and Financial Institutions Act, 2073. This policy has laid down an appropriate framework for the effective compliance of the prevailing Asset (Money) Laundering Prevention Act 2064 (Second Amendment), Anti (Money) Laundering Prevention Rules 2073, and the Directives issued by the Financial Information Unit (FIU) and Nepal Rastra Bank (NRB) from time to time.

Name of the Policy Document shall be "Rastriya Banijya Bank Limited AML/CFT Policy 2074" and the possession of the Policy shall remain on the Compliance Department, Rastriya Banijya Bank Ltd.

This Policy shall be deemed to have come into force from the date of approval from the Board.

1.2 Definitions of Terminologies

In this Policy, unless the subject or the context otherwise requires,

- **The Bank** shall mean Rastriya Banijya Bank Ltd.
- **The Board** shall mean Board of Directors of Rastriya Banijya Bank Ltd.
- **Chairman** shall mean the Chairman of the Board of Directors of Rastriya Banijya Bank Ltd.
- **Chief Executive Officer / (CEO)** shall mean the person appointed as the Chief Executive Officer of the Bank, appointed by the Board and entrusted with the overall management, administration and operations of the Bank and accountable to the Board.
- **Branch Manager** shall mean the head of branches of the Bank.
- **Department Head** shall mean the head of a particular department of the Bank.



- AML/CFT Committee shall refer to the Board level AML/CFT Committee of the Bank.
- AML/CFT Management Committee shall refer to the Management level AML/CFT Committee of the Bank
- Risk Management Committee shall refer to the Board level Risk Management Committee of the Bank.
- The Policy shall refer to "Rastriya Banijya Bank Limited AML/CFT Policy - 2074"
- **Money Laundering (ML):** Money laundering shall refer to any of the following acts:
 1. The conversion or transfer of funds, by any person who knows or should have known or there are sufficient grounds for suspecting that such funds are the proceeds of illegal sources, for the purpose of concealing or disguising the illicit origin of such funds or for assisting any person who is involved in the commission of the predicate offence to evade the legal consequences of his/her actions.
 2. The concealment or disguising of the true nature, source, location, disposition, movement or ownership of or rights with respect to funds by any person who knows or should have known or suspects that such funds are the proceeds of crime.
 3. The possession, acquisition or use of funds by any person who knows, should have known or there are sufficient grounds for suspecting that that such funds are the proceeds of crime.
- **Financing Terrorism:** An act committed by any person who in any manner directly or indirectly and willingly, provides or collects funds, support, or attempts to do so in order to use them by knowing that these funds may be used in whole or in part for the execution of a terrorist act or by a terrorist or terrorist organization.
- **"Act", "Rules" and "Directive":** In this policy, "Act" shall refer to the Asset (Money) Laundering Prevention Act 2064 and its latest amendment. The "Rules" shall refer to the Asset (Money) Laundering Prevention Rules 2073 and "Directive" shall refer to the Directives issued by Nepal Rastra Bank and Financial Information Unit.
- **Terrorist:** Any natural person or organization who commits any of the following acts:
 1. Commits or attempts to commit terrorist acts by any means, directly or indirectly, unlawfully and willfully.
 2. Participates as an accomplice in a terrorist act
 3. Organizes or directs others to commit terrorist act or
 4. Contributes or cooperates to the group of persons acting with a common purpose of commission of terrorist acts where such contribution or cooperation is made intentionally and with the aim of continuing the terrorist act or with the knowledge or the intention of the group to commit a terrorist act.
- **Corresponding Banking:** The provision of banking services by one financial institution (correspondent bank) to the customer of another financial institution (respondent bank).
- **Proceeds of crime:** Any property derived from or obtained directly or indirectly through the commission of money laundering or predicate offence and it shall also include any other property and economic advantage gained or derived from such property or any property transferred or converted into other property or advantage, in full or in part, from such property or advantage.



- Transaction: Any agreement made in order to carry out any economic or business activities and the term shall also mean the purchase, sale, distribution, transfer or investment and possession of any assets, or any other acts as follows:-

1. Establishing business relationship.
2. Opening of an account.
3. Any deposit or collection, withdrawal, exchange or transfer of funds in any currency or instruments, payment order by electronic or any other means.
4. Use of any type of safe deposit box (locker).
5. Entering/establishing into any fiduciary relationship.
6. Any payment made or received in satisfaction, in whole or in part, of any contractual or other legal obligation,
7. Any payment made or received in respect of a lottery, bet or other game of chance.
8. Establishing or creating a legal person or legal arrangement, or
Such any other act as may be designated by the Government of Nepal by publishing a notice in the Nepal Gazette.

- **Legal Person:** Any company, corporation, proprietorship, partnership firm, cooperatives, or any other body corporate
- **Legal Arrangement:** Trust (express trust) or other similar kind of legal arrangements.
- **Client/ Customer:** Any individual or entity seeking/attempting to enter or has already entered into a business relationship, or conducts a one-off transaction with the bank as principal or as a client/ agent. Any person or entity connected with a financial transaction that may impose significant reputational or other risks to the Bank.
- **Employee / Staff:** Employee / Staff shall mean the employee / staff of the Bank as defined in the Staff Service Bylaws of the Bank.
- **PEPs:** "PEP" shall mean a politically exposed person. PEPs are individuals who are or have been entrusted with prominent public functions in Nepal and in foreign countries. The term shall also mean the family members and close associates of such persons.

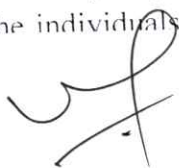
Explanation: Family members shall include the following types of relationship/s:

- i. Parents and children of PEPs;
- ii. Spouse/partner
- iii. Siblings
- iv. Uncles and aunts
- v. Even slightly indirect family members (such as in-laws) will be considered as politically exposed persons.

Close associates include the following types of relationship/s:

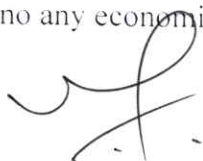
- i. Anyone who has a close business relationship or joint beneficial ownership of legal entities or legal arrangements with the PEPs.
- ii. Anyone who has the sole beneficial ownership of a legal entity which is known to have been set up for the de facto benefit of the PEPs.

- **Domestic Politically Exposed Persons (PEPs): Domestic Politically Exposed Persons (PEPs)** shall mean the individuals who are or have been entrusted domestically with prominent public



functions. For example The President, Vice-President, Minister, parliamentarians, officials of the constitutional bodies, officials remained in the special class or equal to special class or their senior of the Government of Nepal, judge of the High Court and their senior, senior politician, central member of national political party or senior executives of any institution partially or fully owned by the Government. It shall also include other group of person as designated by the Government of Nepal upon the recommendation of National Coordination Committee.

- **Foreign Politically Exposed Person: Foreign Politically Exposed Person** shall mean the individuals who are or have been entrusted with prominent public functions by foreign country, for example Head/s of State or of government, senior politician, central member/s of the national level political party, senior government, judicial or military official, senior executives of state owned corporations of a foreign country.
- **Beneficial owner: Beneficial owner** shall mean any natural person who, directly or indirectly, owns or controls or directs or influences a customer, an account, or the person on whose behalf a transaction is conducted, or exercises effective control over a legal person or legal arrangement or remains as an ultimate beneficiary or owner of such activities.
- **Customer Due Diligence (CDD):** Customer Due Diligence shall mean the process of identifying and evaluating the customer/s and the assessment of customer risk as a part of know your customer (KYC) process, allowing banks to better identify, manage, and mitigate the AML related risks. The level of due diligence is based on the risk level of the customer and, thus, there may be various levels of due diligence prescribed by the regulator/s or may be decided by the bank itself. Currently, followings are the categories of due diligence specified by the NRB Directives:
 1. **Simplified Customer Due Diligence (SCDD):** Simplified CDD is the lowest level of due diligence that can be completed on a customer with low risk category.
 2. **Standard/Normal Customer Due Diligence:** This is conducted for medium risk customers who do not fall under enhanced and simplified customer due diligence.
 3. **Enhanced Customer Due Diligence (ECDD):** Enhanced Customer Due Diligence is conducted for high risk customers. It refers to the additional due diligence pertaining to the identity of the customer, source of income, nature and value of transaction and others specified by directives.
- **Risk Based Approach (RBA): Risk Based Approach (RBA)** shall mean the approach of management which focuses on identifying and addressing potential risks of money laundering and terrorism financing. The core element of this approach is to create the match between "risks and controls" by understanding of the ML/TF risks to which the banks are exposed and apply AML/CFT measures in a manner and to an extent which would ensure mitigation of these risks. There is no universally accepted methodology, which prescribe nature and extent of risk based approach. It provides every bank the flexibility to manage their ML/FT risks in their own way.
- **Suspicious Transaction: Suspicious Transaction/s** shall mean the transaction/s, including an attempted transaction, whether or not made in cash, which to a person acting in good faith:
 1. Gives rise to a reasonable ground of suspicion that it may involve proceeds of an offenses specified by the prevailing law/s, regardless of the value involved;
 2. Seeks to conceal or disguise the nature or origin of funds derived from illegal activities;
 3. Appears to have no any economic rationale or bona-fide purpose;



4. Appears to be in circumstances of unusual, or unjustified complexity;
 5. Appears to be deviated from profile, character and financial status;
 6. Seems to be made with the purpose of evading the legal and regulatory reporting requirements and
 7. Is found to be conducting or supporting the activities relating to terrorism.
- **Suspicious Transaction Report: Suspicious Transaction Report** shall mean the report to be made by Financial Institutions to Financial Information Unit on any suspicious transaction/s or any attempts under the provisions of "Chapter 3, Section 7dha of the Asset (Money) Laundering Prevention Act 2064" and point no. 19 of the NRB Directives No. 19.
 - **Wire Transfer: Wire Transfer** shall mean any transaction carried out on behalf of an originator (both natural persons and legal entities) through the bank by electronic means with a view to make an amount of money available to a beneficiary at any another FI. The originator and the beneficiary may be the same person/s.
 - **Financial Information Unit (FIU): Financial Information Unit (FIU)** shall mean the Financial Information Unit (FIU established on April 21, 2008 pursuant to Section 9 of the Assets (Money) Laundering Prevention Act, 2008 within Nepal Rastra Bank (the Central bank) as an independent unit in order to work against the money laundering and terrorist financing activities. It is the financial intelligence unit of the State of Nepal. It is the central, national agency accountable for receiving, processing, analyzing and disseminating financial information and intelligence on suspicious money laundering and terrorist financing activities.
 - **Shell Bank/entity: Shell Bank/entity** shall mean any bank or entity, which has no physical presence in the country in which it is incorporated, licensed or located, and which is not affiliated with a regulated financial services group that is subject to effective consolidated supervision. For the purpose of this clause, presence of local agent or junior level staff does not constitute physical presence. Shell banks/entities in themselves may not be illegal as they may have legitimate business purposes. However, they can also be a main component of underground activities, especially those based in tax havens.

One of the classic tax avoiding activities can be buying or selling of Shell Companies established in tax havens to disguise the actual profit/s. Furthermore a firm may carry out its international operations through these types of entities and not report to its home country about the sum involved and thereby avoid tax obligation/s.

1.3 Objectives of the AML/CFT Policy

The followings shall be the objectives of the Policy:

2. To develop a sound mechanism for the compliance of AML/CFT measures as required by the legal, regulatory, and international practice/convention/s.
3. To adopt Risk-Based Approach and functionally adequate system controls.
4. To enable conducive business environment in compliance with the AML/CFT standards in an economical and effective manner.
5. To develop protective environment for the Bank, its employees and the clients.



6. To establish the Bank as the leading Financial Institution in AML/CFT system implementation.

1.4 Scope and Availability

The policy shall be applicable to all of the banking operations of the Bank, including the Central office, Regional Offices, all branches, and representative offices. This policy shall be enforced in alignment with the AML/CFT Procedures, 2074 by all of the staffs of the bank in their respective role.

1.5 Money laundering and Financing of terrorism

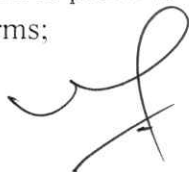
A person, natural or legal, conducting various predicate offences may place the proceeds of crimes into the banking system, create different layers to disguise the origin of the money and integrate the money into regular purchase and investment activities. An overview of money laundering and terrorist financing activities is provided as follows:

1.5.1 Money Laundering Process

- A person collects money from various predicate offences in the areas such of tax evasion, corruption and bribery, forgery, corporate crime, fraud and organized theft, organized crime, illegal logging/fishing, illicit narcotics trafficking, counterfeiting/piracy of products, counterfeiting currency, illicit arms trafficking, people smuggling, terrorist financing etc.
- The money is placed in to the financial system via banks. Various channels such as funds transfer, deposits, foreign exchanges etc. are used for this purpose. This process is known as placement. This is the first stage of money laundering.
- Second stage is stage of layering. Different layers are created around the money using transfer between offshore/onshore banks to hide the origin of the money. At this stage, money launderers use.... different techniques to layer the funds like using multiple banks and accounts having professionals act as intermediaries and transacting through corporations and trusts. This helps launderers to disguise the origin of funds.
- The final stage is called the stage of integration. The cleaned money is now integrated into the financial system for regular purchase and investment for future. Thus, the original 'dirty' money has achieved the appearance of legitimacy.

1.5.2 Risk of Money Laundering and Terrorist Financing

Risk of misuse of banking system/s for criminal proceeds is the consequence of Money Laundering and Terrorist Financing. Money laundering and terrorist financing risks posed by each customer accumulates to form institutional risk of the Bank. Failure to reduce money laundering and terrorist financing risks by each bank shall result into sectoral risk and towards national money laundering and terrorist financing. A banking institution is prone to following risk due to Money laundering and terrorist financing in any of the following forms;



- **Reputation risk:** When money laundering and terrorist financing activities are permitted, in the bank, its reputation could be damaged irreparably. A strong AML/CFT/CDD policy will help to prevent a bank from being used as a medium for illegal activities.
- **Compliance risk:** Failure to prevent/minimize money laundering and terrorist financing activities will result into non-compliance of its banking operations with the AML/CFT compliance standards.
- **Legal risk:** The bank may face legal sanctions and/or fines from the regulatory bodies.
- **Financial risk:** the banking system may lose control over its financial structure and flow and funds.
- **Operational risk:** In the absence of AML/CFT/CDD policy or in case, such policies are not implemented properly, there may be a chance of resource wastage and a chance that the resources may be used by the criminals for illegal purpose, giving rise to wastage of time and money which will make the bank operationally unsound.



Chapter 2

Legal and Regulatory Obligations and International Standards

2.1 Legal and Regulatory Obligations

The general legal framework of AML/CFT in Nepal includes the efforts of controlling money laundering, predicate offences and terrorism financing. Prevailing laws in AML/CFT sector in Nepal include the followings:

1. AML/CFT Act, 2064,
2. AML/CFT Rules, 2073,
3. Nepal Rastra Bank (NRB) Directives on AML/CFT to Banking and Financial Institutions,
4. NRB Directives to Money Value Services,
5. NRB, FIU Guidelines on TTR,
6. NRB, FIU Guidelines on STR,
7. Correspondent bank's requirements in AML/CFT,
8. NRB FIU AML/CFT Directives
9. Related international standards on AML/CFT,
10. Other normative measures related to banking, money-value businesses, financial and other crimes.

The legal and regulatory obligations that Rastriya Banijya Bank Limited shall follow are provided by the above stated legal/institutional framework. The primary legal obligations include the KYC/CDD management, Sanction Screening, Risk Based Assessment and Management, Monitoring, detecting suspicious transaction, reporting, TTR, STR to FIU and regulatory information to Nepal Rastra Bank, and record keeping. It shall also be the legal duty of the bank to support initiatives taken by the regulator, FIU, Law Enforcement Agencies and other concerned authorities.

2.2 International Standards

AML/CFT international standards are the general guidelines for the overall activities of the bank. Since the bank is one of the players in the international financial system and the part of domestic and international payment, it has very significant role in common international efforts against money laundering and terrorism financing as well as combating other financial crimes. The Bank has made commitment to maintain AML/CFT standards issued by the Financial Action Task Force, Basel Committee and other concerned International Organizations.



Chapter 3

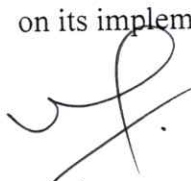
Know your Customer (KYC)/ Customer Due Diligence (CDD)

Customer Due Diligence (CDD) is a process of identifying a customer trying to maintain business relationship or has already maintained such relationship or has requested for or already conducted one-off or similar transactions. It is required to identify and verify the customer/s; to assess the risks and manage the risks; to develop risk-based, effective, efficient and economic monitoring system; and to identify further business potential. The CDD process has to be continued to a certain period of time even after such relationship has terminated or transaction has been completed. CDD is a process to review overall activities of a customer and reach to a conclusion. However, Know Your Customer (KYC) and CDD are sometimes taken synonymously. Both of them can be taken as a unit.

3.1 Purpose of KYC/CDD

The purpose of KYC/CDD process is to identify ground truth about the customer's background for prospective money laundering and terrorist financing risk associated. Such identification of characteristics and behavior of customers, customer's customers and employees is crucial to identify theft, prevent terrorist financing, money laundering and financial fraud. It shall help to understand the customer better and manages risk prudently.

3.2 KYC Policy Elements

1. **Customer Acceptance:** The point at which a new customer is accepted or rejected is the easiest point at which the risk of dealing with illegal money can be avoided. The Bank follows good customer acceptance policies while dealing with entities and individuals who might engage in illegal transaction/s can be avoided.
 2. **Customer Identification and Verification:** Establishing the identity of customers and verifying by using reliable, independent source documents, data or information to the Bank's satisfaction is the core of the KYC policy both for the customer acceptance or rejection decision and for the ongoing monitoring of customer accounts and transactions. The Bank ensures that it follows customer identification and verification procedures while dealing with the customer/s.
 3. **Accounts and Transactions Monitoring:** The Bank ensures that all its customers and transactions are regularly monitored through the threshold based monitoring, suspicious transaction monitoring and ongoing monitoring for high risk customers.
 4. **Risk management:** To make sure that the risks posed by money laundering and other criminal activities are identified, mitigated and managed, the bank follows the risk management practices. The bank will assess the customer under risk assessment as high, medium and low risk. Moreover, the bank will have its board approved policy, procedures and management oversight on its implementation.
- 

3.3 Types of CDD

Based on different levels of risk, the Bank will adopt the following 3 types of CDD.

- **Simplified CDD:** Simplified CDD is the lowest level of due diligence that can be completed on a customer. This will be implied to the customer with low risk category. The customer risk categorization will be conducted in AML/CFT IT system as per the AML Act, AML rules and NRB Directives.
- **Normal CDD:** Normal CDD is implied to the customers in general or in medium risk or those who do not fall under High Risk or Low Risk. The AML/CFT IT system of the Bank provides workflow for entering, storing, updating, and retrieval of the normal CDD information.
- **Enhanced CDD:** Enhanced CDD is applied to the customers categorized as high risk under AML/CFT IT system. ECDD includes higher degree of CDD that requires collection of additional information and documents as well as surveillance in every stage of transaction. Prior approval should be taken from high level of authority during account opening and high value transaction for such high risk customers. The Bank can terminate the relationship with the customers or can postpone the transaction in case, they are unable to comply with CDD and consider due examination thereon. The bank shall develop ECDD form in order to conduct ECDD of high risk customers.

3.4 Beneficial Ownership

The bank will ensure that the staffs of the bank are accountable enough to establish and verify the identity of the ultimate natural person, who owns or controls the customer or its assets or on whose behalf the transaction is being carried out or the business relationship is being established or transaction is being conducted at each and every stage of transaction. The staff/s shall obtain the information about the beneficial owner from the customer, publicly available sources and business domain and shall deploy sanction screening programs to safeguard itself from establishing, maintaining relationship or carrying out transaction of a person, group or organization in which a party is sanctioned or directly or indirectly linked to a transaction or is Beneficial Owner (BO) or beneficiary. It shall instigate a control measures for safeguarding the Bank against being used as a conduit for ML, TF, PF and other crimes.



3.5 PEPs

The Bank will develop a timely update system and maintain the list of high ranking officials and politically exposed persons as per the prevailing law of the state. The Bank will also adopt an IT system for identifying, monitoring and managing risks associated with this



3.6 KYC Review and Update

Review and update of customer's information is very essential and critical for a better KYC system application. The Bank has been following a periodical system of updating the customer identification data (including photograph/s) as and when an account has been opened or any transaction is being carried out.



0



Chapter 4

Risk Based Approach

The bank incorporates a Risk Based Approach (RBA) for the implementation of AML/ CFT measures. It is ensured that an effective CDD program is in place, which is possible by establishing the appropriate procedures and their effective implementation based on risk.

4.1 ML/TF risks

Use of financial systems for money laundering or financing terrorism creates a serious threat to the state, society and the overall economy. Different vulnerability points such as entry of cash into financial system, cross-border flows of cash, transfer within the financial system, acquisition of investments and other assets, incorporation of companies and formation of trusts are used to launder money. Terrorist groups and organizations may find financial support and conduct revenue generating activities via terrorist financing. The bank with the help of policy/procedures and AML/CFT IT system aims to minimize this risk.

4.2 Sanction risks

Sanction designated individuals and entities pose greater threat of money laundering and terrorist financing. Enrollment of such individuals and entities into the financial system and delivery of financial services for such individuals/ entities are strictly prohibited. The Bank uses United Nations' Sanction List of individuals and entities and OFAC's Specially Designated Nationals list of individuals, entities, cargo, and vessels. Screening against these lists prohibits sanctions designated persons from enrolling into the banking systems as well as restrict further interactions with the bank. The list of the sanctions includes:

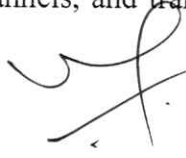
- United Nations Sanction List
- The Office of Foreign Assets Control (OFAC) List of the US Department of the Treasury
- HM Treasury List of Office of Financial Sanctions Implementation, HM Treasury, UK
- Consolidated list of sanctions of European Union External Action

Other sanctions lists shall be incorporated as and when deemed necessary by national and international AML/CFT law and practice.

Business relationship or transaction directly or indirectly related with a person, group or activities under the sanction list including false-positives shall be frozen at the very time of identification.

4.3 Customer risks

Natural as well as legal persons trying to establish relationship with financial system pose certain level of risk as per their background, occupation, affiliated industry, subscribed products, services, and delivery channels, and transactions. Risk profile of each customer is established while enrolling to the



Bank, performing transactions, and other routine operations such as regular profile update, sanction lists update, PEP database update etc.

4.4 Customer risk rating

The Bank uses scientific risk rating of its customers that includes risk analysis of customer's background, occupation, industry, products subscribed, services subscribed, delivery channels subscribed, geographic footprints and transaction patterns.

4.1. Risk Management

The Bank shall adopt a proper management, oversight, systems, controls, segregation of duty, training and other related matters. All activities of the Bank shall be conducted on risk based approach. Systematic and scientific approach including assessment, analysis, scoring, and adaptable methodology will be applied for the assessment of risk as provided in the AML/CFT Procedure of the Bank.

DI h N

uf.

Chapter 5

Account and Transaction Monitoring and Reporting

5.1 Monitoring

The Bank shall ensure that a sound monitoring system is in place to detect unusual/unrealistic/suspicious activities/transactions. Once the customer is on-board... monitoring the relationship, transaction, and activity of customer/s shall be the major focus of the Bank. Effectiveness of monitoring shall also be the target of the compliance, audit, and the management of the Bank.

The automated system shall be the primary tool of monitoring. Every transaction shall be monitored on a regular basis for making revaluation of the customer/s for risk grading and for any suspicious transaction/s. Staff/s of the Bank shall be required to review the monitoring tools on a timely basis and add value to the AML/CFT IT system accordingly. Human monitoring shall be another regular tool for the system. Generally, monitoring shall be made as follows:

- Customer accounts are monitored for profit changes, nature of business change etc.
- Transactions are monitored for threshold transactions and suspicious activities.

For the effective monitoring, the bank shall adopt a strategy of regular KYC/CDD update and review mechanism so as to discover the ground/s of truth and realistic picture of the business relationship and activities.

5.1.1 Threshold Transaction

Transaction/s crossing the threshold/s in their respective types of transaction/s shall be monitored and reported accordingly.

5.1.2. Suspicious Transactions

Transaction/s shall also be matched against the suspicious transaction patterns as prescribed by Nepal Rastra Bank as well as against the industry standard.

5.1.3. Customer Profile

Changes in customer's background, occupation, industry, associations, adverse activities, products subscribed etc. shall also be monitored and reflected into the AML/CFT IT system so as to incorporate them into the monitoring process.

5.1.4. Lists

The customer shall also be monitored regularly against the sanctions lists upon the update.

5.1.5. Others

Other lists such as PEPs lists, adverse media lists, risk changes in products and services shall also be monitored continuously.

5.2. Reporting

Reporting is the cardinal organ of AML/CFT regime. The Bank shall make the optimum focus in identifying, preparing and submitting the qualified reports as follows:



- Regulatory reports
- FIU reports
- Law enforcement reports
- Internal reports
- Other reports

5.2.1. Threshold Transaction Reports

Threshold transaction reports are submitted to the respective regulatory body in every 15 days. The reports shall also be submitted to other competent authorities accordingly, as and when required.

5.2.2. Suspicious Transaction Reports

Upon occurrence/notification of any suspicious transactions/activity, a case shall be prepared analyzing the background of the customer/s and the transaction/s patterns. Then the case is reported to the respective regulatory body within 3 days of the occurrence of the cause.

5.2.3. Cash withdrawal transaction

The Bank shall prepare a cash withdrawal report every month in the format as prescribed by Nepal Rastra Bank.

5.2.4. Others

Sensitive information/s related to offence/s and investigation/s shall also be reported to the competent authorities accordingly.

5.3. Record keeping

Bank shall keep a record of every transaction, customer data, and data obtained for the purpose of identification, risk analysis, monitoring and other related information along with the date, time and nature. Similar record of the KYC/CDD documents, correspondence with the customers, sources of fund, as well as all of the documents related to money laundering activities, such as files on suspicious activity reports, documentation of AML account monitoring etc. shall also be maintained accordingly.

- The record/s shall be kept in a safe custody for a period of 5 years in minimum; until a new law/order/ policy require otherwise.
- The activity logs shall also be kept safe for at least 5 years period.
- Audit trails shall also be maintained accordingly

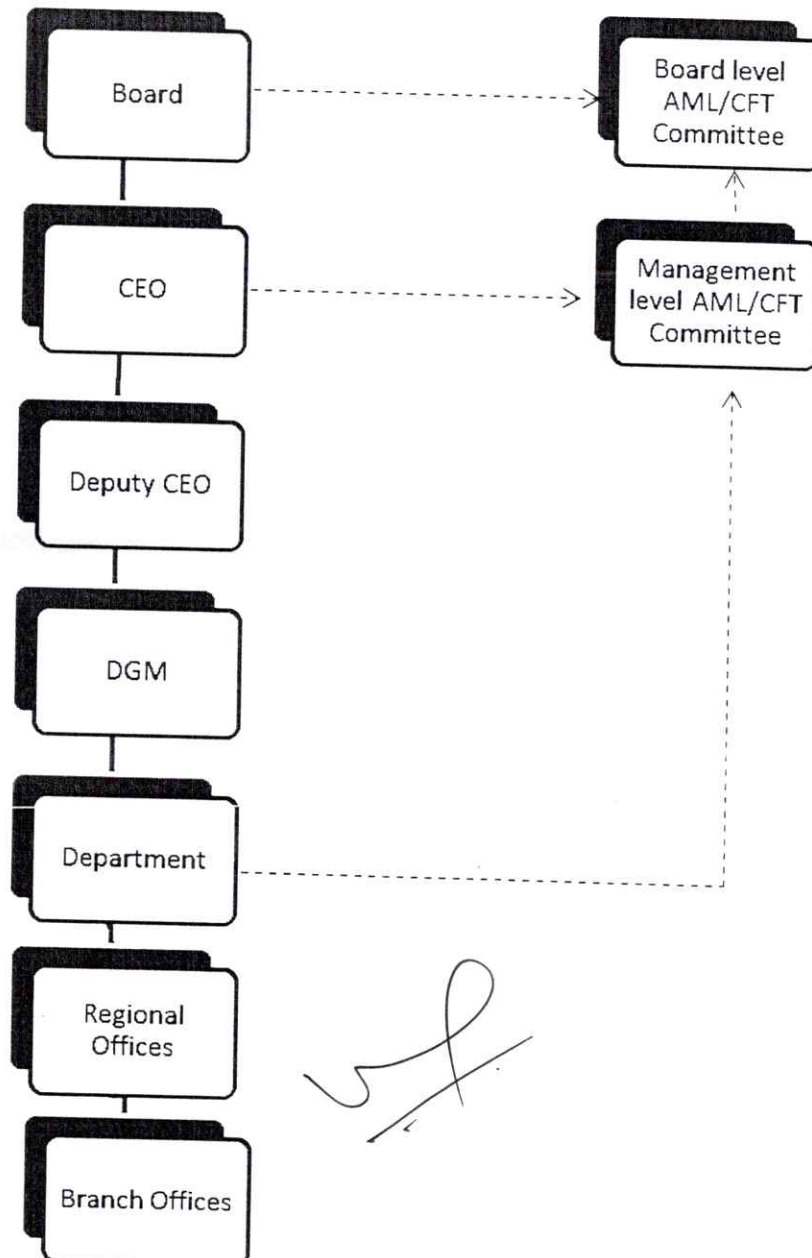


Q

Chapter 6

Governance and Internal Controls for AML/CFT

Governance structure assigns the accountability for designing the Bank's AML/CFT implementation and monitoring structure and an overall accountability for the output. To align with our business requirements, it incorporates the guidance from global standards, NRB Circulars and Directives and elements consistent with evolving the best practices. The key elements of compliance governance structure shall be as below:



6.1. Roles and Responsibilities

The section below details the various roles and responsibilities of the governance structure for AML/CFT Compliance.

6.1.1. Roles and Responsibilities of the Board of Directors

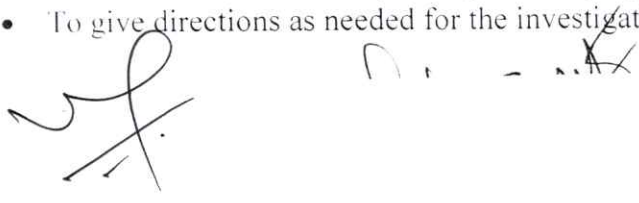
- Approving and enforcing internal AML/CFT policy, procedure and guidelines.
- Establishing and approving the organizational structure, roles and responsibilities in AML/CFT of individual/department/unit.
- Review AML/CFT system as per the NRB guidelines.

6.1.2. Roles and Responsibilities of AML/CFT Board Committee

AML/CFT Committee is the Board Level Committee which shall constantly monitor the norms of AML/CFT being taken by the Bank. The illustrative but not exhaustive roles and responsibilities of AML/CFT Committee related to this Policy shall be as follows:

- Review and support AML/CFT Policy for the purpose of approval from the Board of Directors.
- Evaluate and review the reports submitted by Management level AML/CFT committee.
- Review AML/CFT related activities and implementation of policy and procedures and submit its report to the Board of Directors.
- To make schedule of the reports submitted by management level AML/CFT committee for the evaluation, monitoring and directions as needed.
- To perform the related activities for the implementation of Anti Money laundering Act 2064, and NRB directives.
- To give additional directions to the management level AML/CFT committee as per the requirement.

6.1.3. Roles and Responsibilities of management level AML/CFT

- To approve the AML/CFT Policy and Procedures presented by Compliance Department and submit that to Board level AML/CFT Committee.
 - To monitor and evaluate the corporate governance and money laundering related activities performed by the Bank and give directions to Compliance Department as per the requirement.
 - To evaluate the activities at least once a month in order to ensure that the activities performed are as per the prevailing act. Rules and Directives submit the report to Board level AML/CFT committee.
 - To give approval for the capacity enhancement programs conducted for the staffs working in AML/CFT unit and compliance department.
 - To act as a liaison between Board level AML/CFT committee and Compliance Department as required.
 - To make annual work plan of AML/CFT and KYC and submit to the Board level AML/CFT Committee and evaluate quarterly for the proper implementation.
 - To give directions as needed for the investigation of AML/CFT and KYC related issues.
- 

- To review the reports submitted by compliance department and submit it to Board level AML/CFT Committee for the implement of remarks and suggestions.
- To evaluate the activities performed by compliance department and submit report to the Board level AML/CFT Committee.
- To evaluate the implementation of the remarks and suggestions as remarked in report submitted by Nepal Rastra bank during supervision and monitoring and also submit report of record keeping to Board level AML/CFT committee.
- To evaluate whether the prevailing laws and NRB directives are complied or not and mention in the report accordingly.
- To evaluate whether the banking activities ensure continuity, relevancy, effectiveness, and efficiency and submit report to Board level AML/CFT Committee.
- Bank should manage the adequate manpower and resources for the management level AML/CFT Committee in order to perform their roles and responsibilities. Management level AML/CFT committee should prepare their own work plan and work accordingly.
- To perform the related activities for the implementation of Anti Money laundering Act 2064, and NRB directives.
- To perform as per the prevailing laws and rules.

6.1.4. Roles and Responsibilities of the Chief Executive Officer (CEO)

Chief Executive Officer is the head of the management who shall be primarily responsible for the implementation of the Policies/procedure and guidelines of the Bank/Regulators and ensure an effective compliance of the same. The illustrative but not exhaustive roles and responsibilities of the Chief Executive Officer of the Bank related to this Policy shall be as follows:

- Circulating and implementing the Policy approved by the Board.
- Carrying out and managing the Bank activities in a manner consistent with the business strategy, risk appetite and other guidelines provided and required by the Board.
- Ensuring that the bank has all the required procedural guideline in place to effectively achieve the objectives of this policy.
- Promoting compliance as a culture and considering AML/CFT compliance as a basic ethic of doing business.
- Approving all of the procedural guidelines containing the controls, monitoring and reporting procedures.
- Ensuring that sufficient resources and required access to information, documents and staffs have been arranged for carrying out compliance functions efficiently and effectively.
- Reviewing on quarterly basis as to whether or not the provisions of Anti-Money Laundering law, including the rules, directives, orders or policies have been formulated under such act are complied with and submitting a report to Financial Information Unit after completing the review of the same in three month from the end of fiscal year.
- Exercising other discretionary authorities accordingly, as delegated by the Policy or by the Board from time to time.

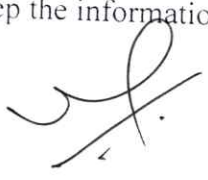


6.1.5. Role and Responsibilities of Compliance Department (In relation to and addition to AML Laws)

- Responding to account related queries received from the NRB and other concerned authorities.
- Responding to Suspicious Transaction compliance queries of/to branches/divisions.
- Reporting Threshold Transaction.
- Reviewing of AML and KYC compliance activities, making implementation and reporting them accordingly.
- Reviewing of CDD/ECDD/Customer Risk Categorization Report.
- Making Review of Compliance Risk Assessment
- Review of existing/new products, services, and processes from the compliance prospective.
- Critically analyze the action taken by the management and assure that they are consistent with the strategy and policies approved by the Board.
- Setting of code of conduct and reviewing the adherence by BOD, Employee, and all concerned as applicable.
- AML Questionnaire Reply of Nostro/Correspondent Banks/Remittance Partners.
- AML/CFT Risk Identification and Evaluation Report as per the requirement of NRB Unified Directives no. 19.
- Submit Compliance and compliance Audit report to D/CEO.
- Prepare AML/CFT report and submit it to the CEO.

6.1.6 Role and Responsibilities of the Compliance Officer

Designated officer at compliance Department and Operation in charge of the branches shall act as the Compliance Officer. The major responsibilities of the Compliance officers shall be as follows:

- To ensure compliance with AML Act, 2008 along with the internal AML/CFT policy and procedures.
 - To authenticate KYC as required under AML/CFT procedures.
 - To maintain record to KYC information as prescribed under AML/CFT procedure.
 - To maintain the record of transaction/s exceeding threshold limit and file Transaction Threshold Report to compliance department.
 - To file suspicious transaction/s report to the Compliance Department, of the transactions which do not match with the general financial status of the customer/s.
 - To keep the information of the customer/s confidential at all time.
- 

Chapter 7

Compliance Management

7.1. Implementation Strategies

The Bank shall materialize the objectives of the AML/CFT policy by the issuance of AML/CFT Procedures and establishment of necessary operational and system controls. The Bank concentrates on a systematic approach for

- Customer Due Diligence (CDD).
- Risk-Based Approach (RBA).
- Monitoring and Fraud Detection.
- Reporting.
- Internal Controls.
- Capacity Building.
- Review and Appraisal

7.2. Action Plan and compliance

The Bank shall develop annual plans and programs to implement AML/CFT system and conduct a regular review as well as annual appraisals to ensure its functioning, effectiveness, and further enhancement.

To ensure an effective implementation of AML/CFT measures, the Bank has developed standard procedures for customer due diligence, risk profiling and management, monitoring, reporting, governance and internal controls, record keeping, human resource management, and training and capacity building.

The bank shall integrate the AML/CFT measures with overall policies, strategies, plans, programs, management, functions, code of conduct, guidelines and other internal regulations.


7.2.1. Compliance measurement

AML/CFT shall be an integral part of the internal and external audit of the bank. In addition, the Compliance Department may conduct AML/CFT compliance assessment or make a review audit reports. Such reports and reviews along with reformative measures shall be regularly assessed and monitored by the CEO and the Board.

Compliance of AML/CFT framework shall be measured in the performance appraisal of officials and staff. It will be one of the major performance indicators.

7.2.2. Non-Compliance

The Bank adopts zero tolerance policy against non-compliance of AML/CFT measures. Any department, office, official or staff non-complying with AML/CFT framework shall be punished as per RBB personnel bye-laws and other prevailing laws.







7.3. Training & Awareness

The Bank has been conducting training and orientation programs to all existing as well as newly recruited employees on AML/CFT. All employees (including trainees and temporary personnel) responsible for carrying out transactions and/or for initiating and/or establishing business relationships shall undergo training and orientation. The Bank will conduct informative AML/CFT programme to its investor, BoDs, and Higher Level Management. The Bank shall also spread awareness amongst the customers about AML/CFT measures and the rationale behind them. An annual training schedule includes comprehensive training to all stakeholders of the AML/CFT program.

7.5. New Technology

The Bank shall have an AML/CFT-friendly new technology in system and interface it with the Core Banking System so that they could perform the entire tasks against the money laundering and terrorism financing and take appropriate measures to prevent the damages to the Bank from its customers. The Bank will ensure that appropriate KYC procedures are duly applied to the customers while using new technology driven products.



Chapter 8

Miscellaneous

8.1. Amendment to the policy

The Board of the bank may amend the policy for better compliance and performance.

8.2. Interpretation

The Board of the Directors may interpret the provision of the policy in case so required. Such interpretation shall be submitted to the Board for its information.

8.3. AML/CFT Procedure

The Board of the Directors shall issue the AML/CFT Procedure of the Bank. The procedure shall be applicable and mandatory to all Bank officials, and activities. Non-compliance of the AML/CFT procedure shall be punishable.

8.4. Action

The Bank shall integrate the AML/CFT compliance and action against non-compliance into its Personnel bye-laws and code of conduct of the staff.

The Bank shall develop and implement Know Your Employee (KYE) strategy and format under the Personnel bye-laws to control bribery and any other fraudulent activities.

The compliance officer shall be responsible for identifying and recommending AML/CFT non-compliance. Other responsible officials shall support the compliance officer in discharging his/her duty of identifying and recommending AML/CFT non-compliance.

8.5. Repeal and Saving

The Rastriya Banijya Bank Limited AML/CFT policy 2069 is hereby repealed. All actions taken and functions performed before the commencement of this Policy shall be considered to have been taken or performed pursuant to this Policy.

