

Rastriya Baniya Bank Limited

AML/CFT Procedures
2074

Contents

Chapter 1	3
General Provisions.....	3
1.1. Scope and availability	3
Chapter 2	4
Know Your Customer/Customer Due Diligence (KYC/CDD).....	4
2.1. Introduction to KYC/CDD.....	4
2.2 Types of CDD based on risk	8
2.3 Beneficial ownership.....	11
2.4 PEPs	12
2.5 Screening against Sanctions, Negatives and Adverse lists.....	13
2.6 KYC Update and review	14
Chapter 3	16
Risk Management.....	16
3.1 Risk-Based Approach Procedure	16
3.2 Risk Classification of Customers	17
3.3 Risk Based Approach Steps	19
Chapter 4	20
Monitoring.....	20
4.1 Steps of Monitoring.....	20
4.2 Steps of detecting suspicious transactions.....	21
4.3 STR Triggers	22
Chapter 5	27
Reporting.....	27
5.1 Threshold Transactions & Reporting	27
5.2 Suspicious Transaction Reporting.....	29
5.3 Tipping Off.....	29
Chapter 6	30
Governance and Compliance: Roles and Responsibilities.....	30
6.1 Roles.....	30
6.2 Role and Responsibilities of Customer Service Desk (CSD).....	30
6.3 Role and Responsibilities of Branch Manager.....	30
6.4 Role and Responsibilities of Compliance Officer.....	31

6.5 Role and Responsibilities of Compliance Department (In relation to and addition to AML Laws)	31
6.6 Roles and Responsibilities of Regional offices	31
6.7 Roles and Responsibilities of Chief Executive Officer (CEO)	32
6.8 Roles and Responsibilities of AML/CFT Committee	32
6.9 Roles and Responsibilities of AML/CFT management Committee	33
6.10 Role and Responsibilities of Audit Department	33
6.10 Roles and Responsibilities of Board of Directors	34
6.11 Roles and Responsibilities of Legal Department	34
6.12 Role and Responsibilities of Human Resource Department	34
Chapter 7	35
Record Keeping	35
Chapter 8	36
Miscellaneous	36
8.1 Employee Training Program	36
8.2 Amendment to the policy	36
8.3 Interpretation	36
8.4 Repeal and Saving	36
8.5 Code of Conduct	36
8.6 Departmental Action	37

Chapter 1

General Provisions

This procedure has been issued by the Chief Executive Officer (CEO) of the Bank, upon the recommendation of AML/CFT Board level Committee, by exercising the power provided under the AML/CFT Policy of the Bank. It shall be read and implemented in the spirit of AML laws, AML/CFT policy, operational and systems controls of the Bank, relevant international standard, and the best practices.

The Bank hereby, makes this standing order and requires that the Board, Management, Official, and staff/s of the Bank adhere to this procedure and broader framework of AML/CFT in respect to the discharge of their roles and responsibilities. Non-compliance and violation of the said norm/s shall be considered as a serious ground for taking departmental and other legal actions.

- a) Contradicting business relationship/s or transaction/s being carried on against the compliance of prevalent AML/CFT laws, AML policy of the Bank, and this procedure is strictly prohibited.
- b) This procedure shall be implemented fully by each and every staff/s of all of the departments of the Bank in their respective area of work.
- c) The Head of the Department may develop Standard Operating Procedures (SOPs) required for the smooth and stringent compliance of AML/CFT measures without making any compromise to this procedure.
- d) The procedure is an internal document of the Bank and cannot be disclosed to any other person and/or entities, except the concerned competent authorities.
- e) The Bank may develop user manual or guidelines on AML/CFT.

1.1. Scope and availability

The procedure is applicable to all banking operations of Rastriya Banijya Bank including head office, regional offices, all branches and representative offices. This procedure shall be enforced in alignment with the AML/CFT Policy, 2074 by all staff/s of the bank in their respective roles.



Chapter 2

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

2.1. Introduction to KYC/CDD

Know Your Customer or 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 occasional transaction/s. It helps the Bank to identify and verify the customer/s; assess risk and manage it; develop risk-based, effective, efficient and economic control system; and identify further business potential. Know Your Customer (KYC) and CDD can also be taken as a unit in certain business context. The Bank's KYC and AML/CFT standards are based on the following 4 pillars:

- a) Customer Acceptance Policy;
- b) Customer identification Procedures;
- c) Monitoring of Transactions and
- d) Risk Management

2.1.1 Customer Acceptance Policy

Bank's customer Acceptance Policy (CAP) lays down the criteria for acceptance of customer/s. The guidelines in respect of the customer relationship in the Bank broadly are:

- No account shall be opened in the name altering from the primary identity document, anonymous or fictitious (benami) name(s), blank names or numeric/alphanumeric characters.
- Accounts shall be opened only in the name of natural and legal person/organization, the name being the same as in the primary identity document of the person/entity. Accounts may however be opened with different account titles identifying the nature/use/purpose/type/ of account at the written request of the legal person/organization with appropriate control parameters.
- Minimum required information and documents i.e. proper identification and information pertaining to the prospective client shall be obtained prior to opening account or performing business relation of any kind, as per the AML Act, AML Rule, FIU Directives, NRB regulations/Directives and as per the product paper/policy/guidelines set forth by the Bank.
- Necessary checks/ examinations/ verifications shall be made before opening a new account so as to ensure that the identity of the customer does not match with any person withcriminal background or with banned entries such as terrorist individual/s or terrorist organization/s etc.
- Not to open an account: Where the staff/s designated to open new accounts, find sufficient ground/s that the identity of the prospective customer/s could not be verified and/or the prospective customer/s is not disclosing the required identity, the reason for opening account, transaction frequency and volume, etc and any other such information/s deemed necessary for account opening. The refusal shall be documented properly, and shall be communicated to the HO AML compliance Officer through Branch AML Compliance Officer.



n

- Further, the Bank shall freeze an existing account under the situation when the designated staff/s is unable to apply appropriate customer due diligence measure/s i.e. unable to verify the identity and/or obtain document/s required as per the risk categorization, due to non-cooperation of the customer or non-reliability of the data /information furnished to the Bank. Decision for closure of such accounts shall be approved by Senior Management level official under recommendation of AML Compliance Officer at HO and also after giving due notice to the customer explaining the reason for such decision, Closure of such accounts shall be informed to the FIU in written.
- The Bank shall not establish any business relationship/s with the shell companies and the institution/s that deal with shell companies. Any identified business relationship/s with the financial and other institution/s that allow the transaction of shell bank, shall be discontinued. The bank shall not be associated with the entities located in the non-cooperative jurisdictions as identified by the FATF or those sanctioned by the agencies that the Bank refers to like, UN, OFAC, HMT, EU etc.
- Implementation of CAP should not be too restrictive resulting into denial of banking services to the general public, especially those who are financially or socially disadvantaged.
- The decision to open an account for Politically Exposed Persons (PEPs) and Person in Influential Position (PIP) shall be approved by the senior Management Level official/s. Information of such account shall be provided to the AML Compliance Officer at HO.

2.1.2 Customer Identification/Verification Procedures

Customer identification/verification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information to the Bank's satisfaction and also to satisfy the independent authorities that the due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. The customer identification procedures shall be carried out at the following stages;

- While establishing a banking relationship;
- While opening the account;
- While transferring fund through wire transfers
- Whenever the Bank feels that it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account;
- When the bank sells third party products as an agent;
- When high risk customer/s and politically exposed person/s conduct each transaction/s.
- When the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data;
- Customer identification shall also be carried out in respect of the non-account holders approaching the bank for high value one-off transaction/s as well as any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Bank.

D1 to

NDX

~

n

uf

While identifying the natural person or legal person, the bank shall obtain the documents, data and information as mentioned below. All the documents and information pertaining to the identification of the natural and legal person shall be retained in a legible manner and in the managed way.

Natural Person/s

1. Legal name;
2. Permanent and current mailing address;
3. Mailing address of current working organization;
4. Date of birth and gender;
5. Full name of Father and Mother;
6. Nationality;
7. In case of Nepalese citizen, Citizenship copy or Election voting identification card or driving license or Passport number with issued date, issued place and expiry date;
8. In case of those Nepalese citizens who have not obtained the citizenship certificates, recommendation letter issued by the local government.
9. In case of foreign nationals, passport number, issued date issued place and validity;
10. In case of Indian citizens who do not have passport, legal certificate verifying Indian citizenship with certificate number, issued date, issuing authority and place;
11. In case of the refugee, identity card issued by government and international authorities with identity number, issued and expiry date and issued place.

Legal Person/s

1. Name of the legal person/s;
2. Detail information of registered address or business address with phone number, email address, website or other mailing address, if any;
3. Legal entity and nature of business;
4. Registration certificate, license, certificate to commence business, renewal certificate with issued date, expiry date, issuing authority and issuing country;
5. Registration and approval certificate of business, if any, required as per the nature of the entities;
6. Permanent Account Number (PAN) certificate;
7. Personal details of Board of Directors or Management Committee or such higher level committee if any;
8. Personal details of proprietor or partners or shareholders subscribing 10% or more shares of the company;
9. Personal details of account operator and
10. In case a company holds 10% or more shares of another company, personal details of shareholders subscribing 10% or more shares of the former company.



Legal arrangement:

1. Name of legal arrangement, main objectives and functions:
2. Registration or incorporation certificate, country of its operation and its address, contact number, email, website or any other detail contact address:
3. Approval certificate or License and approval letter for transaction, renewal certificate, date of issue, validity, particulars of issuing authority and issuing country:
4. Name, permanent address or current contact address of trustee, controller, protector or settler:
5. Permanent Account Number or such certificate issued by government entity for taxation purpose:
6. Name and address of beneficiary and
7. Personal details of account operator.

2.1.3KYC Steps

1. Responsible staff is required to collect information on all mandatory fields of KYC form and make every effort possible to collect additional information as far as possible as stated in AML/CFT IT System.
2. The staff shall verify the information with the legal documents the customer brings for KYC form (e.g. citizenship) or in case such documents are not available, verify the information with other documents (e.g. passport, driving license or voting card) or in case that is also not possible, verify the information with other documents required by law and practice to ensure that it does not pose higher risks.
3. The staff shall then screen the customer/s, related person and beneficial owner against sanction lists, PEP list, adverse or negative list to ascertain whether a customer or related person or beneficial owner, or beneficiary falls under such list or not.
4. The staff is required to fill in the Internal Observation Form during the initial and later on phases as stated in the Internal Observation section of KYC form in the AML/CFT IT System.
5. While establishing the business relationship, information about the objective of such relationship as well as intended objective shall be collected along with the documents clarifying such objectives in regard to legal person and arrangements.
6. All related staff/s shall write observation remarks on the KYC form during CDD, transaction/s and at a time when any other information is received by any means.
7. Once the staff collects information and documents as stated above, the staff shall confirm that the regulatory and other essential criteria are fulfilled.
8. The staff shall calculate the risks of the customer as designated by the risk module in the AML/CFT IT System and upon self assessment.
9. In case the staff/s succeeds in collecting the mandatory information and documents, and gets satisfied with their assessment of internal observation and finds no any riskier gaps, then the staff/s shall accept/refer business relationship or transaction.
10. While mandated to accept, the staff shall on-board the customer or transaction, and in case, the intended business relationship belongs to a PEP that should be referred to the compliance



division by forwarding the screening KYC request and may be accepted or denied as per the instruction/s of the scrutinizer from the compliance division as stated in the reply - risk profiling notification in the AML/CFT IT System.

11. Once accepted, the details and documents shall be archived into the AML/CFT IT System and a printed copy shall be maintained alphabetically in separate index files.
12. However, list of PEPs, High risk and Low Risk customer shall be positioned in such a way that they can also be separated and maintained differently as provided in the KYC review form in the AML/CFT IT System.

Additional mandatory norms

- In case of natural person, thumb print of both thumbs of a/c operator and in case the account operator is another person then the thumb print of both thumbs of the person operating the account shall be obtained. But in case of a minor, thumb print of the account operator only will be sufficient.
- If a legal person is a subsidiary, information of all layers of holding person (including share holder/s, holding 10% or more equity) shall be obtained

Additional measures for Know Your Customers Customers (KYCC)

- Staff shall collect the additional information by following the KYCC.
- Information about shareholders having substantial ownership or such level of control.
- Information about the customer's customer who has large saving or investment with the customer such as 5% and more of the entire saving.
- Information about customer's customer who has obtained large credit from the customer such as 5% and more of the entire credit portfolio.
- Information about an individual who has direct or indirect control or influence over the customer.
- Information to be collected for KYCC is almost similar to KYC of customer.
- All other provisions of KYC shall be applicable for KYCC too.

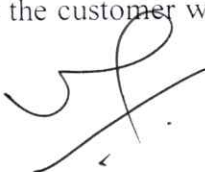
2.2 Types of CDD based on risk

Based on the risk, the Bank adopts following 3 types of CDD.

1. Simplified CDD
2. Normal CDD
3. Enhanced CDD

2.2.1 Simplified Customer Due Diligence

Simplified CDD is the lowest level of due diligence that can be completed on a customer. This is implied to the customer with low risk category. The customer can be categorized as low risk in the risk



assessment of AML/CFT IT system conducted as per the AML Act, AML Rules and NRB Directive are met. However, no simplified CDD can be applied in following circumstances.

- customer identified as non-low risk in bank's risk assessment;
- foreign national;
- customer from AML/CFT non-compliant country or the customer who has main transactions in such country;
- customer listed in stock market of such country which is deficient in comprehensive AML/CFT compliance;
- legal person or arrangement that does not disclose its beneficial owner publicly;
- if customer or beneficial owner is a politically exposed person;
- if the person is high risk or suspicious;
- customer who has annual turnover more than NRs. 100,000;
- transactions conducted through ATM, telephone banking and mobile banking;
- transactions conducted through fax or electronic mediums or any other such instruments and
- Transactions conducted through prepaid card or card in which value added or accounts through which cash payment or deposit collection are done.

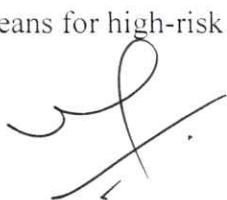
Simplified CDD process can be applied to the customers requesting products or services issued for local programme related with socio-economic interest of Nepali citizens

2.2.2 Normal Customer Due Diligence

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.

2.2.3 Enhanced Customer Due Diligence

Enhanced CDD shall be applied to the customers categorized as high risk. ECDD includes higher degree of CDD that requires collection of additional information and documents as well as surveillance in every stage of transaction. The Bank aims to reach to the reality of the customer and transactions through ECDD process. Certain customer or transactions may need special and extended attention of the bank. Hence, a rigorous and robust additional KYC/CDD process shall be applied for ECDD customer or transactions with additional reasonable measures to verify and validate the customer's identity, understand and test the customers profile, business and account activity as well as risk associated. It should seek to identify relevant adverse information and risk by assessing the potential for money laundering or terrorist financing or other risks to support actionable decisions to militate against financial, regulatory and reputational risk and ensure regulatory compliance. Prior approval shall be taken from management in account opening and high value transaction for the customer through the quickest means for high-risk category.



Steps of ECDD

- a) A separate staff or unit will be designated for ECDD and monitoring of transaction of such customers.
- b) The staff/unit shall ask the high risk customers to fill the ECDD form to identify the purpose of transaction, source of fund, and to monitor the transactions.
- c) Staff/Unit designated for conducting ECDD, shall collect additional information from the customer and other sources such as:
 - KYC and transactions profile
 - Review of personal background, family information
 - Related person information
 - Financial backgrounds and changes
 - Anticipated or actual volume of transactions
 - Source of wealth
 - Business and other activities
 - Ownership and control structures
 - Transactions involving higher risk jurisdictions
 - Search in the websites and information of related Government agencies or units
 - Search in the website and publications of legal persons or arrangements
 - Media and social information
 - Internet search
 - Law enforcement agencies' information
 - Other information
- d) All such information collected shall be added in the Internal Observation Form in the KYC of AML/IT system.
- e) ECDD shall be done at each and every stage of transactions of high risk customers.

Following customers normally undergo ECDD, but not limited to it:

- High risk customer as categorized in AML/CFT IT system;
- Customer with complex, large and unrealistic transactions where financial or legal objective is not clear;
- Natural person, legal person or legal arrangements of such countries who do not comply or partially comply the international standards set for AML/CFT;
- Politically exposed persons and their close associates;
- Customers who conduct transactions through electronic medium;
- High net worth customers;
- Customers who use high risk product/services;

- Customers that might have possibility to have involved in crimes related to money laundering and terrorist financing;
- Customers of such countries which are categorized under high risk in terms of corruption, tax evasion or any other criminal activities;
- Customer/s having unreasonable activities;
- Customer/s going beyond normal legal and economic practices and
- Customer/s with cash business

2.3 Beneficial ownership

Identification of beneficial ownership is one of the prime concentration works of the Bank. Responsible staff shall 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 carried out or the business relationship is established or transaction is conducted.

2.3.1 Steps of Beneficial Ownership Identification (BOI)

Staff should collect beneficial ownership information from natural, legal person or arrangement in following conditions:

- At each and every activity or transaction;
- During the process of establishing business relationship;
- At the time of change in ownership structure and
- During enhanced customer due diligence

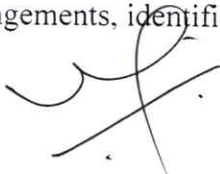
Following are the procedures to be followed while collecting BOI

- Obtain the information from customer;
- Obtain the information available publicly;
- Analyze the information available in social sites;
- Obtain the information maintained as per prevailing law and
- Obtain the statistics from business domain.

While a legal person or arrangement has layers in structure, staff should collect information about all structures up to the holding company or trust, including personal detail of a person holding 10% or more shares or control or interest over the customer or has controls in management and functions.

While exploring BOI, staff should also take care of the following measures:

- Subject to above description, with respect to companies, limited partnerships, or similar arrangements, identification should be made of each natural person that:



- owns directly or indirectly 10% or more of the vote or value of an equity interest;
- exercises management of the company, limited partnership or similar arrangement and
- Controls or exercises control of the legal person or arrangement.
- With respect to a trust or similar arrangements, identification should be made of the settler, trustee, and beneficiary of the trust corpus.

In determining indirect ownership of equity interests

- An equity interest held by a company, limited partnership, or similar arrangement and by a trust should be considered as being owned proportionately by its shareholders, partners, or vested beneficiaries; and
- An equity interest held by a family member shall be considered as also being owned, in its entirety; by each family member (family members include brothers and sisters, spouse, grandfather/mother).

2.4 PEPs

The Bank shall develop timely update and maintain the list of PEP as per the prevailing Nepali laws. The Bank shall also adopt an IT system for identifying, monitoring and managing risks associated with this. Following are the procedures to be followed while collecting PEPs information:

- Obtain the information from customer;
- Obtain the information available publicly;
- Analyze the information available in social sites;
- Obtain the information maintained as per prevailing law and
- Obtain the statistics from business domain.

2.4.1 Steps of PEP Identification

- PEP list are available on PEP master search form in the AML/CFT IT System;
- Staff might place suggestion for the addition and deletion or management of PEP list as per the information received from the customer and other source of information using PEP notification form;
- Designated staffs are required to take prior approval of designated official via confirmation and notification before establishing business relationship or carrying out transactions of PEPs and PEP associates as provided in screening form and screening workflow of the AML/CFT IT System;
- Enhanced CDD is to be done for PEP customers to identify source of wealth, source of fund;
- For PEP customers, approval of DGM overseeing compliance activities shall be required.
- PEPs and PEP associates shall be categorized as high risk customer.

A handwritten signature and initials are present at the bottom of the page. The signature is a large, stylized 'S' shape, and the initials are 'R' and 'S'.

2.5 Screening against Sanctions, Negatives and Adverse lists

The Bank shall deploy sanction screening programs to safeguard itself from establishing, maintaining relationship or carrying out transaction of a person, group or organization that is enlisted in the sanction, negative or adverse list or of those who are directly or indirectly linked with the enlisted person. It shall instigate a control measures for safeguarding the Bank against being used as a conduit for ML, TF, PF and other crimes. The Bank shall have following lists maintained in its MIS IT system to achieve the said objectives.

- UN list
- EU list
- OFAC list
- HMT list
- Acuity sanction list
- Nepal sanctions list
- Adverse Media
- PEP match
- Hot list match
- Investigation match
- Domestic risk match
- Previous screening match
- Existing KYC match
- Other countries' sanctions list as far as possible
- Nepal credit information list
- Nepal convicted list
- Nepal under-investigation list
- The Bank's internal negative list

The Bank shall update the lists as and when appear. No excuse or liberal attitude should be granted/presented to any related staff of the Bank, if sanction screening is ignored, less cared or overlooked. The Bank shall not keep relationship with those financial institution/s that do not follow the sanction screening as per the prevailing laws of the country.

2.5.1 Steps in screening against the list

- It is mandatory to check the customer against the lists using screening form in the AML/CFT IT System before accepting every business relationship or carrying out occasional transactions including receiving or sending money or value from Nepal to other countries and vice versa.
- While remitting or receiving remitted value, the staff/s shall cross check the name/s of sender, receiver, BO, and beneficiary against the lists.
- Procedures for checking the list should be as follows
 - Provide customer information into the screening form.



0

- Find match of the customer using search function.
- Confirmation of the check list is made on the result displayed in the screening form by selecting appropriate match/s.
- Any staff or official may recommend a person to put into check list or remove from the list by filling in the PEP, adverse media, negative list forms available for compliance user in the AML/CFT IT System and submit it to the Compliance, with due reasons.
- While screening against the lists, designated staff should look for any other relevant names including the half names or word.
- In case, such name is available, it should be referred to compliance via notification, followed by stopping all other further actions.
- Referred official should check the name, try to confirm whether it is a false-positive, and if the name is an exact match with the sanction list, all the actions, amounts and transactions are to be frozen immediately and a form report form should be filled to submit to FIU, Regulator, and the Compliance Department/Unit head instantly.
- In case any staff finds a customer or a transaction related to a person under negative list, it shall be referred for ECDD.
- Designated staff is required to take prior approval of designated senior official by forwarding it as notification before establishing business relationship or carrying out transactions of person listed as above.

2.6 KYC Update and review

Review and update of customer's information is essential and critical to better apply KYC system. All other efforts may fail if KYC system is not updated. Hence the Bank has a system of periodical updating of customer identification data (including photograph/s) after the account is opened or transaction is completed.

2.6.1 Steps for KYC Review & Update

- Designated staff shall keep the date of review of KYC while on-boarding a customer as per the risk and other relevant factors.
- Date for review may pop up in the system or shall be reviewed for updating dates.
- Review shall be completed within a week or before any transaction occurs on to that account.
- While updating, the staff/s shall collect only the information that has not been collected before or changed or new information.
- Staff shall collect additional information about a customer, when it is found that problems exist in sufficiency and veracity of information or document provided before.
- Staff shall collect additional information about a customer, when suspicion or unusual activity that is not compatible with ones given profile is noticed.
- Staff shall collect additional information about a customer, when it is found that the staff finds or feels problems in sufficiency and veracity of information or document provided before.

- Information collected under this process shall be added in the KYC profile and Internal observation form of our AML CFT IT system.
- Update and review of customer shall be done immediately in following cases:
 - If transactions of the customer do not match with the details provided in KYC form
 - If KYC is not complete:
 - If the Bank suspects the adequacy and authenticity details mentioned in KYC form.
- Update and review of a customer shall be based on the risk as follows, at a minimum, unless circumstances need something else or there is urgent need of changing the category of risk:
 - High risk one year
 - Medium risk three year
 - Low risk five year
- The Bank shall prepare a separate list of those customers who do not come in contact despite of continuous effort of the Bank.



Chapter 3

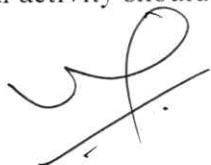
Risk Management

The Bank incorporates Risk- Based Approach (RBA) for the implementation of AML/ CFT measures. It ensures effective CDD program is in place by establishing appropriate procedures and their effective implementation based on risk. It shall also cover proper management, oversight, systems, controls, segregation of duty, training and other related matters.

3.1 Risk-Based Approach Procedure

The procedure on RBA will be as follows:

- All activities of the Bank shall be conducted on risk-based approach.
- Systematic and scientific methods shall be applied for the assessment of risks.
- Risk shall be derived from the calculation of factors such as customer, occupation, industry, product, service, transaction, geography, delivery channel, etc. It will also consider international and national status of the country, legal, enforcement, economic, political, and social surroundings and values for risk assessment.
- Profession, nature of business, nature and objective of relationship, account activities, related parties, sufficiency of documents and possibility of verification, BO information, etc. will also be basis for risk assessment.
- Risk module will produce a grade of risk of a customer which a staff of the Bank can review upon personal observation and may request to supervisor for change in the grade with due reasons.
- High risk/s will be given topmost priority in allocating and distributing resources human, financial or technical for due diligence, monitoring, and reporting.
- Every staff relating to a customer or transaction will pay special attention to every high risk customer in every business relationship and transaction.
- Risk category will be reviewed as follows:
 - High and above : At the time of relationship establishment, at transaction, or every six month
 - Medium and above: Every year
 - Low and above: Every 2 year
- Control and oversight measures commensurate to risk will be central focus of the Bank so that inherent risk is well covered with manageable residual risk.
- Business and AML/CFT will go together in risk management.
- However any change in the portfolio or activities beyond the KYC profile or suspicious or unusual activity should trigger review of risk within 3 days



3.2 Risk Classification of Customers

For proper risk assessment of business relationship with customers and evolving suitable monitoring mechanism, all new customers are to be categorized as High risk, Medium risk and Low risk. It is to be specifically noted that risk categorization is meant for proper monitoring of accounts and does not reflect in any way on the account holders. Risk Categorizations done by the Branch should not be disclosed to the customers. While the extent of knowledge /information available on customers to prove their identity sufficiently will determine the risk perception and concomitantly risk categorization.

We give below an illustrative list of Accounts/ customers / groups who may be assigned different risk categories:

1. High risk
2. Medium risk
3. Low risk

3.2.1 High Risk

- Customer identified as high risk with higher rank of risk scoring by RBA module in screening result and KYC risk profiling in the AML/CFT IT System and national, regulatory and internal risk assessment.
- All account of customers domiciled in high risk countries as categorized by FATF and updated by FIU/Home Ministry from time to time.
- All other accounts classified by FIU-NRB as high risk accounts.
- Customer or transactions related with a jurisdiction fundamentally deficient for the control of following types of crimes in general, but not limited to.:
 - Terrorism and Financing of terrorist activities,
 - Money Laundering
 - Proliferation Financing, Arms and Ammunition
 - Corruption
 - Tax / Revenue evasion
 - Narcotic Drugs and psychotropic substances
 - Human trafficking
 - Organized crime
 - Counterfeiting
- Customer or transactions related with a jurisdiction largely deficient for the control of above listed types of crimes in general or are under a kind of international monitoring
- Non face-to-face Customers or Business Transactions, particularly,
 - Cross border correspondent banking
 - Wire transfers
 - Business relation through Internet, Telephone, Fax, Postal service etc.
 - Internet Banking, ATM Transaction, Mobile Banking
 - Transaction through instruction / request by Fax/wire
 - Transaction through Wire or prepaid card, etc.
- Politically exposed persons (PEPs) both domestic and foreign PEPs their family member and person associated with them.

- Antique dealers (individuals and entities), Money service bureaus, Dealers in arms, Casinos, Bullion dealers including sub dealers & jewelers.
- Business of precious herbs and medicines.
- Export/import trade, Travel agencies, Cooperatives, and company service providers, real Estate agents, Dealers in vehicles.
- All accounts of Trusts, NGOs, Charities, Charities and Organizations receiving domestic or foreign donations and accounts operated by Power of Attorney holders may be classified as High Risk.
- STR reported customer
- Customer under investigation or prosecution or convicted
- Customer with suspected Beneficial Owner.

3.2.2 Medium Risk

- Customer identified as with higher rank of medium risk scoring by RBA module in screening result and KYC risk profiling in the AML/CFT IT System and country with low good governance.
- Transactions with foreigners and NRNs
- Suspected customer
- Customer who conducts complex, unusual large transactions and unusual patterns of transactions or with no apparent economic or visible lawful purpose.
- Public servant beyond PEPs and above section officer or equal to that, family member and person associated with them,
- Chief of municipalities, district level and above beyond PEPs
- Members of political parties of district level and above beyond PEPs
- Customer consuming risky products and services.
- Low range non-face to face activities
- Unregulated Business or business with no need to mandatory financial disclosures
- INGOs and its affiliates in Nepal
- Person with a position in a political party
- NGOs
- Dormant A/Cs with KYC requirements for activation and fund freezing order
- Transactions related to those entities that are highly regulated/inspected and supervised.
- Those customers who are not categorized as high and low risk are to be classified as medium risk customers.

3.2.3 Low Risk

These are the type of customers whose identity and source of income clearly disclosed and the transactions in the accounts by and large do not raise any suspicion. Normally, following customers may be categorized as low risk:

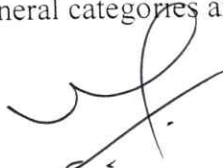
- Salaried employees/pensioners whose salary structure is well defined.
- People belonging to lower economic strata of the society whose accounts show small balances and low turnover.
- Current account and saving account having annual turnover less than NPR 1 Lakh.



- Government departments and Government owned companies, Regulators, Financial Institutions, Statutory Bodies, etc.
- All deposit and borrower accounts pertaining to the Government of Nepal, Governmental bodies/Corporations/Companies/Organizations, Joint ventures with Government, Regulators, Financial Institutions, and Statutory Bodies may be classified as low risk account.
- All borrower accounts other than those classified as high risk and medium risk.

3.3 Risk Based Approach Steps

- After on-boarding a customer, indication of risk should be obtained from the customer information using RBA module.
- Responsible staff will consider the result and observation and if the module given result does not seem appropriate, recommends so with reasons to the designated officials.
- Once all these activities are completed, the customer is assigned a risk level and the system keeps the customer under that category.
- IT system will reflect the designated category of risk in the customers profile and statement.
- The staff should list a customer as a high risk if so referred by the Risk Module or observation provides that ground or risk assessment (national, regulatory, institutional or other) provides that ground.
- If the staff finds a customer or a transaction related to a person under High Risk that should be referred for ECDD.
- The staff should place any suggestion for the addition and deletion or management of high risk list as per the information received from the customer and expert judgment from the relation of the customer and transaction lodging such suggestion via risk overriding form in the AML/CFT IT System.
- General categories are provided in category management form in the AML/CFT IT System.



Chapter 4

Monitoring

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

Automated system will be the primary tool of monitoring. Every transaction will be monitored on a regular basis for revaluation of customer for risk grading and for any suspicious transaction. Designated staffs at the Bank are required to review the product of monitoring tool and add value to information. Human monitoring will be another regular tool for the system. Generally, monitoring will be made against:

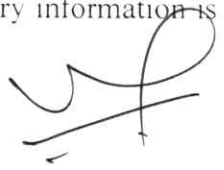
- a) Transactions beyond KYC declaration
- b) Unusual activities/transactions/behavior
- c) Transaction without or unclear economical/legal objectives
- d) Cash transactions
- e) Other suspicious grounds

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

4.1 Steps of Monitoring

- (a) Staff responsible for dealing with a customer or transaction should review the activity of a customer and transaction in the following situations:
 - i. Significant mismatch with KYC profile, except due information is provided or legal or justifiable reason is given;
 - ii. Activities that are not normal or seem unusual from the perspective of nature of relationship, objective of relationship, transactions significantly differing from such objective and nature;
 - iii. Overhearing of suspected or illegal or criminal activity from the customer and
 - iv. From other sources with certain grounds of illegality or suspicion
- (b) Monitoring Mechanisms based on
 - Customers,
 - Transactions,
 - Products,
 - Services,
 - Delivery channel,
 - Geography
- (c) Low risk customer may be monitored within a year unless contrary information is received.
- (d) Medium risk customer may be monitored within every six month unless contrary information is received.

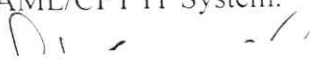
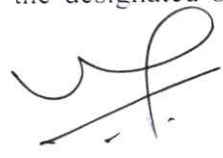
DI to ...



- (e) High risk customer shall be monitored in every transaction or activity.
- (f) Special attention should be given to any large, complex and unusual transactions or activities any time.
- (g) The staff shall consider and try to guess an answer for the following WHs items for monitoring:
- Who
 - What
 - Where
 - When
 - How
 - Why
- (h) The staff shall make analysis of both machine generated and person- ally suspected activities and should prepare a customer-wise report of monitoring by setting parameters, rules, scheduling the rules and scenarios, generating TTR and STR flags, building cases then and submit it to FIU, Regulator, and compliance division/unit chief using the report generator form in the AML/CFT IT System.
- (i) Special attention shall be given on the following accounts or relationships
- Trust/Nominee or Fiduciary Accounts
 - Client accounts opened by professional intermediaries
 - Walk-in Customers
 - Accounts of non-face-to-face customers
 - Accounts of Politically Exposed Persons (PEPs)
 - Cross border transaction or relations
 - Wire transfer including domestic
 - Correspondent banking

4.2 Steps of detecting suspicious transactions

The bank will monitor suspicious transactions in timely manner and report to the respective regulatory agency within three days of occurrence.

- a) Staffs are required to go through the STR Alerts below to detect STR at a minimum.
- b) Every staff should use the IT based monitoring system to collect machine based unusual activities and analyze them in every week or any time or before transaction or relationship if suspected.
- c) Every staff responsible for any function is under obligation to be careful in observing, detecting, monitoring and analyzing unusual activities of a customer or transactions either detected by self or alerted from system or instructed or guided by other information.
- d) Staffs who detect unusual activity will make a written note of it with due reasons and supporting documents if any as provided in SAR Report Form and submit it to the designated senior as provided in the AML/CFT IT System.
- 
- 

- e) Compliance department/unit may consult with other departments, official or expert and may ask for written views on suspicious activity to reach to decisions if so needed as in the format SAR Review Form in the AML/CFT IT System.

4.3 STR Triggers

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 (structuring).
- Transactions conducted by using several different individual names for the interest of a particular person (smurfing).
- The purchase of several insurance products in cash in a short period of time or at the same time with premium payment entirely in a large amount and followed by policy surrender prior to due date.
- 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 (pass-by).
- Receipts/payments of funds made by using more than one (1) account, either in the same name or a different one.
- Fund transfers using the account of reporting entities' employee in an unusual amount.
- If multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate.

4. Behaviors of the Customer

- Unreasonable behaviors of the relevant customer when conducting a transaction (nervous, rushed, unconfident, etc.).

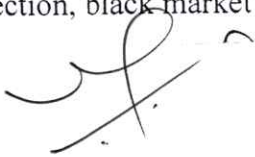


- Unusual curiosity about internal system, control and reporting.
- Customer/prospective customer gives false information with respect to his/her identity, sources of income or businesses.
- Customer/prospective customer use identification documents, that is unreliable or alleged as fake such as different signature or photo.
- Customer/prospective customer is unwilling or refusing to provide information/documents requested by the officials of the relevant reporting entity without any clear reasons.
- Customer or his/her legal representative tries to persuade the officials of the relevant reporting entity in one way or another not to report his/her transaction as a Suspicious Financial Transaction.
- 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 of the relevant reporting entity request information with respect to his/her transaction.
- If anyone, for no apparent reason, often comes for transaction at pick hour or only in crowd.
- If anyone tries to maintain close relation unnecessarily or unnaturally with the employees.
- If anyone automatically unnecessarily clarifies or tries to clarify legality of amount or transaction.
- If customer-conducting transaction looks confused, nervous, hurried, or wants to remain reserved at the time of transaction.

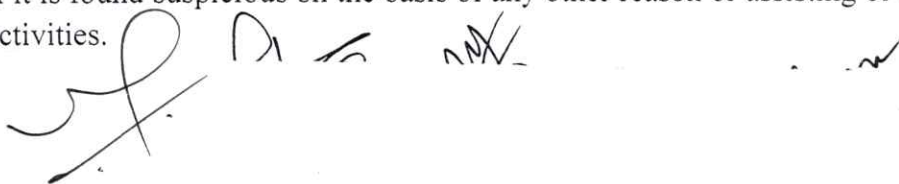
5. Miscellaneous grounds for suspicion

- If it is evident that any one is earning wealth (including cash) by evading tax, custom duty, land revenue, electricity bill, and water bill, phone bill and any other revenue or government fees.
- If anyone lives unusual lifestyle compared to his/her economic strength, profession/business.
- If unreasonable economic growth or economic strength is evident.
- If no information about the source of income is disclosed or stated or information about the source of income is not satisfactory.
- If any act or transaction is not found reasonable or is found to have been conducted with irrelevant party or where the transaction has no justifiable purpose.
- If it is evident that repeated transactions below threshold amount fixed by the FIU for reporting purpose take place.
- If any transaction is related to any person being investigated against or wanted by Police, CIAA, Tax, Revenue Investigation or any other crime investigating agencies in relation to any crime.
- If reporting institution suspects any transaction relating to the customer against whom the regulatory authorities including Nepal Rastra Bank, Insurance Board, Securities Board, Stock Exchange, Company Registrar, Registrar of Cooperative, Bar Council, Institute of Chartered Accountant of Nepal, etc., have initiated proceedings.

- If there is suspicion on the transaction due to the fact that the customer is blacklisted by Credit Information Bureau or the reporting institution itself has placed the concerned customer in a high-risk customer category.
- The transaction of the customer, where it is known or is evident that any investigation or proceeding has been or is being taken by competent law enforcement or regulatory institution of foreign state.
- If it is evident that the asset is earned from any offence against or abuse of children, women or destitute or any other individual.
- If it is evident that the asset is earned from extortion, coercive donation collection or from any forcible means to compel one to pay amount or asset.
- If it is evident that the asset is earned from offence of smuggling, illegal profession, trade and business, theft, bribery, robbery, piracy, illegal production, misuse or illegal transportation of goods.
- If it is evident that the asset is earned from the offence relating to arms and ammunition under the prevailing law.
- If it is evident that the asset is earned from the offences under the prevailing foreign exchange regulation laws.
- If it is evident that the asset is earned from the offence of murder, theft, fraud, forgery of documents, counterfeiting, trafficking of human beings, abduction and hostage taking under the relevant prevailing laws.
- If it is evident that the asset is earned from the offences under the prevailing narcotics control laws.
- If it is evident that the asset is earned from the offences under the prevailing national park and wildlife conservation laws.
- If it is evident that the asset is earned from the offences under the prevailing human trafficking and transportation control laws.
- If it is evident that the asset is earned from the offences under the prevailing cooperatives laws.
- If it is evident that the asset is earned from the offences under the prevailing forestry laws.
- If it is evident that the asset is earned from the offences under the prevailing corruption control laws.
- If it is evident that the asset is earned from the offences under the prevailing bank and financial institution laws.
- If it is evident that the asset is earned from the offences under the prevailing banking offense and punishment laws.
- If it is evident that the asset is earned from the offences under the prevailing ancient monuments conservation laws.
- If it is evident that the asset is earned from the offences under the prevailing consumer protection, black-market control and competition laws.



- If it is evident that the asset is earned from the offences under the prevailing company, commerce, supply, transport business laws.
- If it is evident that the asset is earned from the offences under the prevailing education, health, drugs, and environment laws.
- If it is evident that the asset is earned from the offences under the prevailing foreign employment laws.
- If it is evident that the asset is earned from the offences under the prevailing lottery, gambling and charity laws.
- If it is evident that the asset is earned from the offences under the prevailing insider trading, fake transaction, securities and insurance laws.
- If it is evident that the asset is earned from the offences under the prevailing negotiable instrument laws.
- If it is evident that the asset is earned from the offences under the prevailing election laws.
- If it is evident that the asset is earned from the offences under the prevailing intellectual and industrial property laws.
- If it is evident that the asset is earned from the offences under the prevailing communication, transmission, and advertisement laws.
- If it is evident that the asset is earned from the offences under the prevailing land, house and property laws.
- If it is found that the asset is earned by the offences under the prevailing immigration, citizenship and passport laws.
- If it is found that the asset is earned by the offences under the prevailing non-governmental organization laws.
- Transaction of individual or organization declared to be involved in terrorist or criminal activities by the Government of Nepal or individual or organization listed as terrorist or criminal by United Nation through various resolution or transaction of those directly or indirectly assisting terrorism, terrorist activities, terrorist organization, organized crime, drug offences and any other offences.
- If transaction seems to be reported based on the news or commentary published in national or international news media about any individual or organization.
- If it is evident that the transaction is related to any person who is involved in suspicious transaction, likely to promote money laundering, terrorist or any other criminal activities or the transaction that appears to be unnatural or suspicious in any manner.
- If same address or telephone number/mobile number is provided for different unrelated customers.
- If such transaction comes under suspicion on the basis of the ground provided by regulator or concerned authority
- If it is found suspicious on the basis of any other reason or assisting or advising above mentioned activities.



Handwritten signatures and initials are present at the bottom of the page, including a large stylized signature on the left and several smaller initials or marks to its right.

- If any customer shows unnecessary interest in suspicious transaction or makes unnecessary and unnatural queries about the internal management of such transaction.
- If there is cross transaction between customers who are not related with each other or any individual transmits or receives amount from unrelated person or business institution's account.
- If unnaturally huge amount is transferred to the name or account of any foreign citizen, tourist, student, visitor, worker or a person recently migrated to Nepal from the country or region where terrorist organizations operate
- If there is suspicion that any transaction is aiding criminal activities or receiving amount from such activities.
- If cash is handled unnatural binding or packaging during transaction.
- If with no apparent reason there are multiple transactions with the people living in the country where AML/CFT regime is poor.
- If unrelated third party is unnaturally, unnecessarily involved or is more active in transaction.
- If anyone tries to complete transaction by paying more without any reason.
- If person sending money cannot provide even general information about the recipient of money.
- If there is unnatural inflow or outflow in the name of the firm, company, organization or person involved in such organizations which are not regulated or where no system of economic inspection is developed.
- If there is repeated transfer of money to and from the name of foreign individual or the individual living outside Nepal.
- If anyone transfers or receives amount differently from the way of his professional objective or transfers or receives from different place.
- If there are multiple claims for the amount received from one person.
- If anyone repeatedly receives multiple amount from different places.
- If anyone uses different channels to transfer the amount ignoring the usual way.
- If anyone denies providing identity of the transferor though there are sufficient grounds for him to know such identity.
- If anyone attempts to transfer or receive amount in a suspicious manner.
- If a small capital holder tries to transfer or receive unreasonably huge amount.
- Any other transaction the reporting institution finds the grounds for suspicious transaction reporting as per the prevailing law.

Chapter 5

Reporting

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

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

Regulatory reports

- The bank shall produce all regulatory reports including off-site reports along with historical trends and patterns electronically as prescribed by the regulator and required by the Bank.

FIU reports

- Threshold transactions: as determined by Nepal Rastra Bank, updated time to time.
- Suspicious transactions/activities: STR is the heart of the AML/CFT system. Special care and mechanisms are essential for effectiveness of these functions. Hence the Bank has adopted an IT system as well and human controlled case management system in detecting, analyzing and reporting suspicious activities.
- Sensitive information: The bank shall adopt a procedure to detect sensitive information related to offenses and investigation such as requested by regulator, FIU, law enforcement agencies or information under monitoring order and will build proper mechanism to report such information timely and sufficiently.
- Additional information: The bank shall develop a mechanism to review the position of the reported activity upon certain event or time gap so as to collect additional information and submit it to FIU.

5.1 Threshold Transactions & Reporting

- a) The Bank shall submit the particulars of transactions following a threshold or in excess of such threshold within 15 days from the date of transaction to the Financial Information Unit (FIU) as per Annex -2 format. The AML/CFT IT System of the Bank may generate such report everyday or in a batch.
 - Deposit or withdrawal of **NRs. 1,000,000 (NRs One Million) or more** into the same account in one transaction or in a series of transactions in one day.
 - Inward or outward remittance of **NRs. 1,000,000 / - (NRs One Million) or more** into or out of the same account in one transaction or series of transaction in one day or inward or

outward remittance of NRs. 1,000,000/- (NRs One Million) or more by a customer (in case of non-account-holder customer) in one transaction or in a series of transactions in one day.

- Exchange of foreign currency equivalent to NRs. 500,000/- or more by a customer in one transaction or in a series of transactions in one day.

Clarification: With respect to foreign currency transactions, the amount stated above shall mean the amount derived by multiplying the same at the prevailing exchange rate on that date.

- b) Threshold Transaction Report (TTR) shall require the source of fund involved with a transaction to be mentioned therein. Self declaration of the customer will do with that purpose.
- c) Source of fund shall be mentioned in every cash deposit from NRs. 1,000,000 or above in a or several transactions in a day.
- d) Staff shall write the same source of fund in the transaction of cash deposit.
- e) Customer may be allowed to declare (self declaration) that the fund is not earned from any illegal activities including Terrorism, drugs dealing, human trafficking and/or any organized crime (The customer has to present supporting documents if required).
- f) The bank shall filter cash withdrawal activities of NRs. 1,000,000 or more and maintain a separate record of such activities.

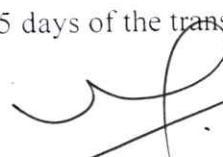
5.1.1 Exempted transaction to TTR reporting

The Bank shall not submit the threshold transaction detail of the followings to the FIU.

- CHEQUE transaction
- Transaction made by Govt. and Govt. entity
- Transaction between NRB approved financial institution
- Transaction of public limited co. with Govt., Govt. entity and the entity established under special Act.
- Transaction of special established entity
- Reinsurance transaction of insurance co.
- Staff facilities of financial institutions
- Transaction of UN and other International entities
- Transaction of loan, advances & facilities provided to customer by any financial institutions

5.1.2 Steps of TTR

- Collect all transaction with amount NRS. 1,000,000 or more.
- Analyze the transaction along with customer and account details.
- Separate exempted transactions and mark for non-reporting.
- Review the filtered list for submission.
- Submit the report to FIU manually/electronically reachable within 15 days of the transaction



5.2 Suspicious Transaction Reporting

Responsible staff at the Bank must review the STR flags raised by the AML/CFT IT System; build the case, forward for review to designated official. Designated official may override, approve, and reschedule the cases for review. Upon approval of the designated official, the reports of STR can be obtained from the STR reporting form in the AML/CFT IT System and must be reported to FIU within 3 days of arriving at a conclusion that the transaction/s are suspicious.

5.2.1 Steps of STR


- Collect unusual transactional and behavioral activities and/or/ alerts detected from monitoring, observation, and other source of information/intelligence.
- Examine each and every unusual activity with the following elements.
 - Transaction deviating from:
 - The profile;
 - The characteristics; or
 - The usual transaction pattern of the relevant customer.
 - Transaction reasonably suspected to have been conducted with the purpose of evading the reporting that must be conducted by the relevant reporting entity.
 - Financial transaction conducted using fund alleged to be attributable to predicate offences.
 - Transaction that have no economic or legal rationale or bonafide purpose.
- Prepare a case profile as provided in the internal STR Form.
- Submit the internal STR form to the designated official.
- Review and decide on the STR form for submission to FIU.

The Bank shall submit reports of suspicious transactions covering; cash, economically irrational transactions, fund transfers, behavior of customer and miscellaneous grounds of suspicion that are deemed necessary for reporting.

5.3 Tipping Off

The bank or any of its staff shall not disclose to its customer or to any other person that a following report, document, record, notice or information concerning suspected money laundering or terrorist financing or predicate offence has been initiated or is being submitted to FIU and/or any other enforcement authorities and their officers:

- Report of suspicious or threshold transaction.
- Order received from FIU or any other enforcement authorities for conducting ongoing monitoring of any customer and make reporting in given time.
- Any document, record or information provided to the FIU and other investigating authorities.
- Disclosing name and any other detail of bank staff/s providing report, document or information to concerned authorities



Chapter 6

Governance and Compliance: Roles and Responsibilities

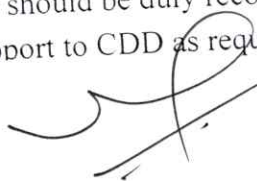
6.1 Roles

- The Bank has integrated AML functions with business functions. Roles and functions of the staffs/departments in terms of AML/CFT are different according to their designation and work. In other words, same business staff will carry out AML/CFT functions related to their respective designation, though certain roles have defined below.
- **Head of Compliance Division/Unit/Department** functions as a focal point to implement these policies and guidelines and to establish and maintain adequate arrangements for training on prevention of money laundering and financing of terrorism. S/he shall also be responsible for ensuring prompt response to queries from internal/external authorities and for assisting Business Units/Branches in meeting their responsibilities.
- At branch level, Assistant Branch Managers are appointed as **Compliance Officer** who shall be performing the roles of AML/CFT Compliance officers.
- Business supervisors in their respective roles shall be the supervisor of AML/CFT functions.

6.2 Role and Responsibilities of Customer Service Desk (CSD)

- To interview the potential customer.
- To verify the introductory reference/customer details/profile.
- KYC/CDD in accepting new customers.
- To exercise due diligence in identifying suspicious transactions.
- To ensure against opening of accounts in the name of terrorist/banned organization.
- Take management level approval for a/c opening of High Risk Customer.
- Update the information of customers, including internal observations as well.
- To comply with the guidelines issued by the Bank from time to time in respect of opening and conduct of account.

6.3 Role and Responsibilities of Branch Manager

- To scrutinize and satisfy himself/herself that the information furnished in the account opening form/customer profile/ are in strict compliance with KYC guidelines before authorizing opening of account.
 - Make efforts to implement AML/CFT measures effectively and efficiently.
 - Forward the report of unusual and suspicious transaction to Compliance Officer including unusual information that is received through various means even including gossips of customers or activities should be duly recorded by all the related staffs.
 - Provide support to CDD as requested.
- 

6.4 Role and Responsibilities of Compliance Officer

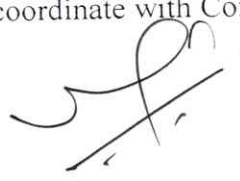
Designated officer at compliance Department and Operation in charge of the branches shall act as Compliance Officer. The major responsibilities of Compliance officers will be as follows:

- To ensure compliance to AML Act, 2008 along with 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 record of transaction exceeding threshold limit and file Transaction Threshold Report to compliance department.
- To file suspicious transaction report to Compliance Department of the transactions which do not match with general financial condition of the customer.
- To keep customers information confidential at all time.

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

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

6.6 Roles and Responsibilities of Regional offices

- To ensure prompt reporting of prima facie suspicious transactions to the Compliance Officer.
 - To verify KYC Compliance at branches during branch visits.
 - To coordinate with Compliance Officer for conducting trainings on KYC/AML/CFT matters.
- 

6.7 Roles and Responsibilities of Chief Executive Officer (CEO)

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

6.8 Roles and Responsibilities of AML/CFT Board Committee

AML/CFT Board 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 are as follows:

- Review and support AML/CFT Policy for the purpose of approval from Board of Directors.
- Review of Reports submitted by Compliance Department on periodic basis.
- Monitoring AML/CFT related activities to implement AML/CFT Policy.
- 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.





6.9 Roles and Responsibilities of Management Level AML/CFT Committee

- 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.

6.10 Role and Responsibilities of Audit Department

Internal Audit Department shall be responsible for check and review effectiveness of this Policy. The illustrative but not exhaustive roles and responsibilities of Internal Audit Department related to this Policy are as follows:

- Internal Audit shall provide independent evaluation of compliance with this policy.
- Internal Auditor shall be responsible for conducting checks and reviews to ensure that the control and monitoring and reporting procedures under this policy.
- Internal audit shall specifically check and verify the application of KYC/AML procedures at the offices/branches and comment on the lapses observed.



- The compliance in this regard shall be placed on the Audit committee and the board at quarterly basis.
- Ensure the process and procedures mentioned in this Policy are duly followed.
- Check the breach of internal and external provision and regulations.
- Conduct the audit as per the provision of NRB.

6.10 Roles and Responsibilities of Board of Directors

Approving, enforcing internal AML/CFT policy, procedure and guideline.

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

6.11 Roles and Responsibilities of Legal Department

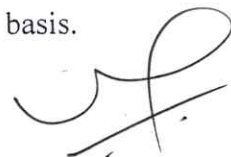
Legal Department is the department responsible for ensuring compliance to all legal and regulatory requirements as well as all applicable laws of the land related to the Policy in the daily business and operations of the Bank. The illustrative but not exhaustive roles and responsibilities of Legal Department related to this Policy shall be as follows:

- Providing legal opinion as and when required;
- Providing recommendation on statutory and internal requirements on the need basis with regards to the AML / CFT.

6.12 Role and Responsibilities of Human Resource Department

Human Resource Department is responsible for managing overall human resources of the Bank. The illustrative but not exhaustive roles and responsibilities of Human Resource Department related to this Policy shall be as follows:

- HR Department shall ensure that screening against sanction list and due diligence have been made before appointing any person in the permanent and contract positions in the bank.
- HR shall also ensure that due diligence of the employees is updated regularly and record is maintained appropriately.
- Assessment of adequate human resources requirement.
- Training to human resources in the area of AML / CFT on need basis.



Chapter 7

Record Keeping

Bank shall keep a record of every transaction, customer and beneficial owner data, and data obtained for the purpose of identification, risk analysis, monitoring and other related information along with the date, time and nature, KYC/CDD documents, correspondence with the customers, sources of fund, as well as all documents related to money laundering activities such as files on suspicious activity reports, documentation of AML account monitoring, etc. These records must be kept for a minimum of 5 years until other policy/act is prescribed for more time.

7.1 Reviews

- a) Each branch and department shall prepare and submit monthly AML/CFT report to the Compliance Department (CD) including the problems and reforms required.
- b) CD shall assess the branch and departmental reports and independently prepare the report of the Bank every three months.
- c) CD shall present such reports to the CEO for discussion at BoD and necessary directions to be prescribed.

A series of handwritten signatures and initials in black ink, including a large stylized signature on the right and several smaller initials or marks to the left.

Chapter 8

Miscellaneous

8.1 Employee Training Program

Training shall be provided to business units that offer products and services that are subject to the legislative requirements. Staff involved in customer facing areas, remittance, SWIFT etc. of the bank shall receive periodic training and reminders on the detection and reporting process for suspicious activities. Communication of changes to AML/CFT legislation or any emerging risks are communicated to the relevant staff.

In addition to the above, Human Resource Department shall make sure that the training on AML/CFT/KYC/CDD will also be provided to all staff of Rastriya Banijya Bank Ltd. using internal or external resources and as and when there are changes in AML/CFT Policy, procedures or there are new developments in the AML/CFT trends worldwide.

8.2 Amendment to the policy

The CEO of the Bank upon the recommendation of AML/CFT Committee may amend the procedure for better compliance and performance.

8.3 Interpretation

The AML/CFT committee may interpret the provision of the procedure if so required. Such interpretation will be submitted to the CEO for the information.

8.4 Repeal and Saving

The Rastriya Banijya Bank Ltd. AML/CFT Procedure 2069 has been repealed. Any activity carried out under AML/CFT Procedure 2069 procedure shall be considered to have been conducted under this procedure.

8.5 Code of Conduct

A responsible staff of the bank, every staff of the bank shall adhere following code of conduct relating to prevention of money laundering and combating financing terrorism:

- No any staff of the bank (including board members) shall, by any means, be involved in money laundering or terrorist financing directly or indirectly, in part or in whole, unlawfully and willingly
- No any staff of the bank (including board members) shall, by any means, support to money laundering or terrorist financing directly or indirectly, in part or in whole, unlawfully and willingly

D. K. N. A. ✓



- No any staff of the bank (including board members) shall inform/share/talk/disclose/warn, by any means, to any unauthorized persons about the bank's policies and procedures relating ML/FT risk management.
- No any staff of the bank shall inform/share/talk/disclose/warn, by any means, to any unauthorized persons about bank's consideration as suspicious or any investigation initiated by bank or other competent authorities regarding any of its customers or other parties.
- Concerned staff shall provide access to offices or furnish information requested by authorized persons of the bank entrusted with responsibility of legal and regulatory compliances.
- Concerned staffs shall extend full cooperation to the legal and regulating bodies during their investigation in relation to ML/FT activities.
- No staff shall provide customer or any third party, at the customers' request, with incomplete or otherwise misleading documents or information in connection with the customer's accounts and transactions

8.6 Departmental Action

At each event of violation of the provisions of this policy, the Bank shall take departmental action to it staff under staff service by rule, 2070.

 DI ~~B~~ NA  0 1 .