Anti-Money Laundering / Counter Financing of Terrorism Policy
(AML / CFT POLICY)

Revised: January 2023

APPROVED BY 416TH BOD MEETING DATED 4TH JAN 2023

Contents

VERSION CONTROL

Version Control No.	Date	Remarks
Version 1	July 2012	
Version 2	August 2015	Revised
Version 3	December 2017	Revised
Version 4	December 2018	Revised
Version 5	February 2020	Revised
Version 6	January 2023	Revised

ABBREVIATIONS

AML	Anti-Money Laundering
ALPA	Asset (Money) Laundering Prevention Act, 2064
APG	Asia/Pacific Group on Money Laundering
BOD	Board of Directors
CDD	Customer Due Diligence
CCO	Chief Compliance Officer
COCO	Chief of Country Operations
CEO	Chief Executive Officer
COO	Chief Operating Officer
CFT	Counter-Financing of Terrorism
ECDD	Enhanced Customer Due Diligence
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
HMT	Her Majesty's Treasury, United Kingdom
HRD	Human Resource Department
KYC	Know Your Customer
KYE	Know Your Employee
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
ML/TF	Money Laundering and/or Terrorist Financing
NRB	Nepal Rastra Bank
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
Rules	Asset (Money) Laundering Prevention Rules 2073
STR	Suspicious Transaction Report
TBML	Trade Based Money Laundering
TF	Terrorist Financing
The Policy	Anti-Money Laundering / Counter Financing of Terrorism Policy of the Bank
TTR	Threshold Transaction Report
UN	United Nations

WMD	Weapons of Mass Destruction

CHAPTER 1: INTRODUCTION

1.1 Background

Global IME Bank Limited, hereinafter referred to as the "Bank", is Nepal Rastra Bank (NRB) licensed "A" Class commercial bank. The Bank is committed towards providing entire commercial banking products and services. The Bank's shares are publicly traded in the Nepal Stock Exchange.

The Bank is well aware of the importance of preventing money laundering and terrorist financing activities and is fully committed towards the implementation of the highest standards of anti-money laundering and counter financing of terrorism (AML/CFT). The Bank is subject to applicable legislation designed to prevent ML/TF. This legislation includes Asset (Money) Laundering Prevention Act 2064, Asset (Money) Laundering Prevention Rules 2073, and NRB directives/circulars and amendments thereof issued from time to time.

Further, the Bank acknowledges the FATF recommendations against criminal activities related to money laundering/terrorist financing and adopts appropriate mechanism to address those recommendations to prevent the Bank being used for ML/TF activities. The Bank is also committed to continually fulfill its anti-money laundering obligations to its foreign correspondent banks, which may also require bank to conduct due diligence on them to ensure that they comply with the FATF recommendation.

Hence, the Bank's policy on anti-money laundering, and counter financing of terrorism (hereinafter referred to as "The Policy"), outlines the minimum general unified standards of internal AML/CFT program which should be strictly adhered to by the Bank in order to mitigate the legal, regulatory, reputational, and subsequent operational and financial risks. In order to mitigate the ML/TF risks, the Bank shall formulate guideline, controls and procedures as deemed necessary to effectively manage such risks based on principles of the Policy.

This Policy establishes standards which every employee and business partner of the Bank should adhere to. BOD and all employees are under an obligation to implement the provisions laid down in this Policy. This is a revised Policy compatible with local and international regulations.

1.2 Definitions of key terms

1.2.1 Money Laundering

Money laundering is the process by which criminals disguise the illegal origin of the funds. In simple words, it is the process of laundering black money for the purpose of converting the same into clean money. Money laundering is done by launderers worldwide to conceal funds from criminal activities. There are three stages of Money Laundering:

a) Placement: It is the first stage in money laundering where the cash proceeds of criminal activity enter into the financial system.
b) Layering: It is the second stage in money laundering where attempts are made to distance the money from its illegal source through layers of financial transactions.
c) Integration: It is the third stage of money laundering. This stage involves the re-introduction of the illegal proceeds into legitimate commerce by providing a legitimate-appearing explanation for the funds.

1.2.2 Financing of Terrorism

Financing of Terrorism means financial support to any form of terrorism or to those who encourage plan or engage in terrorism. Financing of Terrorism involves the solicitation, collection or provisions of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both licit and illicit sources. More precisely, according to the International Convention for the Suppression of the Financing of Terrorism, a person commits the crime of financing of terrorism "if the person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an offense within the scope of the Convention. The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the financing and the nature of the financed activity.

1.2.3 Proliferation Financing

Proliferation Financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials that would contribute to the Weapons of Mass Destruction (WMD) proliferation (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. Bank shall work towards raising awareness and be watchful to providing funds or financial services which are not intended towards proliferation and proliferation financing of WMD.

1.2.4 Anti-Money Laundering (AML)/Counter-Financing of Terrorism (CFT)

AML/CFT is a term used in the industry to describe the legal controls that require the financial institutions and other regulated entities to prevent, detect, and report ML/TF activities. The Bank has implemented standard KYC norms to prevent, detect and report of ML/TF activities to the FIU.

1.2.5 Trade based money laundering

Trade based money laundering is the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illegal origins.

1.2.6 Customers

Customers of the bank shall denote any of the followings:

a) A person or entity that maintains an account with the Bank and/or has business relationship with the Bank.
b) A person on behalf of whom an account is maintained (beneficial owner).
c) Any person or entity connected with the financial transaction that may impose significant reputational or other risks to the Bank.

1.2.7 Shell bank and shell entity

A shell bank means a financial institution that has no physical presence in the country in which it is incorporated and licensed and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Appointment of local agent or presence of its staff(s) does not constitute physical

presence.[1] Shell entity is an entity that has no assets or does not have active business operation.

1.2.8 Beneficial owner

Beneficial owner is natural person(s) who has/have ultimate control over the funds through ownership or other means and/or who are the ultimate source of funds for the account. Individuals who have control over an account/fund or having 10% or more shareholding in case of a legal entity shall be considered as beneficial owner.

1.2.9 Tipping Off

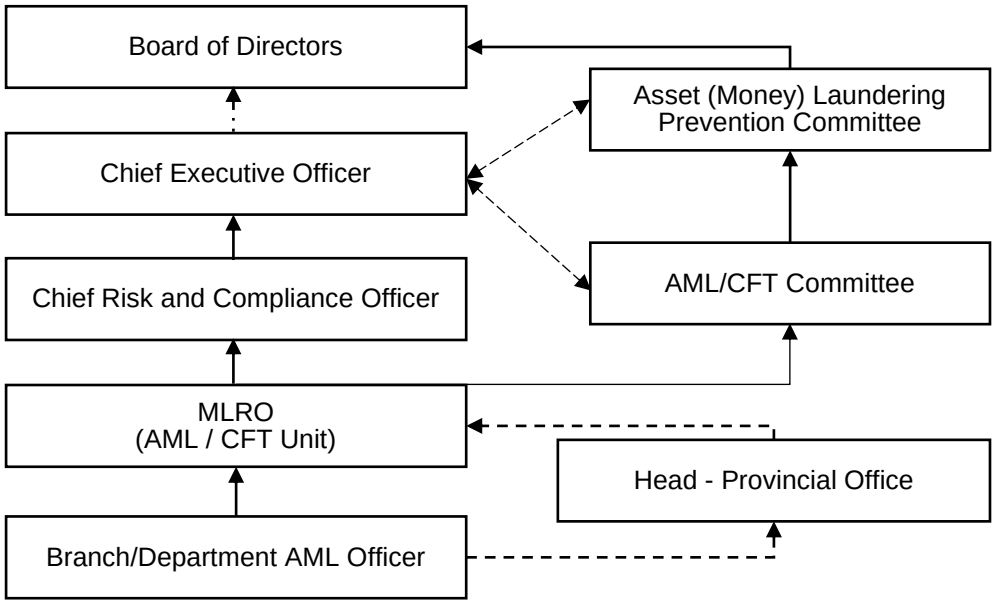
Tipping off refers to disclosing information to the parties who are not related to the investigation of the suspicions or directly alerting a customer that a suspicious transaction report (STR), suspicious activity report (SAR), threshold transaction report (TTR) has been filed or sharing any other information from which it could be reasonably inferred that the bank has submitted or is required to submit an STR[2].

1.3 Objective

The objective of this Policy is to prevent the Bank from being used for ML/TF activities by establishing a sound risk management policy framework of the Bank. The policy framework shall encompass the mechanisms for identifying ML/TF risks faced by the Bank, NRB guidance, requirements of law, including international AML/CFT standards and as guided by FATF recommendations.

1.4 Governance Structure

For effective implementation of The Policy, a governance structure including Board of Directors (BOD), and Senior Management has been designed as under:



1.4.1 Board of Directors

AML/CFT risk management is an important aspect of overall risk management of the Bank and BOD are an integral part of AML/CFT governance structure. The BOD is responsible for policy formation as well as ensuring effective implementation of such policies and procedures by the management of the Bank.

[1] ALPA – Chapter 1, Clause (2)(LA)
[2] ALPA – Chapter 8, Clause (44 KA)

The BOD shall be timely reported with relevant information on ML/TF to make the informed decision on mitigating ML/TF risks.

1.4.2 Senior management

Senior management is responsible to ensure that the procedures, and mechanisms related with prevention of ML/TF activities are formulated as per The Policy and are effectively implemented. Senior management must ensure that such procedures and mechanisms are appropriate in a manner where risk management and controls are effective and authority and responsibility have been clearly communicated to all staffs.

1.4.3 AML/CFT Unit

The Bank shall have a dedicated AML/CFT Unit under Risk Department; A Managerial level staff shall be the Chief of the unit[3] as Manager AML/CFT. The Manager AML/CFT shall be called as Money Laundering Reporting Officer (MLRO) and shall be responsible for evaluating and strengthening the effectiveness of set controls and internal systems of the Bank to help identify, monitor and report ML/TF activities.

1.4.4 Asset (Money) Laundering Prevention Committee

The Bank shall have a Board level Asset (Money) Laundering Prevention Committee which is constituted in line with the NRB Directives.

The Committee highlights on risk governance and identifies the need for a strong and well-defined ML/TF risk management framework and mechanisms. The Committee shall review the AML/CFT Policy and recommend for approval to the BOD. The meeting shall be held at least once in every 3 months or as required.

A board member shall be the coordinator of this committee. In absence of the coordinator, the remaining board member shall conduct the meeting as Coordinator and in the absence of Member Secretary, CCO shall act as Member Secretary. The quorum necessitates a simple majority of the total members of the committee. The Committee comprises of the following members:

Board Member	-	Coordinator
Board Member	-	Member
Chief Risk Officer	-	Member
Chief Compliance Officer	-	Member
MLRO	-	Member Secretary

Terms of Reference (TOR) of the Committee shall be as per Unified Directive issued by NRB regarding Corporate Governance[4].

1.4.5 AML/CFT Committee

The Bank shall have a management level AML/CFT Committee. The purpose of the committee shall be

a. To assess, review, and monitor the status of the Bank's standing on complying with KYC principle,
b. To ensure effective implementation of The Policy through a standard guideline,

[3] ALPA – Chapter 3, Clause (7)(TA)(3)
[4] Unified Directive 2078, directive no. 6/078, Clause (7) (5)

c. To evaluate and strengthen the AML control so as to mitigate the ML/TF risks,

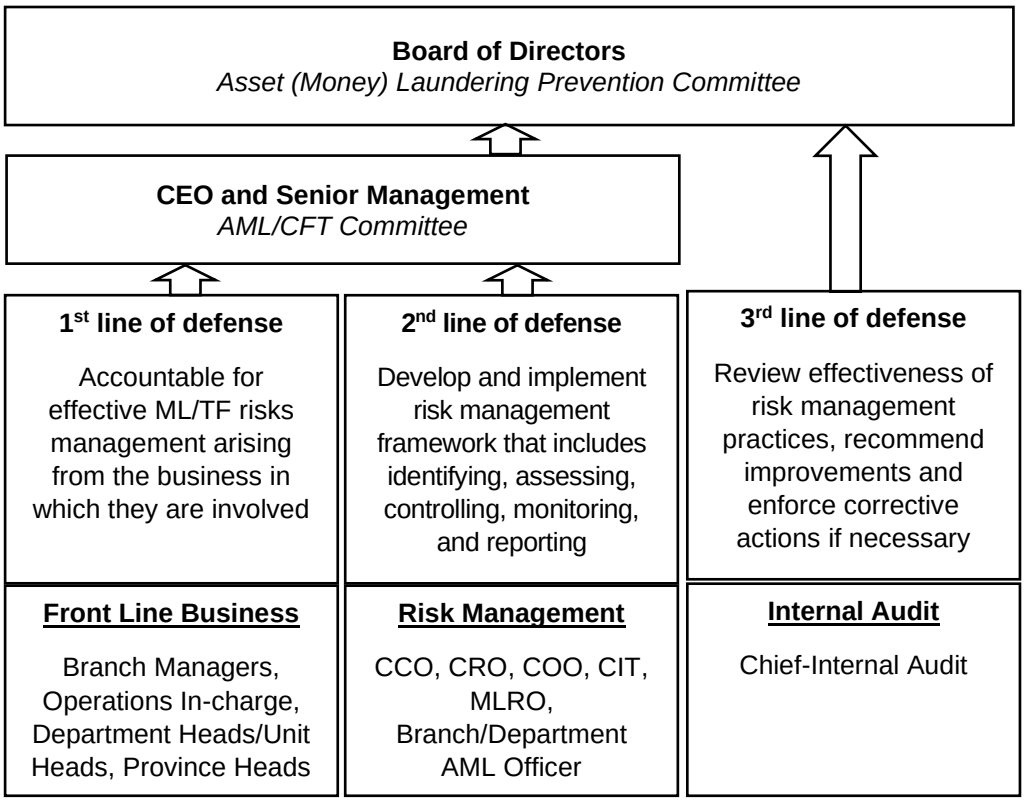
The Committee shall also review the AML/CFT related reports and forward the report to Asset (Money) Laundering Prevention Committee with necessary recommendations, if deemed necessary. The meeting shall be held at least once in every 3 months or as required.

Senior Deputy Chief Executive Officer shall be coordinator of the committee. In absence of the Coordinator, Deputy Chief Executive Officer shall conduct the meeting as Coordinator and in the absence of Deputy Chief Executive Officer, remaining members shall decide as required. In absence of Member Secretary, CCO shall act as Member Secretary. The quorum necessitates a simple majority of the total members of the committee. The Committee comprises of the following members:

Senior Deputy Chief Executive Officer	- Coordinator
Deputy Chief Executive Officer	- Member
Chief Operating Officer	- Member
Chief Business Officer	- Member
Chief Compliance Officer	- Member
Chief Risk Officer	- Member
Chief Information Technology Officer	- Member
Chief of Country Operations	- Member
Chief Marketing Officer	- Member
MLRO	- Member Secretary

1.4.6 Three-line-of-defense

In order to facilitate timely detection of problems that exposes the bank towards higher ML/TF risks thereby limiting the damage to the Bank, an effective internal control system shall be in place. Following the best practices, the Bank shall implement three lines of defense as part of the effective risk management from AML/CFT aspect:



1.4.6.1 First line of defense: Business units / front line staff

The first line of defense shall identify, asses, and manage the ML/TF risks arising from the business/accounts in which they are involved, and are responsible for having controls in place to mitigate the risk and promoting AML/CFT principles.

a. Branch Managers / Branch In-charge shall be responsible for ensuring and executing the task related to their branch in compliance to The Policy.

b. Department Heads in Corporate Office and Province Heads should implement ongoing employee training to adequately train all of the staffs in their departments, offices, and branches as per employee's specific responsibility to ensure effective implementation of this policy. Province Head shall facilitate implementation of this policy and monitor activities performed in all areas in line with this policy in their respective jurisdictions.

1.4.6.2 Second line of defense: risk management and compliance function

The second line of defense shall support the first line of defense and to oversee all type of compliance and financial controlling issues. They are also involved in monitoring for suspicious activity, sanctions compliance screening (batch screening), and guiding in conducting initial and ongoing screening of customer onboarding. Are to monitor and report risk related practices and information,

The second line of defense, besides MLRO, shall be performed by the following officers/authorities

a. Chief Compliance Officer shall be responsible to ensure that the Bank has adequate policies and systems to safeguard the Bank against the risks of being used for any illicit activities. He/she shall communicate to the top management and the Board level committee towards managing the ML/TF risk. CCO shall also be responsible for effective implementation of the policies and guidelines/manuals, in all areas within the Bank.

b. Chief Risk Officer shall have to monitor operating effectiveness of mitigating controls and conduct assessment of the residual risk, which considers the effectiveness/status of the controls against the ML/TF risks of the bank. The residual risk should be measured and within the bank's risk appetite, otherwise an action plan is to be developed in correcting underperforming controls based on identified gaps.

c. Chief Operating Officer shall be responsible for establishing proper implementation mechanism of checks/control as per this Policy across the Bank.

d. Chief-Information Technology Officer shall be responsible for providing appropriate level of assurance to the Bank that the system produces accurate results / reports that helps to implement AML/CFT program.

e. Branch/Department AML Officer (Operations In-charge or an official designated by MLRO in consultation with AML/CFT Committee) shall ensure that norms of AML/CFT are fulfilled in the branches/departments. This officer shall report to the MLRO or the AML/CFT Unit.

1.4.6.3 Third line of defense: internal audit function.

The Third Line of Defense will be performed by internal audit. The Bank's internal audit shall carry out AML/CFT theme-based audit, through a risk-based approach, where it will review activities (effectiveness) of the first two lines of defense with the purpose to ensure to the BOD and senior management that applicable act/ rules/ directives and internal policies / manuals requirements are being carried out effectively.

CHAPTER 2: CUSTOMER IDENTIFICATION AND DUE DILIGENCE

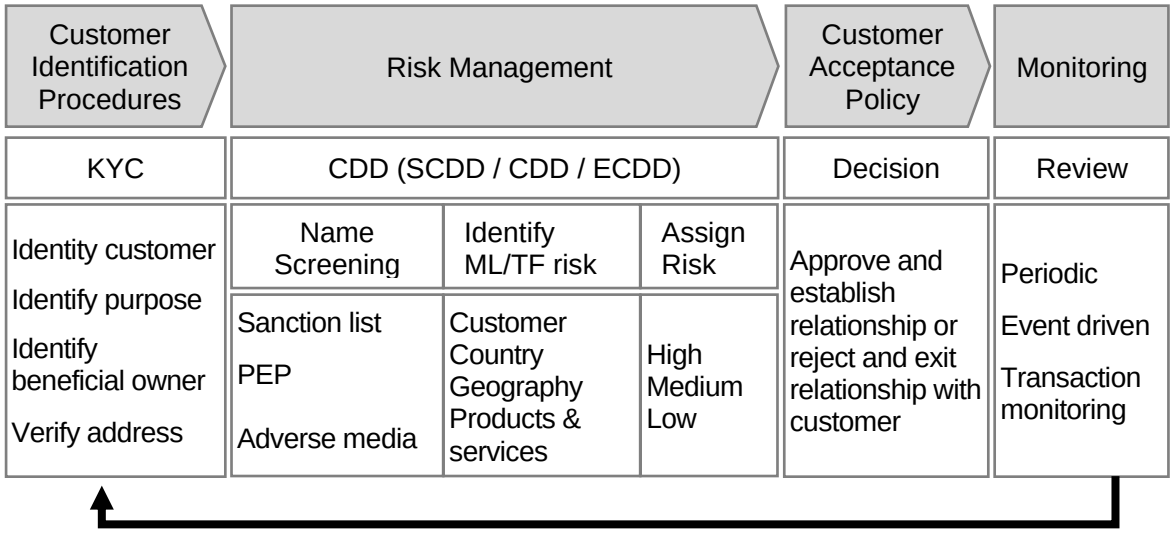
2.1 Know Your Customer

To manage ML/TF risks effectively, Bank must understand its customers. The purpose of understanding its customers is to verify the identity of its customers to safeguard the bank from being used by criminal elements for ML/TF activities.

2.2 KYC Elements

The Bank shall incorporate the following four key elements required for KYC:

a. Customer Identification Procedures
b. Risk Management
c. Customer Acceptance Policy
d. Monitoring of transactions



2.2.1 Customer Identification Procedures

The bank shall perform customer identification procedures to identify its customers while onboarding a new customer and throughout the banking relationship with the customer. The bank shall

a. Obtain all required information necessary to establish the identity of a new customer and the purpose of the transaction with the bank.
b. Verify the identity of the customer using reliable, independent source documents, data or information.
c. Identify the beneficial owner. This includes knowing and understanding the ownership and control structure of the customer.
d. Conduct periodic name screening of the customer base to identify high risk or any prohibited customers.
e. Give special consideration to the treatment of PEPs (whether as customer or beneficial owner). The bank shall:
    i. Have appropriate systems to determine whether the customer or the beneficial owner is a PEP.

ii. Obtain senior management approval for establishing or continuing such relationships.
iii. Take reasonable measures to establish the source of wealth and source of funds
iv. Conduct enhanced customer due diligence.

f. Conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted by its customers are consistent with the Bank's knowledge of the customers and the customers' businesses and risk profiles.
g. Customer onboarding and verification through technological applications (internet, telephone, fax, postal services or others) shall be based on a risk-based approach which shall be as robust as those for face- to-face customer verification and in adherence with the prevailing regulations and laws.

2.2.2 Risk Management

The Bank shall establish system of risk grading of each customer based on their risk profile by evaluating the impact of transactions to the Bank and as guided by Asset (Money) Laundering Prevention Act and NRB Directive. The Bank shall consider other influencing factors such as geography or country, customers (including occupation, profession, and type), product or service availed, nature of the transaction, and delivery channels used in categorizing customers as per the risks associated with them into "Low Risk", "Medium Risk", and "High Risk" categories.

2.2.2.1 Identification of inherent ML/TF risk

To assess the inherent ML/TF risks faced by the Bank, Bank shall include the following risk categories in its risk assessment process:

a. Customer

The Bank shall determine the potential ML and TF risks posed by a customer, or category of customers, based on occupation, profession, and transaction, which shall be in line with the recommendation of FATF and the Regulator.

b. Country

The Bank shall introduce mechanism / system to identify high risk jurisdiction/ sanctions countries known to be supporting international terrorism, and those with deficiencies in combatting money laundering and terrorist financing before establishing relationship and carrying out the transaction on behalf of a customer thus requiring ECDD. In doing so the bank shall include countries identified by FATF as lacking adequate money laundering laws and regulations.

c. Geography

The Bank shall assess the risk of its customers or transactions conducted in geographical areas within the country where illegal activities are high.

d. Products and services offered

The Bank shall identify the High-risk product and delivery channels and apply appropriate measures to mitigate the risk of ML/TF. The Bank shall pay special attention to the ML/TF threats arising from new or developing technologies.

2.2.2.2 Assessment of internal controls

The Bank shall ensure that the process and practices to manage the inherent risks identified are proper. For this, the Bank shall rely on internal audit and internal compliance testing. The Bank shall conduct self-assessment of control effectiveness of AML/CFT program to develop risk mitigating strategies.

The assessment shall consider the followings

a. Identify and assess the ML/TF risks that are significant to the Bank.
b. Effectiveness of controls to manage and mitigate the assessed risks.
c. Alignment of the risk based on the National Risk Assessment report of the country.
d. Managing risk based on business relationship, transaction threshold and nature of customer.
e. Mechanism to record digitally customer information obtained in the process of Customer Identification in unified way and ensure that such customer data are updated in line with the risk profile.
f. Mechanism where Customer Identification process requires customer to be identified based on centralized record of the customer kept digitally by the bank, when updating data/information of the customer availing different product/service of the bank it shall be updated in one single system.

2.2.2.3 Assessment of residual risk

Risk management generally shall be regarded as a continuous process. The Bank therefore, ensures that its risk management process for managing ML/TF risks are kept under regular monitoring and review.

The Bank shall revisit its assessments at least annually as per the provision in Unified Directive[5]. The risk-based approach principals propose identification, assessment, understanding, and mitigation of ML/TF risk including explicit consideration to key risk factors and its impacts in management of such risks.

The results of the risk assessment and measures taken by the Bank to manage the identified risks shall be consolidated within a comprehensive report and communicated to the AML/CFT Committee and Asset (Money) Laundering Prevention Committee. This will ensure that the bank is aware of the key risks, control gaps, and remediation efforts.

2.2.3 Customer Acceptance Policy

The Bank shall clearly define the information and documents required to establish a new relationship with a customer. The Bank shall define circumstances under which a new relationship would not be accepted, or a current relationship would be

[5] At present Unified Directive 2078, Directive no. 19/078, clause (9)(7)

terminated. The customer acceptance policy shall take a risk-based approach to understand and mitigate risk.

2.2.3.1 Prohibition of relationship

The Bank shall not accept or maintain relationship with the following person/entities:

a. Anonymous or Fictitious customer /accounts.
Bank shall ensure that no anonymous accounts or accounts that are in the name of fictitious persons are opened or maintained. The Bank must take all reasonable steps to confirm the true identity of the customer by collecting all relevant information and documents to ascertain the identity of the beneficial owner of the account.

b. Shell banks including those banks that maintain relationship with shell bank.
The Bank shall ensure that it does not maintain any relationship with shell entities including those banks that maintain relationship with shell bank.

c. Unregistered entity (except allowed by regulator or legal body for specific purpose).
The Bank shall not establish relationship with entities that are not registered under the law of Nepal.

d. The customer acting on behalf of another customer to open an account.
The Bank shall not establish relationship with a customer who is acting on other person's behalf without any legal right to do so.

e. Entities/persons appearing in sanctioned lists of Nepal Government and international bodies that include UN, HMT, EU, OFAC, Australian list.
The Bank shall not establish relationship or enter into any transaction directly or indirectly with sanctioned person, group and entity.

f. The customers who are unwilling and/or unable to provide mandatory documents, information, and/or details required for customer identification and verification.[6]
The bank shall not establish or continue relationship with a customer who is reluctant to provide documents, and information mandatorily required to identify and access ML/TF risk associated with the customer.

g. The customers whose documents, information, and other details provided to the Bank appear conflicting to the identity of the customer.
The Bank shall not establish relationship with a customer whose information provided to the Bank is found to be suspectable, dubious, conflicting, or misleading in accessing ML/TF risk associated with the customer.

[6] Unified Directive 2078, directive no. 19/078, Clause (16) (7) added through NRB circular 4/079/80 dated 2-Dec-22 (2079/8/16 BS)

h. Those who deal with crypto currency.[7]
The Bank shall not establish relationship with a customer who deals with crypto currency as there is limited identification and verification of participants as well as lack of a proper regulator for supervision and legal enforcement regarding crypto currency.

i. Those who deal with armaments.
The Bank shall not involve in any transactions related with purchase or sale of arms.

j. The customers involved in activities prohibited under Nepalese jurisdiction.

k. End of relationship
Where the Bank is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by an existing customer, the Bank shall initiate to terminate the business relationship[8] after issuing notice to the customer explaining the reasons for taking such a decision.

2.2.4 Monitoring of Transactions

The Bank shall monitor the transactions of its customers based on risk profile, size, complexity, and activities to check and ensure whether they are consistent with the bank's knowledge of the customer. Transaction monitoring shall be conducted to identify any unusual activity and to assist the Bank in meeting statutory obligations with respect to reporting potentially suspicious transactions. In identifying, investigating, and reporting suspicious activity, banks can collect relevant information from various departments, branches, and subsidiaries.

The Bank shall give more attention to the transactions that do not match with the customers/profile, the line of business, high value transactions, high account turnover and transactions exceeding threshold limit. The automated system shall be deployed for monitoring purpose and any deviation in the transaction performed in the account against the customer profile shall be followed by reviewing of the customer profile and by conducting proper due diligence based on transactions and risk categorization of the customer.

2.3 Customer Due Diligence

The bank shall conduct due diligence of its customers and update such due diligence throughout the banking relationship with the customer based on the customer risk level. The Bank shall apply customer due diligence in the following circumstances:[9]

a. Establishing a new business relationship
b. Opening of an account
c. Carrying out occasional transactions above the established threshold limit
d. Cross-border and domestic wire transfers
e. When there are doubts about the authenticity or adequacy of previously obtained customer identification data.

[7] Prohibition on dealing in crypto currency is an existing provision of our policy. NRB has banned dealing in crypto currency through the notice published on 2078/10/09
[8] ALPA – Chapter 3, Clause (7)(ANA)(2)
[9] ALPA – Chapter 2, Clause (7)(KA)(1)

f. There is suspicion of money laundering or terrorist financing.
g. Each transaction conducted by high-risk customers
h. Other provision as prescribed by the Regulator.

2.3.1 Types of CDD based on customer risk rating

The Bank shall assign customer risk ratings to determine the level of controls needed to be employed to manage the risk, including the type of ongoing suspicious activity monitoring. Following customer due diligence will be applied to the customers categorized under high risk, medium risk, and low risk as per ALPA, Rules, and NRB directive.

a. Simplified Customer Due Diligence (SCDD):
   Simplified CDD is the lowest level of due diligence, which shall apply on those customers with low risk of ML/TF activity. The Bank shall establish a separate simplified mechanism to obtain information/ and documents of such customers.

b. Customer Due Diligence (CDD):
   Customer due diligence shall be applied to those customers who have moderately higher ML/TF risk. The due diligence shall be made to understand the purpose and intended nature of the business relationship from the type of transactions or business relationship established.

c. Enhanced Customer Due Diligence (ECDD)
   The Bank shall apply ECDD measures if the customer risk is deemed to be higher. ECDD shall be applied to satisfy the Bank for the establishing and continuing relationship. The bank may apply ECDD to low or medium risk customer on its own discretion.

CHAPTER 3: MONITORING AND REPORTING

3.1 Transaction monitoring

Transaction monitoring involves analyzing transactions of the customers of the Bank based on defined parameters to determine whether such transactions are as per the Bank's knowledge of the customer. Transaction monitoring is targeted towards informing the Bank to unusual activities in meeting the Bank's statutory obligations with respect to reporting potentially suspicious transactions.

The Bank shall monitor the transactions based on risk-based approach through an automated system in addition to the exception reports developed internally by the Bank. For transaction monitoring, the Bank shall consider customer risk profiles and information collected during the CDD process. Alert scenarios and setting limit for particular activity shall be as guided at least by AML/CFT Committee.

In addition to the regular activities, the Bank shall provide special attention to the following activities:

a. Wire Transfer:
   Messages associated with wire transfers shall be subject to ongoing monitoring. In the context of wire transfers, the Bank shall identify the sender and beneficiary of the wire transfer.

b. Trade related transactions:
   All the trade transactions including all related parties thereto shall be strictly sanction checked / monitored prior to the execution ensuring that the appropriate customer due diligence is carried out properly and periodically and to prevent TBML.

c. Correspondent Banking:
   The Bank shall carry out ECDD while establishing a new correspondent relationship. Treasury Department shall review existing correspondent banking relationship at least on an annual basis. Treasury Department shall perform CDD for all the existing Banks/Financial Institutions with which the Bank has correspondent relationship. If the assessment is not satisfactory to the Bank in terms of AML/CFT measures, it shall be communicated to AML/CFT Unit for presentment in AML/CFT Committee for appropriate instructions/ guidance. Treasury Department shall collect questionnaire in the Bank's format or Wolfsberg Questionnaire during onboarding and every year and provide it to AML/CFT Unit.

d. Remittance agents / other partners:
   The bank shall carry out ECDD of remittance partners while establishing a new relationship for remittance. Remittance Department shall review existing relationship at least on an annual basis. Remittance Department shall perform CDD for all the existing remittance partners. If the assessment is not satisfactory to the Bank in terms of AML/CFT measures, it shall be communicated to AML/CFT Unit for presentment in AML/CFT Committee for appropriate instructions/ guidance. Remittance Department shall collect questionnaire in the Bank's format or Wolfsberg Questionnaire during onboarding and every year and provide it to AML/CFT Unit.

e. Downstream Correspondent Banking (Nested Account): The Bank shall not allow downstream correspondent banking service and nested account activities to other financial institutions.

f. Payable-through Accounts or Pass-through Accounts
The Bank shall not allow its customers to directly access the correspondent account to conduct business on their own behalf.

g. Use of personal accounts for business purposes
The Bank shall discourage use of personal saving accounts to be used for business purposes.

3.2 Reporting

3.2.1 Resubmission Policy

Bank shall not attempt to resubmit any transaction that has already been rejected due to the concern over Sanctions or ML/TF. The records of such transactions are to be maintained.

3.2.2 Failure to Report

Staff failing to report any identified unusual and suspicious transactions, shall be subject to action in accordance with Bank's policy ALPA or NRB Directive as appropriate. MLRO shall have the authority to recommend suitable action for such staffs failing to adhere with this policy in consultation with CCO.

3.2.3 Sanctions and Name Screening

Any person or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of WMD shall be screened and such listed person/entity asset/fund, held singly or in joint ownership, increment in such fund/asset shall be blocked (freeze) and reported as per the Chapter 6 (kha), Section 29 (cha) of Asset (Money) Laundering Prevention Act 2064.

Bank shall have an appropriate Sanction Screening mechanism (including batch screening); the sanction list whenever gets updated shall be reflected in the system. Further, Departments/Branches while opening account, reviewing account, and initiating the wire transfer transaction shall perform the sanction check against customer and parties involved in the transaction. If any exact/true match is found with the list of United Nations Security Council, the Bank shall block/freeze the accounts/assets of such customer immediately and notify to the regulator[10]. Similarly, any customer under doubt on their information should also be referred to the MLRO as suspicious. The MLRO shall investigate on such issues and derive conclusion within reasonable time and give appropriate instruction.

Further, the Bank shall check various lists directed/required by ALPA Act, Regulator and any other competent authorities so as to safe-guard Banks reputation and prevent it from being used by money launderers and terrorists, such as OFAC, UN, EU, HMT, Australian sanction list, Government of Nepal or any other sanctions list as deemed necessary by the Bank.

[10] ALPA, 2064 – Chapter 6KHA, Clause (29 CHHA)(5)

3.2.4 PEP and adverse screening

Bank shall adopt appropriate mechanism to screen the customer against PEP and adverse media list, while establishing and maintaining the relationship, so that the enhanced customer due diligence could be performed.

3.2.5 Reporting Obligations

Bank shall generate AML/CFT related reports as per the NRB Directive in prescribed format/system and submit the same to the Regulator, for which the Bank shall have effective reporting system so that reports are generated and reported on time.

Bank shall develop and implement guidelines on the identification of suspicious transaction based on STR Guidelines issued by FIU, National and International risk assessment, and the Bank's Annual Risk assessment reports so that all staffs - especially dedicated Branch/Department AML Officer - shall be able to identify and report suspicious/unusual transactions to the MLRO or AML/CFT Unit. However, this shall not limit any staff member to speak up and directly report suspicious/unusual transactions to the MLRO. The MLRO shall further analyze and, if suspicion is established, shall be reported to FIU. Similarly, TTR shall also be reported to the FIU by the AML/CFT Unit as per TTR and other related guidelines issued by FIU.

3.3 Record Keeping

The Bank shall maintain following records accurately and securely records for minimum of five years after the termination of business relationship or from the date of transaction or from the date of occasional transaction:

a. Documents and records related to identification and verification of customer and beneficial owner,
b. Documents, records and conclusion of the analysis of customer or beneficial owner and transaction,
c. Documents, details and records related to accounting and business relation of the Bank
d. Documents, details and records relating to domestic and foreign transactions,
e. Documents, details and records of attempted transactions,
f. Other documents, details and records as prescribed by regulators.

CHAPTER 4: AWARENESS AND TRAINING

4.1. Training

Bank staffs, BOD, and shareholders holding 2% and above shares shall be made aware of the statutory and regulatory obligations on AML/CFT in coordination with HRD. The Bank shall refresh employees' knowledge on the practices of ML/TF from time to time with indications to the recognition of suspicious transactions. Awareness on prevention of money laundering & financing of terrorism shall be raised through a periodic and regular training to all the staff members including new recruits of the bank about what money laundering & financing of terrorism is, the identification of suspicious transactions, the regulatory requirements on prevention of money laundering and financing of terrorism, the Bank's policy, procedure, and controls for prevention of money laundering & financing of terrorism.

Further, onsite/offsite branch/departments visits shall be conducted by the AML/CFT Unit as felt necessary to check/monitor the activities and to create awareness in aspect to AML/CFT. Feedback of onsite visits shall be submitted to the CCO for review. More extensive training including foreign training shall also be provided to staff under AML/CFT functions. The training shall be conducted in coordination with HRD. All Branch Managers/ Head of Departments shall ensure that all staff members have read and understood The Policy and Guideline.

4.2. Confidentiality and Tipping off

The Bank shall keep the details of all transaction of STR, TTR, and correspondence record to and from the regulatory body on Bank's customers under the investigation as confidential and this information shall not be shared with the customer or any irrelevant bank staff, unrelated official meetings or anyone outside the Bank. Tipping off will be treated as a criminal offense and be punished accordingly.

Further, any documents, information and transaction details of the customer shall be kept confidential and not leaked/shared to an unauthorized person. Such personal data is considered as confidential and is prohibited to be shared to the third party unless otherwise stipulated by the applicable Legislation[11].

4.3. Non-Compliance

Failure from staffs to abide by The Policy set by the Bank to prevent ML and TF will be treated as a disciplinary issue. Any deliberate breach will be viewed as gross misconduct. Further, such actions shall also attract the penalty as per the applicable legislation and regulatory provision. MLRO shall have the authority to recommend suitable action for such staffs failing to adhere with this policy in consultation with CCO.

4.4. Not to be Liable for Providing Information

In case any loss occurs to a person/customer or to the business of the bank as a result of submission of information to the FIU or other investigating authorities by the designated staff in good faith, the Bank shall not take any action to such designated officials.[12]

4.5. Importance of Know Your Employee (KYE)

The bank employees will conduct themselves in accordance with the highest ethical standards. Staff should not provide advice or other assistance to individuals who are indulging in ML/TF activities. Any knowledge / information of any staff involved in such

[11] ALPA – Chapter 6, Clause (26)
[12] ALPA – Chapter 8, Clause (37)

activities shall not be kept hidden and as per the Whistle-blowing Policy of the Bank, it shall be informed to the competent authority.

Similarly, HRD shall conduct Know Your Employee (KYE) procedure and maintain up-to-date information of each employee of the Bank. It shall also monitor the transaction of the employees and if any suspicious nature of activities related to ML/TF is observed it shall be notified/ reported to MLRO (or as designated).

4.6. Code-of-conduct

As per the Personnel Policy Guidelines of the bank, HRD shall obtain signed and accepted Code of Conduct from every staff ensuring that the staffs have understood and aware of code of conduct of the Bank. Also, a code for conduct for the BOD is also to be obtained[13].

[13] Unified Directive 2078, directive no. 19/078, Clause (18) (10) added through NRB circular 4/079/80 dated 2-Dec-22 (2079/8/16 BS)

CHAPTER 5: MISCELLANEOUS

5.1. AML/CFT Guidelines

A separate Guidelines document shall supplement this Policy. The Guidelines shall be reviewed by the MLRO at least on an annual basis or as and when required and may be amended/revised as per the requirement with approval of the CEO through AML/CFT Committee.

5.2. Others

All other internal documents of the Bank (policies, manuals, process notes, guidelines, etc.) shall be developed in compliance to this Policy. Likewise, all the process notes and product papers should mention about the monitoring and control mechanism of ML/TF as per this Policy and AML/CFT Guidelines where applicable.

While introducing new products and services or entering affiliation with any third party, the Bank shall confirm that it is in accordance with this Policy and NRB Directives and Act. Any affiliates of the Bank shall have policies and practices which prevent the organization from money laundering and terrorist activities. The Bank may review AML/CFT related documents and practices of such affiliates. The subsidiary companies of the Bank shall prepare their own AML/CFT Policy as directed by their respective Regulators and shall also be in line/spirit with the Policy of the Bank. The Bank representative office established abroad shall follow the ALPA and Provisions of their jurisdictions as well as The Policy and Guideline. Where there is a conflict or confusion between such, the more stringent policies, guidelines and rules shall apply.

5.3. Maintenance and Update

The review and update of this Policy shall be an ongoing process to ensure continuous alignment with the Bank's strategy, Risk assessment reports as per NRB Directives (such as Annual ML/TF Risk Assessment Report, etc.), and internal and external dynamics in which Bank operates. Such factors shall include the developments, changes, and trends whether required by law or by generally accepted risk management or business practices within the financial sector. Review and amendments of The Policy shall be assessed and approved by the BOD.

This Policy shall be subject to review at least once a year or whenever circumstances justify.

5.4. Repeal and Savings

The existing policy of the bank shall be repealed upon approval from BOD. All actions taken and functions performed shall be considered to have been taken or performed pursuant to The Policy.

5.5. Effective Date

The Policy shall come into effect following approval from the BOD with immediate effect.