NIC ASIA Bank Limited

Policy for Prevention of Money Laundering and Combating Financing of Terrorism and Proliferation

2026

Policy for Prevention of Money Laundering and Combating Financing of Terrorism and Proliferation

In exercise of the power conferred by Section 14(2) of Bank and Financial Institution Act 2073 and the Articles of Association of NIC ASIA Bank, the Board of Directors of NIC ASIA Bank has approved this "Policy for Prevention of Money Laundering and Combating Financing of Terrorism and Proliferation" vide its **773rd** Board Meeting dated **21st Aug 2026** for implementation after review and recommendation of **124th** "Assets (Money) Laundering Prevention Committee" meeting dated **06th Aug 2026** The core purpose of this policy document is to lay down a framework for prevention of money laundering and combating financing of terrorism, combating of proliferation and provide guidelines on AML/CFT/CFP compliance across all the functions of the Bank.

Version History

S. No.	Version	Approving Authority	Date of Approval
1	1st	Board of Directors	March, 2007
2	2nd	Board of Directors	September 15, 2014
3	3rd	Board of Directors	January 26, 2016
4	4th	Board of Directors	April 13, 2017
5	5th	Board of Directors	April 13, 2018
6	6th	Board of Directors	13th June 2019
7	7th	Board of Directors	11th May 2020
8	8th	Board of Directors	11th November 2020
9	9th	Board of Directors	24th February 2021
10	10th	Board of Directors	25th August 2021
11	11th	Board of Directors	10th February, 2022
12	12th	Board of Directors	14th December, 2022
13	13th	Board of Directors	15th March, 2023
14	14th	Board of Directors	11th September, 2024
15	15th	Board of Directors	22nd May 2025
16	16th	Board of Directors	21st August, 2026

Approval Sheet

Review and Approval	Name of Reviewing and Approving Authority	Full Signature	Initial Signature
Initiated By	Binod Gyawali Officer- Strategy		
Reviewed By	Kiran Poudel Manager- Strategy		
Reviewed By	Dipendra Sharma Head Compliance / AML Implementing Officer		
Reviewed By	Sanjish Aryal Head Internal Audit		
Reviewed By	Kamal Khadka Chief Operating Officer		
Reviewed By	Rupesh Luitel Chief Financial Officer		
Reviewed By	Dinesh Bhari Chief Legal Officer/Company Secretary		
Reviewed By	Dipendra Bahadur Rajbhandari Chief Risk Officer		
Supported By	Sujit Kumar Shakya Chief Executive Officer		

Table of Contents

Abbreviations

ALPA	Assets (Money) Laundering Prevention Act
AML	Anti Money Laundering
APG	Asia Pacific Group on Money Laundering
BCBS	Basel Committee for Banking Supervision
CAP	Customer Acceptance Policy
CBS	Core Banking Software
CDD	Customer Due Diligence
CFP	Combating Financing of Proliferation
CFT	Combating Financing of Terrorism
DNFBPs	Designated non-financial Businesses and Professions
FATF	Financial Action Task Force
FT	Financing of Terrorism
FP	Financing of Proliferation
FI	Financial Institution
BFI	Bank and Financial Institution
FIU	Financial Intelligence Unit
KYC	Know Your Customer
ML	Money Laundering
NRB	Nepal Rastra Bank
PEP	Politically Exposed Person
PIP	Person in Influential Position
SOP	Standard Operating Procedures
STR	Suspicious Transaction Report
TTR	Threshold Transaction Report

Chapter 1: Short Title, Commencement and Definitions

1.1 Short Title and Commencement

Anti-Money Laundering (AML) has developed to be of significant importance for financial institutions around the world. The many allegations and revelations that BFIs are used as a vehicle for providing financial services to money launders and terrorists garnered enormous impetus to curb channeling of money derived from crime or aimed at funding terrorism. Moreover, governments are pursuing reforms in regulatory structures and are also cracking down on tax evasion to recover lost revenue. The stringent provisions made in laws and directives reflect the seriousness of this issue; non-compliance of which may cause significant reputational risk as well as may result in adverse consequences for the Bank. Regulators have also been closely monitoring the AML/CFT/CFP policies, procedures, guidelines and practices of financial institutions.

In order to prevent the Bank from being used for money laundering and financing of terrorism, the Board of Directors of NIC ASIA Bank has approved this policy. This policy has laid down appropriate framework for effective compliance to prevailing Asset (Money) Laundering Prevention Act 2064, (and its latest amendment), Assets (Money) Laundering Prevention Rules, 2081 and Directives issued by Financial Intelligence Unit (FIU) and Nepal Rastra Bank (NRB) from time to time.

Name of Policy Document : Policy for Prevention of Money Laundering & Combating Financing of Terrorism and Proliferation

Ownership : Compliance Department

This Policy shall be known as the "Policy for Prevention of Money Laundering & Combating Financing of Terrorism and Proliferation" and shall came into force from the date of approval of the Board.

1.2 Definitions

Unless otherwise specifically indicated, the following terms used in the ***"Policy for Prevention of Money Laundering and Combating Financing of Terrorism and Proliferation"*** shall have the following meaning(s):

a. **"ALPC"** refers to the Board level "Assets (Money) Laundering Prevention Committee" of the Bank.

b. "**The Policy**" refers to "Policy for Prevention of Money Laundering Combating Financing of Terrorism and Proliferation"

c. "**Competent Authority**" in relation to exercise of any power under this Policy means the Board, Chief Executive Officer or any other authority to whom such power is delegated by the Board or Chief Executive Officer from time to time.

d. **"Money Laundering (ML)":**

Money laundering refers to any of the following acts:

1. The conversion or transfer of funds, by any person who knows, should have known or suspects that such funds are the proceeds of crime, for the purpose of concealing or disguising the illicit origin of such funds or of assisting any person who is involved in the commission of the predicate offence to evade the legal consequences of his actions.
2. The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to funds by any person who knows, should have known or suspects that such funds are the proceeds of crime.
3. The possession, acquisition, or use of funds by any person who knows, should have known or suspects that such funds are the proceeds of crime.

e. **"Financing Terrorism"**

An act committed by any person who, in any manner, directly or indirectly, and willingly, provides or collects funds, support, or attempts to do so, in order to use them or knowing that these funds will be used in whole or in part for the execution of a terrorist act, or by a terrorist or terrorist organization.

f. **"Act", "Rules" and "Directive"**

In this policy, "Act" will refer to the Asset (Money) Laundering Prevention Act, 2064 and its latest amendment. The "rules" will refer to the Asset (Money) Laundering Prevention Rules 2081 and "Directive" will refer to the directive issued from Nepal Rastra Bank and Financial Intelligence Unit .

g. **Terrorist**

Any natural person or organization who commits the following acts:

1. Commits or attempts to commit terrorist acts by any means, directly or indirectly, unlawfully and willfully,
2. Participates as an accomplice in terrorist acts,
3. Organizes or directs others to commit terrorist acts, or

4. Contributes or cooperates to the group of persons acting with a common purpose of commission of terrorist acts where such contribution or cooperation is made intentionally and with the aim of furthering the terrorist act or with the knowledge or the intention of the group to commit a terrorist act.

h. **Correspondent Banking**

The provision of banking services by one financial institution (correspondent bank) to the customer of another financial institution (respondent bank).

i. **Respondent Bank**

A Bank that uses the services of another bank called a correspondent bank for performing certain services, e.g. check clearing and collection, purchase and sale of foreign exchange etc.

j. **Nested (downstream) correspondent banking**

Nested or downstream correspondent banking refers to the use of a bank's correspondent relationship by a number of respondent banks through their relationships with the bank's direct respondent bank to conduct transactions and obtain access to other financial services.

k. **Proceeds of crime**

Any property derived from or obtained directly or indirectly through the commission of money laundering or predicate offence and it shall also include any other property and economic advantage gained or derived from such property or any property transferred or converted into other property or advantage, in full or in part, from such property or advantage.

l. **Transaction**

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

1. Establishing business relationship,
2. Opening of an account,
3. Any deposit or collection, withdrawal, exchange or transfer of funds in any currency or instruments, payment order by electronic or any other means,
4. Use of any type of safe deposit box (locker),
5. Entering/establishing into any fiduciary relationship,

6. Any payment made or received in satisfaction, in whole or in part, of any contractual or other legal obligation,
7. Any payment made or received in respect of a lottery, bet or other game of chance,
8. Establishing or creating a legal person or legal arrangement, or
9. Such other act as may be designated by the Government of Nepal by publishing a notice in the Nepal Gazette.

m. **Legal Person**

Any company, corporation, proprietorship, partnership firm, cooperatives, or any other body corporate.

n. **Legal Arrangement**

Trust (express trust) or other similar kind of legal arrangements.

o. **Client/ Customer**

Any individual or entity who seeks/attempts to enter or has already entered into a business relationship, or conducts a one-off transaction with the bank as principal or as a client agent. Any person or entity connected with a financial transaction that may impose significant reputational or other risks to the Bank.

p. **Employee / Staff**

Employee / Staff means employee / staff of the Bank as defined in the Staff Service By laws of the Bank.

q. **Politically Exposed Persons (PEP)**

A Politically Exposed Person (PEP) is an individual who is or has been entrusted with a influential public position due to which he/she is considered to have a higher risk of money laundering.

PEP shall be broadly classified into following categories:

1. Current Domestic PEP
2. Former Domestic PEP
3. Foreign Neighbor Country PEP
4. Foreign Other Country PEP
5. Foreign High position PEP
6. Former Foreign PEP
7. PEP Associates

Detailed provision related to PEP has been incorporated in Integrated KYC guideline for Customer Acceptance and Correspondent Banking Relationship.

r. **Beneficial owner**

Natural person who, directly or indirectly, owns or controls or directs or influences a customer, an account, or the person on whose behalf a transaction is conducted, or exercises effective control over a legal person or legal arrangement or remains as an ultimate beneficiary or owner of such activities.

s. **Customer Due Diligence (CDD)**

Customer Due Diligence is the process of identifying and evaluating the customers and the assessment of customer risk as part of know your customer (KYC) process, allowing banks to better identify, manage, and mitigate the AML related risks. The level of due diligence is based on the risk level of the customer and thus there may be various levels of due diligence prescribed by the regulators or decided by the bank. Currently, following are the categories of due diligence specified in NRB directive:

i. Standard/Normal Customer Due Diligence

This is conducted for low risk customers who do not fall under enhanced and simplified customer due diligence.

ii. Simplified Customer Due Diligence (SCDD)

This can be conducted for customers who fall under low risk customers having characteristics as specified by NRB directive i.e. financial institutions supervised by NRB, customers whose identity is publically available and controlled by national system and other specified by regulator from time to time.

iii. Enhanced Customer Due Diligence (ECDD)

Enhanced Customer Due Diligence is conducted for high risk and medium risk customers. It refers to the additional due diligence pertaining to the identity of the customer, source of income, nature and value of transaction and others specified by directives.

t. **Risk Based Approach (RBA)**

The approach of management which focuses on identifying and addressing potential risks of money laundering and terrorism financing. The core of this approach is to creating the match between “risks and controls” by understanding of the ML/FT risks to which the banks are exposed and apply AML/CFT/CFP measures in a manner and to an extent which would ensure mitigation of these risks. There is no universally accepted methodology, which prescribe nature and extent of risk based approach. It provides every bank the flexibility to manage their ML/FT risks in their own way.

u. **Suspicious Transaction:**

A transaction, including an attempted transaction, whether or not made in cash, which to a person acting in good faith;

- Gives rise to a reasonable ground of suspicious that it may involve proceeds of an offenses specified in law and regulations, regardless of the value involve.
- Seeks to conceal or disguise the nature or origin of funds derived from illegal activities
- Appears to have no economic rationale or bona-fide purpose
- Appears to be in circumstances of unusual, or unjustified complexity
- Appears to be deviated from profile, character and financial status
- Seems to be made with the purpose of evading the legal and regulatory reporting requirements
- Found to be conducted to support the activities relating to terrorism

v. **Suspicious Transaction Report:**

A report to be made by Financial Institutions to Financial Intelligence Unit on any suspicious transactions or any attempts under the provisions of "Parichhed 3, 7(*dha*) Asset (Money) laundering prevention Act, 2064 (amendment 2080)" and point no. 16 of Unified NRB Directive no. 19/082.

w. **Wire Transfer:**

Any transaction carried out on behalf of an originator (both natural persons and legal entities) through the bank by electronic means with a view to making an amount of money available to a beneficiary person at another FI. The originator and the beneficiary may be the same person.

x. **Financial Intelligence Unit (FIU)**

In order to work against the money laundering and terrorist financing activities Financial Intelligence Unit (FIU) was established on April 21, 2008 pursuant to section 9 of the Assets (Money) Laundering Prevention Act, 2008 within Nepal Rastra Bank (the Central bank) as an independent unit. It is Nepal's financial intelligence unit. It is a central, national agency responsible for receiving, processing, analyzing and disseminating financial information and intelligence on suspected money laundering and terrorist financing activities.

y. **Shell Bank/entity**

A bank or entity, which has no physical presence in the country in which it is incorporated, licensed or located, and which is not affiliated with a regulated financial services group that is subject to effective consolidated supervision. For the purpose of this clause, presence of local agent or junior level staff does not constitute physical presence. Shell banks/entities in themselves may not be illegal as they may have legitimate business purposes. However, they can also be a main component of underground activities, especially those based in tax havens.

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

z. **Vendors**

The term Vendor, for the purpose of this document, denotes any third party who supplies the Bank with any product through transfer of ownership or by with whom such purchases is made by the Bank.

aa. **Subsidiary Company**

Subsidiary company in relation to any other company (i.e. Holding Company) means a company in which holding company holds more than 50 percentage of the shares of a company.

bb. **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 (including both technologies and dual use goods used for non-legitimate purposes) in contravention of national laws or, where applicable, international obligations.

cc. **Payable through Accounts**

The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

dd. **Targeted Financial Sanctions**

As per FATF recommendation 6, the term targeted financial sanctions means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.

Other than the terms specifically defined hereinabove, the terms used in various sections of this Policy shall have the same meaning as has been defined under various other policy documents of the Bank and the applicable laws of land, and NRB Directive wherever relevant.

1.3 Scope and Applicability:

This policy shall be applicable to all the staffs, Bank functions and structures. If any department, branch or business unit of the Bank is unable, in an exceptional circumstance, to apply the standards set by this policy, they must have pre-facto approval of the Chief

Executive Officer (CEO) in recommendation of the Deputy Chief Executive Officer, Assistant Chief Executive Officer, Chief Operating Officer, Immediate Subordinate of Chief Operating Officer, Chief Risk Officer and Head Compliance or AML Implementing Officer.

1.4 Objectives

The major objectives of the policy are:

- To lay down a framework to be implemented by the Bank in order to safeguard it against being used for money laundering, financing of terrorism and proliferation financing.
- To ensure full compliance by the Bank with all applicable legal and regulatory requirements pertaining to money laundering, financing of terrorism, and proliferation financing and
- To provide a broad framework for formulation and implementation of various manuals or procedural guidelines that is required for effective AML/CFT/CFP & KYC compliance.

1.5 Description of Money Laundering, Financing of Terrorism and Proliferation Financing

oney Laundering

The Financial Task Force on Money Laundering defines the money laundering as:

"The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money Laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source.

Illegal arms sales, smuggling, and the activities of organized crime including for example drug trafficking and prostitution can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimize" the ill-gotten gains through money laundering.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

In response to mounting concern over money laundering, the Financial Action Task Force on money laundering (FATF) was established by the G-7 Summit in Paris in 1989 to develop a co-ordinate international response. One of the first tasks of the FATF was to develop Recommendations, 40 in all, which set out the measures national governments should take to implement effective anti-money laundering programs".

a. Money Laundering Process

The Money Laundering consists of the following processes:

I. Placement

In the initial or placement stage of money laundering, the launders introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposit directly, into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.

II. Layering

After the funds have entered the financial system, the second - or Layering – stage take place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channeled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

III. Integration

Having successfully processed his criminal profits through the first two phases of the money laundering process, the launderer then moves them to third stage – integration – in which the funds re-enter the legitimate economy. The launderer m ight choose to invest the funds into real estate, luxury assets, or business ventures.

b. Money Laundering Areas

As money laundering is a necessary consequence of almost all profit generating crime, it can occur practically anywhere in the world. Generally, money launders tend to seek out areas in which there is a low risk of detection due to weak or ineffective anti-money laundering programs. Because the objectives of money laundering is to get the illegal

funds back to the individual who generated them, launderers usually prefer to move funds through areas with stable financial systems. Therefore, Banks have been the targets for money launderer.

Money laundering activity may also be concentrated geographically according to the stage the laundered funds have reached. At the placement stage, for example, the funds are usually processed relatively close to the under-lying activity: often but not in every case, in the country where the funds originate.

With the layering phase, the launderer might choose an offshore financial center, a large regional business center, or a world banking center – any location that provides an adequate financial or business infrastructure. At this stage, the laundered funds may also only transit bank accounts at various locations where this can be done without leaving traces of their source or ultimate destination.

Finally, at the integration phase, launderers might choose to invest laundered funds in still other locations if they were generated in unstable economies or locations offering limited investment opportunities.

One of the latest trends in money laundering involves use of the new payment technologies like Smart Cards, Online Banking and Electronic Cash etc. The Bank should be vigilant and should administer the robust controlling, monitoring and reporting system to Prevent money laundering and financing of terrorism through such channels.

c. Risks of money laundering and terrorist financing to the banks

Bank is exposed to several risks if it fails to prevent the Bank being used for M/L and F/T activities.

I. **Reputational risk:** The reputation of a business is usually at the core of its success. The ability to attract good employees, customers, funding and business is dependent on reputation. Even if a business is otherwise doing all the right things, if customers are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong policy helps to prevent a business from being used as a vehicle for illegal activities.

II. **Operational risk:** This is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If AML policy is faulty

or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, time and money is then spent on legal and investigative actions and the business can be viewed as operationally unsound.

III. **Compliance Risk:** Risk of loss due to failure of compliance with key regulations governing the Bank's operations.

IV. **Legal risk:** Risk of loss due to any of the above risk or combination thereof resulting into the failure to comply with Law and having a negative legal impact on the Bank. The specific types of negative legal impacts could arise by way of fines, confiscation of illegal proceeds, criminal liability etc.

V. **Financial risk:** Risk of loss due to any of the above risks or combination thereof resulting into the negative financial impact on the Bank.

d. International Initiatives

The international community has acted on many fronts to respond to the growing complexity and the international nature of rapidly evolving ML/FT/FP methods. The emphasis is on promoting international cooperation and establishing a coordinated and effective international AML/CFT/CFP regime. Many international agencies have helped countries develop a capacity to prevent and counter ML. The following presents some of the main elements of the global and regional initiatives.

- The Financial Action Task Force (FATF) was established in 1989 by the G-7 countries to respond more effectively to ML. The FATF Forty Recommendations require the criminalization of ML. In addition, the recommendations call on countries to adopt legislative and other measures in order to: freeze, seize and confiscate criminal proceeds; waive bank secrecy laws to permit financial institutions to monitor and report suspicious transactions; protect those reporting these transactions from civil and criminal liability; establish financial investigation units; and, cooperate fully in international law enforcement efforts to combat ML. The FATF Special Recommendations require countries to criminalize the financing of terrorism, terrorist organizations and terrorist acts and to designate these new offences as ML predicate offences. The FATF is also involved in monitoring the progress of members in complying with its recommendations.
- The United Nations Convention on Illicit Trafficking in Narcotic Drugs and Psychotropic Substances (Vienna Convention), the UN Convention against Transnational Organized Crime (Palermo Convention), the UN Convention against Corruption and the International Convention for the Suppression of the Financing

of Terrorism all contain provisions relating to the tracing, freezing, seizing and confiscation of instrumentalities and proceeds of crime.

- Financial regulation standards are also set by the Basel Committee on Banking Supervision. In 1988, the Basel Committee put forward some basic principles as part of its Statement for the Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering. It has also issued a paper a "sound management of risks related to money laundering and financing of terrorism in 2014".
- Wolfsberg Group, which is non- governmental organization of 13 large commercial banks founded in AD 2000, develop and publishes financial industry standards for Anti-money laundering (AML), Know Your Customer (KYC) and Counter Terrorist Financing (CTF) policies. Its work is similar to what the Financial Action Task Force on Money Laundering (FATF) does on a government level.
- Many countries have established financial intelligence units (FIUs) as a focal point for the AML efforts and a point at which information is exchanged between financial institutions and law enforcement. Since 1995, a number of these units have begun to work closely together, to exchange information and to coordinate their AML efforts. They formed the Egmont Group which facilitates international exchanges and cooperation among FIUs in relation to both ML and FT.
- Multi-lateral organizations like World Bank, International Monetary Fund, Asian Development Bank also work on preventing ML/FT risks. They also provide financial and technical assistance to countries wishing to implement the FATF 40 recommendations. They have also published several papers on the theme of preventing ML/FT risks for the financial industry.
- As part of its work to promote good governance and to fight corruption, the Commonwealth has long been involved in international AML/CFT efforts. In 1993, it made available a Commonwealth Model Law. In 1996, it developed Guidance Notes for the Financial Sector which was revised in 2000 and in 2005 based on best practices.
- Asia Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organization founded in 1997 in Bangkok, Thailand consisting of 42 members. APG members are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism. Nepal became the member of APG Group in June 2002.

inancing of Terrorism

Terrorist financing 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 legal 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.

roliferation Financing

It focuses on preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to proliferators or proliferation; and the use of funds or other assets by proliferators or proliferation, as required by the United Nations Security Council (the Security Council).

Recommendation 7 by FATF requires countries to implement targeted financial sanctions 18 to comply with United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available to, and for the benefit of, 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 weapons of mass destruction.

Chapter 2: Legal and Regulatory Obligations and International Standards to be followed

The bank is obliged to comply with the requirements of the following laws, rules and regulations of the homeland. In addition, Nepal has to follow standards prescribed by FATF as an obligation of member country of Asia Pacific Group on Money Laundering, which is a FATF style regional body.

2.1 Legal Obligations

The bank is obligated to comply with the requirements of the following Laws and rules:

a. Asset (Money) Laundering Prevention Act, 2064 (and its latest amendments)
b. Asset (Money) Laundering Prevention Rules, 2081.

2.2 Regulatory Obligations

a. Unified Directives No. 19/082 issued by Nepal Rastra Bank,
b. "Guidelines for Suspicious Transactions Reporting & Suspicious Activity Reporting" issued by FIU effective from July 2021.
c. "Guidelines for Threshold Transactions Reporting" issued by FIU effective from January 2020.
d. Guideline on Targeted Financial Sanctions for Financial Institutions
e. ML/TF Risk Assessment Guidelines for Bank and Financial Institutions, 2022

2.3 International Standards (FATF Recommendations)

Being the member country of Asia Pacific Group on Money Laundering, Nepal has to implement FATF recommendations as required or applicable. FATF introduced forty recommendations in 1990, for the first time, as an initiative to combat money laundering and terrorist financing risks. In 1996 the recommendations were revised to reflect evolving money laundering typologies. These recommendations have been endorsed by more than 130 countries and are being applied by countries in varying extent as the international anti-money laundering standard. FATF reviews recommendations from time to time and publish recommendations with changes or enrichment. The latest publication of recommendations by FATF is on 2012. These recommendations have provided an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing throughout the world. The FATF recognizes that countries have diverse legal and financial systems and so all cannot implement identical measures to achieve the common objectives, especially over matters of detail. The recommendations therefore set minimum

standards for action for countries to implement the detail according to their particular circumstances and constitutional/legal frameworks. The recommendations cover all the, measures that national systems should have in place within their criminal justice and regulatory systems; the preventive measures to be taken by financial institutions and certain other businesses and professions; and the international co-operation.

The major themes on which FATF recommendations have been issued on 2012 relating to money laundering are as follows:

1. Assessing risks & applying a risk-based approach
2. National cooperation and coordination
3. Money laundering offence
4. Confiscation and Provisional measures
5. Terrorist financing offence
6. Targeted financial sanctions related to terrorism & terrorist financing
7. Targeted financial sanctions related to proliferation
8. Non-profit organizations
9. Financial institution secrecy laws
10. Customer due diligence
11. Record Keeping
12. Politically exposed persons
13. Correspondent banking
14. Money or value transfer services
15. New technologies
16. Wire transfers
17. Reliance on third parties
18. Internal controls and foreign branches and subsidiaries
19. Higher-risk countries
20. Reporting of suspicious transactions
21. Tipping-off and confidentiality
22. DNFBPs: Customer due diligence
23. DNFBPs: Other measures
24. Transparency and beneficial ownership of legal persons
25. Transparency and beneficial ownership of legal arrangements
26. Regulation and supervision of financial institutions
27. Powers of supervisors
28. Regulation and Supervisions of DNFBPs
29. Financial intelligence units

30. Responsibilities of law enforcement and investigative authorities
31. Powers of law enforcement and investigate authorities
32. Cash couriers
33. Statistics
34. Guidance and feedback
35. Sanctions
36. International instruments
37. Mutual legal assistance
38. Mutual legal assistance: freezing and confiscation
39. Extradition
40. Other forms of international cooperation

2.4 Regulatory Actions, Sanctions and Fines/Penalties:

NRB may take any or all of the following actions or sanctions against the Bank, its staffs, directors and officials for failing to comply with any provisions of the Act, Rules and Directive:

- to issue written reprimand warnings,
- to impose fines from one million to NRs fifty million,
- to impose full or partial restriction on the business or transaction,
- to suspend the registration or permission or license,
- to revoke the permission or license or registration
- Other appropriate sanctions

Details of the fines and penalties shall be governed by the provisions of NRB Unified Directive No. 19/082, Clause 21, as amended, revised, or replaced from time to time.

2.5 Not to be Liable for Providing Information:

- No staff or official of the bank is supposed to have violated the professional or financial norms prescribed under other prevailing laws if such act has been carried out in the course of discharging duties under the Asset (Money) Laundering Prevention Act up to the level of performance mandated under the Act.
- No criminal, civil, disciplinary or administrative action or sanction shall be taken against the bank or any of their official or staff who in good faith submit reports or provide report, document, information, notice or records in accordance with the provisions of Asset (Money) Laundering Prevention Act/ Rules and Directives as a breach of secrecy provision under prevailing laws or contractual, administrative or regulatory liability.

Chapter 3: Prevention of Money Laundering & Financing of Terrorism and Proliferation

This policy represents the strategic orientation and management policies for preventing risks related to money laundering and terrorist financing chosen autonomously by the bank. This policy also has set expectations, standards and behaviors to prevent ML/FT risks for the bank. Following are the policies taken by the bank:

3.1 Full adherence to laws and regulations

The bank is committed to full compliance with the money laundering laws and regulations applicable in the country.

3.2 Implementing evolving national and international best practices

The bank adopts policy of not only adhering country's legal and regulatory requirement, but also adopts international best practices to the extent reasonable and practicable to effectively manage ML/FT risks in the bank.

3.3 Use of Automated AML solution

It shall be the policy of the bank to make maximum use of technology and upgrade the systems and procedures in accordance with the upcoming challenges regarding ML/FT. Likewise, bank shall implement / use automated AML solutions across its network for effective KYC management, risk assessment, transaction monitoring etc.

3.4 Use of Online Platform for Customer Onboarding and KYC Process

In line with the Bank's Long Trem Strategy to achieve the innovator's stage in the Digital Adaption, bank shall develop/procure and use various online platforms for customer onboarding and KYC verification such as video based KYC platform, e-KYC platform, integration with government's data or other reliable public database as available such as Nagarik app.

3.5 Risk Appetite and Tolerance

The Bank shall pursue a zero tolerance policy on all matters related to AML/CFT/CFP compliance. The bank shall take action for resolving issues in high priority. Bank shall assess the ML/TF/PF risk on all the Bank's products including digital products.

3.6 Customer Acceptance

The bank will not accept any person/entities as its customer if the customer and beneficial owner of the customer cannot be identified, verified and thus bank is unable to have customer's risk profiling as required by the Act, Rules and Directive.

In case where the Customer Due Diligence of the existing customer cannot be completed or accepted as required by law and regulation, Bank shall discontinue the relationship with the customer. Bank shall endeavor to obtain the formal account closing application from the customer whereas in cases where customer cannot be contacted, Bank shall discontinue the relationship with the customer as per Para 16.7 of NRB Directive 19/082 with due approval from CEO or as delegated authority with support from **CRO/Head AML/CFT Compliance** or as delegated authority, **Chief Operating Officer/Head Central Operation** or as delegated authority and Chief Legal Officer or as delegated authority.

3.7 Risk Based Approach (RBA)

The RBA principals propose identification, assessment, understanding and mitigation of ML/FT/FP risk including explicit consideration to key risk factors such as customers, products/services, transactions, country, geographic areas and coverage of banking activities and delivery channel and with varying degrees of impact and levels of risk. It is a continuous process, carried out with a dynamic approach.

The bank shall adopt Risk Based Approach (RBA) in managing its ML/FT/FP risks and assess potential ML/FT/FP risks and implement measures and controls commensurate with the identified risk. The bank shall strengthen, make priorities and perform its activities to manage higher risks first and ensure that greatest risks receive the highest attention. RBA shall be adopted in all activities that are performed to prevent ML/FT/FP risks in the bank.

3.8 Risk Management via Three Lines of Defense

For the effective assessment, understanding, management and mitigation of ML/FT/FP risks, bank shall adopt three line of defense. Identification and analysis of ML/FT/FP risks and effective implementation of policies and procedures to encounter the identified risk is the feature of effective and sound risk management. The line of defense shall act as safeguard of the bank during the adversities and shall be liable for effective risk management.

a. **First line of defense:**
   Business units and departments shall function as a first line of defense to prevent ML/FT/FP risks. Business shall promote AML/CFT/CFP principles while doing

business. Businesses shall own and manage the ML/FT/FP risks arising from the business. Persons involved in business functions must ensure that appropriate controls are in place and operating effectively. Business units shall make an appropriate risk assessment before introducing any product or service and implement required mitigations. It shall be the responsibility of compliance department to assist business units/departments in this process.

b. Second line of defense:

Compliance Department shall function as a second line of defense to prevent ML/FT/FP risks in the bank. The Compliance Department shall monitor overall legal, regulatory and internal compliance of policies, procedures and guidelines. It shall also provide businesses with regulatory compliance expertise and guidance, set standards and trainings for businesses to manage and oversee ML/FT/FP risks.

c. Third line of defense

This shall be performed by internal audit. The internal audit shall review the activities of the first two lines of defense with the purpose to ensure that legislation, regulations and internal policies are processed effectively.

3.9 Commitment of Senior Management

Senior management of the bank is fully committed to establishing appropriate policies, procedures and controls for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. Senior management also commits to ensure that ML/FT/FP risks are understood and appropriately mitigated in the bank. It shall also ensure that effectiveness of controls shall be regularly reviewed. The senior management of the bank shall promote compliance as a core value and culture of the bank and the bank will not enter into, or maintain, business relationships that are associated with excessive ML/FT/FP risks which cannot be mitigated effectively.

Composition of AML/CFT Oversight Committee

The Bank has established an AML/CFT Oversight Committee to ensure effective implementation of the Bank's AML/CFT/CFP framework and to provide management level oversight. The Committee meeting shall be held on every two months period or more frequently (as per requirement).

The size (number of members) of committee shall depend on the business mix and organizational complexity. Unless otherwise decided by the Board of Directors from time to time, the composition of the Committee shall be constituted as follows:

- Deputy CEO shall be the coordinator
- Chief Risk Officer shall be the member
- Chief Operating Officer shall be the member
- AML Implementing Officer shall be the member secretary of the committee.

Coordinator and Other members shall be as prescribed by the Chief Executive Officer (as deemed necessary) taking into consideration of business requirements, regulatory expectations and organizational structure.

AML/CFT Oversight Committee may invite officials to discuss on specific topic as per requirements. The Terms of Reference (TOR) of this committee shall be defined by the Chief Executive Officer from time to time.

3.10 Prohibited customers and transactions

It shall be the policy of the bank not to do the followings:

1. Establish or maintain dummy accounts, anonymous accounts, or accounts in fictitious names or transact in such accounts or cause to do so;
2. Maintain relationship with shell Banks or other banks which deals with shell bank or shell entities;
3. Establish or continue business relationship or conduct transaction with the customser who cannot provide documents, information and details required for the customer identification and verification as required by law and regulation.

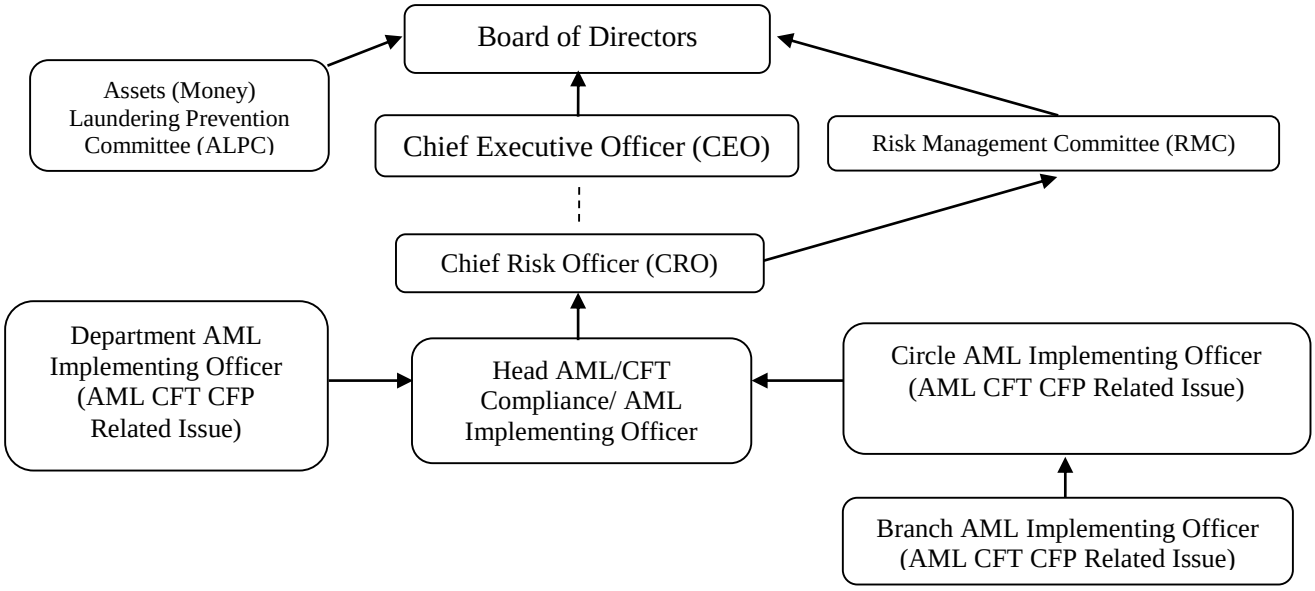
   Exception Note: In case customer submits valid reason for inability of presenting some document or information and bank becomes satisfied with the reason, relationship can be established and transaction can be done with maintaining record of the information of non-existence of document/information along with customer's declaration to submit the document within 3 days' time. However, in case of High Risk Accounts, relationship can only be established after obtaining at least identity documents of account holder and beneficial owner as applicable;
4. Customers who provide conflicting Documents, information and details;
5. Maintain relationship with persons and entities sanctioned by major sanction authorities such as Financial Action Task Force, United Nations, Office of Foreign Assets Control- United States, Her Majesty's Treasury-United Kingdom, European Union (EU) and Ministry of Home Affairs of Nepal;
6. Payment orders with an inaccurate representation of the person placing the order;

7. Acceptance of payment remittances from other banks without indication of the name or account number of the beneficiary;
8. Use of accounts maintained by the bank for technical reasons, such as sundries accounts or transit account, or employees' accounts to filter or conceal customer transactions;
9. Maintaining accounts under pseudonyms that are not readily identifiable;
10. Opening Accounts without name or with notional name;
11. Acceptances and documentation of collateral that do not corroborate with the actual economic situation or documentation of fictitious collateral for credit granted on trust;
12. Payable through Accounts;
13. Providing Downstream Correspondent Banking;
14. Maintain relationship with shell entities or other entities or individuals which deals with shell bank or shell entities.
15. Blacklisted individual, firm, company and organization

    Exception Note: The restriction shall not be applicable for onboarding the accounts or conducting the specified transactions as per the provision of NRB Directions. Details to be guided by the procedural guidelines formed under this policy.
16. Maintain relationship with Customer involved in business of Arms, Defense, Military or Atomic Power.
17. Maintain relationship with Customer involved Unregulated Charities;
18. Maintain relationship with Customer involved in illegal businesses such as virtual currencies, Illegal drugs, gambling, red light business / adult entertainments.

3.11 Governance, Oversight, Structure and Reporting

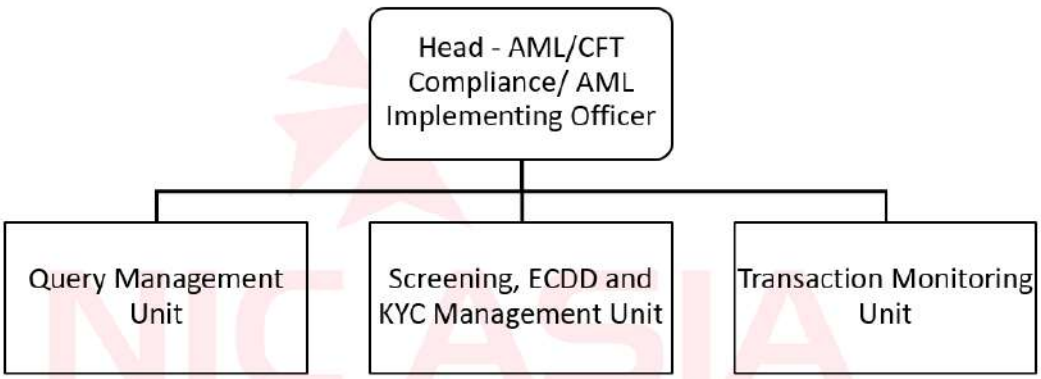
In order to perform effective management of ML/FT/FP risks, the board and senior management of the bank shall provide governance and oversight of the adequacy and effectiveness of management of ML/FT/FP risks. They will also ensure that AML/CFT/CFP programs are aligned with relevant legal and regulatory requirement and AML/CFT/CFP strategy is optimally aligned with international best practices. The AML/CFT/CFP management of the bank shall be carried out on the structure as depicted in following organigram:



a. **Compliance Department**

The Bank shall have a Compliance Department under the purview of Head AML/CFT Compliance / AML Implementing Officer who will look after the overall compliance of AML/CFT/CFP policies and procedures, with direct reporting to Chief Risk Officer and indirect reporting to Board Level "Assets (Money) Laundering Prevention Committee".

The Compliance Department shall be carried out on the structure as depicted in following Organigram:



The Terms of the reference of the units under compliance department is listed on Annexure- I

b. Appointment of AML Implementing Officer

The Bank shall appoint AML Implementing officer to function as a focal point for implementation of this policy, and guidelines formulated to execute this policy, Acts, rules and regulations, and directives from regulatory body regarding Anti-Money Laundering and Combating Financing of Terrorism. Further, AML Implementing Officer shall act as member secretary of Assets (Money) Laundering Prevention Committee (ALPC).

The AML Implementing Officer of the Bank shall put forth quarterly update on the AML/CFT/CFP and KYC compliance of the Bank for deliberation at Assets (Money) Laundering Prevention Committee (ALPC) and the Board of Directors of the Bank.

AML Implementing Officer shall be responsible for the general oversight of the Bank's Policy for Prevention of Money Laundering & Combating Financing of Terrorism, effectiveness of the control, monitoring and reporting procedures and to establish and maintain adequate arrangements for training on prevention of money laundering and financing of terrorism. She/he shall also be responsible for ensuring prompt response to queries from internal/external authorities and for assisting Business Units/Branches in meeting their AML/CFT/CFP related responsibilities.

In addition to above, other responsibilities of AML implementing Officer shall be as follows:

a) To perform and cause to perform activities as required to be followed by the reporting institution under Assets (Money) Laundering Prevention Act and Rules, directive, order circular issued under the said Act as well as other related statutes.
b) To identify the customer as required by the legal instruments including the Asset (Money) Laundering Prevention Act and rules, directives, order circular issued under the said Act.
c) To maintain and cause to maintain updated record of Customer Due Diligence information as per point no. (b)
d) To properly maintain the record of transaction exceeding the threshold and suspected transactions
e) To submit information of transactions as per point no. (d) to Financial Intelligence Unit within the stipulated time .

The obligations of the AML Implementing Officer are as follows:

a) Function as focal point to perform tasks in accordance with the Act, Rules and the Directives,
b) Cause to maintain the secure record of the transactions,
c) Provide information about suspicious or other necessary transaction to the Financial Intelligence Unit through letter or electronic means of communication like fax, email, etc.
d) Provide information about transaction of the branch offices to the Financial Intelligence Unit in a regular basis.

In order to carry out the duties assigned, AML implementing officer may request information/documents to any staff in the bank and it shall be the responsibility of concerned staff to provide information/document as requested. The details of AML implementing officer like name, address, qualification, contact number, email etc. shall be furnished to FIU and information regarding the change in AML implementing officer and details thereof shall also be notified to FIU.

While appointing AML Implementing Officer Bank shall ensure that she/he shall not be immediate family member/ close relative of officials and top level management of related regulatory authority. Further, Bank shall make necessary arrangement for filing STR/SARs vide alternative Compliance Officer in case of suspicious activity/transaction related to immediate family members/ close relatives of Bank's AML Implementing Officer and maintain full confidentiality for the same.

c. Circle / Branch AML Implementing Officer

For effective management of ML/FT risks in the bank, at each branch, Branch AML Implementing officer shall be appointed similarly, at each Circle, Circle AML Implementing Officer shall also be appointed. Operation In Charge and Circle Head shall mandatorily be Branch AML Implementing Officer and Circle AML Implementing Officer respectively while the other staff of the branch and circle may be appointed as alternate Branch AML Implementing Officer or Circle AML Implementing Officer on the need basis by Chief Executive Officer upon the recommendation of AML Implementing Officer. The Branch AML Implementing Officer shall have a direct reporting line to Circle AML Implementing Officer and Circle AML Implementing Officer shall have a direct reporting to AML Implementing Officer for AML/CFT/CFP related issues. For other functions, they shall report as per their job description.

d. Departmental AML Implementing Officer

For effective management of ML/FT/FP risks in the bank, at each department, departmental AML Implementing officer shall be appointed. Departmental AML Implementing Officers are head of the department or his alternate assigned for effective management of Money Laundering and Financing of Terrorism/ Proliferation risks in the department under their supervision with direct reporting to the AML Implementing Officer for AML/CFT/CFP related issues.

e. Compliance Auditor

Bank shall appoint Compliance Auditor listed on the website of Financial Information Unit (Nepal). Bank shall appoint Compliance Auditor listed on the website of Financial Information Unit (Nepal). Such personnel shall be selected six months prior to completion of financial year and the information about the same shall be provided to Board/ALPC/Annual General Meeting.

The Compliance Audit Report shall be submitted to NRB within six months from the end of the Financial Year after conducting audit on the following matters:

a. Regarding the necessary policy, institutional, technical and control structures and their appropriateness,
b. Regarding the establishment and effectiveness of risk assessment, risk-based systems in accordance with the institutional scope,
c. Regarding the implementation of the risk based annual plan, reporting system and monitoring,
d. Identifying and improving weaknesses in risk assessment, policy, institutional technical, control, implementation structure and effectiveness,
e. Related to other matters determined by the regulatory body.

The other provisions related to appointment, qualification, roles, responsibilities and rights of the Compliance Auditor shall be as provided in the relevant Act, Rules and Directives/ Guidelines issued by NRB from time to time.

The bank shall conduct independent review of its risk assessment one month prior to completion of fiscal year. Such assessment shall be carried out either by Compliance Auditor or Risk Assessment related Expert before conducting Compliance Audit of the Bank. The other provisions related to such risk assessment related expert shall be as provided in the relevant Act, Rules and Directives/ Guidelines issued by NRB from time to time.

3.12 Development and implementation of procedural guideline

The Bank has developed and implemented "Integrated Guideline on AML/CFT/CFP and KYC Management" which interprets/implements this policy and sets standards for each business in line with the law, regulations and regulatory guidelines. Compliance with the guideline shall be monitored regularly by the Compliance Department.

3.13 Know your Customer (KYC) and Customer Due Diligence

The Bank is aware that availability of sufficient customer information underpins all other AML procedures and should be seen as a critical element in the effective management of ML risks. The details regarding customer acceptance shall be incorporated in specific guideline which lays down the criteria for the acceptance of customers. The guideline would form an integral part of the bank's AML Policy. KYC and Customer Due Diligence shall be guided by Know Your Customer and Due Diligence Policy and the amendment thereto.

3.14 Due Diligence of Employees

Employees are also emerging as the great source of ML/FT/PF risks for the bank. Therefore, the bank will arrange adequate screening mechanism as an integral part of recruitment/hiring process of staffs. The Human Resource Management Department of the bank shall conduct due diligence of employees before appointing them as staff and during service period on annual basis. Due diligence of employees shall be performed as per procedural guideline framed under this policy.

3.15 Due Diligence of Vendors, Service Providers, Consultants and Business Partners

Vendors, service providers, business partners, consultants, etc. also can pose significant reputational risk to the bank if they are found involved in money laundering and terrorist activities and/or use the relationship for money laundering or terrorist/proliferation financing activities. Therefore, the Bank shall not establish relationship with such parties if they are found involved in money laundering or terrorist/proliferation financing before establishing a relationship. The bank shall conduct regular due diligence of these parties and additional risk management tools will be used, if risk is identified. Similarly, the bank shall report identified suspicious activities found to FIU as its regulatory liability. The execution of due diligence of such parties shall be done as per related procedural guideline. Due diligence of vendors, service providers shall be performed as per procedural guideline framed under this policy.

3.16 Due Diligence of Correspondent Banking Relationships

Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Large international banks typically act as correspondents for several other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international transfers of funds, cheque clearing, and foreign exchange services. It would be the bank's policy to obtain sufficient information about correspondent banks to understand the nature of their business & activities. When considering entering into a cross-border correspondent banking relationship, the bank shall carry out due diligence measures i.e. ownership, management structure, major business activities, customers, purpose of the account, location, etc. In addition, research will be conducted from publicly available information on the correspondent bank's business activities, their reputation, and quality of supervision and whether the institution has been subject to a money laundering or terrorist financing investigation or any regulatory action. Due Diligence of Correspondent Banking Relationship shall be performed as per the procedural guidelines framed under this policy.

3.17 Recognition and Reporting of Suspicious Activities and Transactions

Make prompt reports of suspicious transactions, or proposed transactions or any other money laundering and financing of terrorism/proliferation issues through the internal channels as prescribed by the Bank from time to time to the relevant authorities as required by statutory regulations. Guideline for Detecting Suspicious Transaction issued by FIU states that "Suspicious Transaction Reports (STRs) include detailed information about transactions that are or appear to be suspicious. The goal of STRs filings is to help the Financial Intelligence Unit (FIU) of Nepal identify individuals groups and organizations involved in fraud, terrorist financing, money laundering, and other crimes. The purpose of a STR is to report known or suspected violations of law or suspicious activity observed by financial institutions subject to the provision related Asset (Money) Laundering Prevention Act, 2008 (and its latest amendments).

FIU requires an STR to be filed by a financial Institution when the financial institution suspects insider abuse by an employee, violations of law or more that involve potential money laundering or violation of existing AML/CFT/CFP law, or when a financial institution knows that a customer is operating as an unlicensed money services business.

The general characteristics of suspicious financial transactions as mentioned in Guidelines for Detecting Suspicious Transaction issued by Financial Intelligence Unit (FIU) are as follows:

1. Transactions having unclear economical and business target,
2. Transaction conducted in relatively large amount cash and/or conducted repeatedly and unnaturally.
3. Transaction conducted differently from that of usually and normally conducted by the relevant customer.
4. Huge, complex and unusual transaction.

Any transaction which, based on the available information (provided by customer or from other source), reasonably appears not to be from a legitimate source or appears to be used for money laundering & financing of terrorism/proliferation shall be refused.

Reports of suspicious transactions, or proposed transactions, shall be furnished, through the appropriate internal channels and, where required by regulatory guidelines, to the relevant external authorities. Full cooperation shall be extended for any lawful request made by government agencies during their investigations into money laundering without "tipping-off" the customer.

No information of customer collected through CDD shall be provided or disclosed in any type of conditions by any ways to none, except to the agency, organization or official legally mandated to receive such information. Detailed procedure for reporting of suspicious transactions shall be as described in the Procedural Guidelines framed under this Policy.
There shall be clear documented procedurals in place to enable any member of staff to report knowledge or suspicion of money laundering as soon as possible. The process must include appropriate procedures to allow for the escalation of reports to senior management, and where appropriate, disclosure to external authorities.
Internal reporting procedures may allow for staff to consult with line management, who may wish to comment on any proposed report before escalating a report to the management. However, the procedures must allow all staff to make a report directly to the management.

Copies of disclosures made to the authorities must be retained, together with a record of any enquires undertaken to support the report. Similarly, a record of the reasons for non-disclosure to the authorities of any internal reports must be retained to demonstrate that at the time there was insufficient suspicion to justify making such a disclosure.
Following the making of a disclosure, full and prompt co-operative must be given to all legal requests to provide further information to the authorities to assist their investigations into

money laundering. Under no circumstances should a customer be informed that a disclosure has been made, as such notification could prejudice an existing or potential investigation by the authorities.

Where, following a disclosure, the authorities allow the relationship to continue and management decisions to retain the account, subsequent activity must be subject to particularly close vigilance. Any new activity that adds to the original suspicion must be disclosed.

3.18 Risk Assessment

The Bank shall carry out risk assessment of threats and vulnerabilities related to money laundering and terrorism financing as required by the Assets (Money) Laundering Prevention Act 2064 and its subsequent amendments, NRB Unified Directive 19/082 and its subsequent amendments, Assets(Money) Laundering Prevention Rules 2081 and ML/TF Risk Assessment Guidelines for Bank & Financial Institutions issued by Nepal Rastra Bank. Bank shall submit annual risk assessment report with in first quarter from the end of financial year to Money Laundering Prevention Supervision Division, Nepal Rastra Bank and FIU Nepal. The risk assessment helps to identify and assess threats and vulnerabilities in the Bank's operating environment pertaining to Money Laundering and Terrorism/ Proliferation Financing and thereby the risks the Bank is likely to encounter.

a. The bank shall identify and assess the money laundering or terrorist financing risks before launch of new product, service, business practice, use of new technology and initiating non-face to face customer services or transaction.

b. The risk assessment shall include risks coming out from following sources:

    - ML/FT/FP risks in customer (nature and type),
    - ML/FT/FP risks in Transactions
    - ML/FT/FP risks in products,
    - ML/FT/FP risks in services,
    - ML/FT/FP risks in delivery methods
    - ML/FT/FP risks in geographical areas

c. While conducting risk assessment, the bank shall consider the findings of national and regulatory risk assessment.

d. The risk assessment shall be carried out annually and the risk assessment report shall be presented to the board via Assets (Money) Laundering Prevention Committee. The Annual Risk Assessment report shall also be submitted to Money

Laundering Prevention Supervision Division and Financial Intelligence Unit, Nepal Rastra Bank as required by Unified Directives 19/082 and amendments there to.

e. The bank shall undertake customer due diligence measures in accordance with the level of risks as identified by risk assessment and shall establish appropriate policy, procedural and risk management measures, to manage and mitigate such risks and update such measures.

f. Country Risk, Geographical risk and coverage.

3.18.1 Risk Assessment Framework

Bank shall prepare framework of AML/CFT/CFP Risk Assessment Framework which shall outline the procedures, methods and provide objective basis for final AML/CFT/CFP Risk Assessment of the bank. The Framework shall be submitted to Money Laundering Prevention Supervision Division of NRB.

3.18.2 Annual Review of Policies & Guidelines of the Bank

The bank shall annually update the policy/guidelines, risk based annual plan/ procedures to address the risk arising from changes in AML/CFT related legislations and regulations, latest changes in business methods/technology and changes in means/trends of committing money laundering/terrorist financing/ proliferation financing related crimes and report the same to NRB via SIS.

3.18.3 Risk Based Plan

Annual Risk based plan shall be prepared during first quarter of each fiscal year. The Risk Based plan shall lay down the detailed activities mandated to be carried out during the Fiscal Year by the Compliance Department of the Bank. The plan shall also entail the scope, coverage and resources, and activity of Compliance Department over a defined period. The bank may change the risk based annual plan on the basis of Annual Risk Assessment Report submitted thereon.

3.18.4 Annual Report of Task/Activities on AML/CFT/CFP

Compliance Department shall prepare an annual report of tasks carried out during a financial year on AML/CFT/CFP. The report shall highlight key activities, achievements and challenges faced by the Bank in ensuring compliance with regulations and global standards to prevent financial crimes during a financial year. The report shall serve as a critical document for regulators and stakeholders to assess the effectiveness of the Bank's effort

in mitigating financial crime. The report shall be submitted within two months after completion of each fiscal year to NRB vide its SIS system.

3.19 Transaction and Account Surveillance

Effective ongoing monitoring is vital for understanding of customer's activities and is an integral part of effective AML/CFT/CFP system. It helps to know the customers and to detect unusual or suspicious activities. In line with the regulatory requirements, bank shall adopt the policy of monitoring the accounts in the mentioned time frame as per the risk category of the customer.

The business relationship with a customer should be continuously monitored by:

- Reviewing from time to time, documents, data and information relating to the customer to ensure that they are up-to-date and relevant,
- Monitoring the activities (including cash and non-cash transactions) of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds, An unusual transaction may be in the form of activity that is inconsistent with the expected pattern for that customer, or with the normal business activities for the type of product or services that is being delivered and
- Identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/FT threats
- In case the proceeds/payments related to legal entity/arrangements are executed via personal account or otherwise as permitted by prevailing law in force in case the personal saving account is being used as a medium for carrying out business transactions the same shall be reported as suspicious transaction to FIU.

Priority shall be given to the major threats/ key vulnerable sectors identified in National Risk Assessment Report and APG mutual evaluation report during identification, transaction monitoring, KYC updates and ongoing monitoring.

(Note: National Risk Assessment Report and APG mutual evaluation report has highlighted corruption, tax evasion, human trafficking and hundi as major financial threats while Casino/Internet Casinos, dealers in precious metals/stones, remittance providers. real estate business, cooperatives as key vulnerable sectors.)

Ongoing monitoring of the business relationship should be conducted on a risk sensitive and appropriate basis.

Business Units and Branches must monitor compliance with the policy, standards, legal and regulatory requirements, procedures and controls through the tools as prescribed

through separate Guidelines/Manuals and the results of such monitoring shall be shared with the AML Implementing Officer. These results shall form the basis of a continuing process to improve the overall anti-money laundering & combating financing of terrorism control process including training requirements.

3.20 Design and Implement Reviews, Checks and Control

The Bank shall have adequate procedures and processes to ensure effective checks, reviews and controls in executing AML/CFT/CFP and KYC Compliance. Such reviews, checks and controls shall be designed to help the businesses meet their responsibilities in relation to the prevention of money laundering & financing of terrorism. These standards shall be primarily based on the relevant regulatory/statutory guidelines and the best practices on prevention of money laundering. These checks, reviews and controls shall be regularly updated to identify and mitigate continuously evolving risks. The Bank shall implement checks, reviews, controls in all its functions, products/services, processes, etc. The operating manuals, product paper guidelines, procedural guidelines, standard operating procedures, etc. shall incorporate related checks and controls.

3.21 Sanction Screening

The Bank shall not establish any kind of relationship (customer, employee, vendor, consultant, service provider, business partner, etc.) with sanctioned individuals/entities listed in the Sanction List published by UN, OFAC, HMT-UK, EU. Bank shall also consider the information of the sanctioned list published on official website of Ministry of Home Affairs for as well as the UN list for screening.

The detailed procedure for sanction list screening and reporting shall be as per the Integrated Guidelines on AML CFT CFP and KYC framed under this policy and as prescribed by NRB from time to time.

3.22 Employee Education and Training programs

a. Compliance with Statutory and regulatory requirements:

The bank is responsible to fully comply the entire statutory and regulatory requirements relating to training and awareness of the employees.

b. Risk Based Approach in conducting training and awareness program

The bank shall adopt a risk based approach while conducting training programs. The bank shall aim, strengthen, priorities, and conduct trainings in line with the result of bank's risk assessment as well as emerging ML/FT/FP risks identified by the bank.

c. Education and Training programs

The bank shall conduct specific role based training programs on need basis relating to ML/FT/FP risks and their management as its regular activity. It shall be the bank's policy to provide basic awareness training to all the staffs and other job/responsibility specific trainings on core risk functions/areas i.e. trade finance, credit, customer service, compliance, etc. Such programs may include seminars, workshops, discussions, trainings etc. The bank shall conduct such programs on a regular basis. All education and training programs shall be conducted as per the guideline framed under this policy. The Human Resource Department shall coordinate with Compliance Department to assess Training and Development needs of the Bank's staff with respect to the AML/CFT/CFP at least annually. Based on the feedback/inputs provided by Compliance Department, Training calendar/plan on AML/CFT/CFP shall be prepared by the Human Resource Department for upcoming fiscal year.

d. Adequacy and effectiveness of Training and awareness programs

The AML Implementing officer shall determine the adequacy and effectiveness of the programs. The bank shall take the Skill Assessment Test (SAT) on trainings provided to the staff to ensure effectiveness of the training programs.

e. Record Retention

The bank shall maintain the record of all education and training programs conducted by the bank. Such record is kept in a way that it is capable of disclosing name, date, major issues discussed/covered, participants, etc.

3.23 Customer Education

The cooperation of the customers is the significant factor for the bank to achieve its AML/CFT/CFP goals. In order to get utmost cooperation of the customers, the bank shall conduct customer education programs to make them knowledgeable regarding seriousness of money laundering and terrorist financing risks to the bank and ultimately to its customers, why bank asks for various kinds of information from its customers and their vitality for creating a safer bank and so on.

It is crucial to be aware of the potential risks and legal considerations associated with commingling or mixing business and personal funds. Thus Branch manager/Branch In-charge/ Experience manager to ensure creation of awareness among customers regarding the importance of avoiding business transactions in personal accounts and promoting the use of dedicated business accounts.

3.24 Cooperation to lawful enforcement agencies

Co-operate with any lawful request for information made by authorized Government Agencies/Statutory Bodies during their investigations into money laundering and financing of terrorism.

Support Government Statutory Bodies and law enforcement agencies in their efforts to combat the use of the financial system for the laundering of the proceeds of crime or the movement of funds for criminal purposes. Similarly, bank shall ensure that all the instructions and queries received from various enforcement agencies shall be enacted upon the stipulated time. The query handling functions of the bank shall be guided by the procedural guidelines formed under this policy.

3.25 Sharing of information between or among entity or groups

Bank shall aid in exchange of information between or among entities or groups in relation to facilitation of customer identification and authentication from the third party, wire transfer and cross-border correspondent bank in line section 7T of Asset (Money) Laundering Prevention Act, 2064.

3.26 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.

As per provision of ALPA, information shall not be disclosed even in judicial proceedings that discloses or may disclose the introduction of official or staff.

ALPA has allowed NRB to fine up to ten million rupees fine to the bank if tipping off is done. Similarly, the bank is to take departmental action to its staff as per Staff Service by law.

3.27 Independent Testing

The AML/CFT/CFP framework of the Bank shall be tested and reviewed by independent function such as internal audit, statutory audit etc. Such testing shall be conducted at least once every year.

3.28 Safe Keeping of customer's transaction record

The Act requires to maintain the secured record, pertaining to transactions made beyond threshold limit prescribed by Nepal Rastra Bank at a single or in a series of transactions by a person and any other transaction which appears to be suspicious or transacted with the motive of asset laundering, at least for a period of five years from the date of such transaction. However, the bank shall adopt policy of maintaining full and secured record of activities performed in the process of execution of this policy for a minimum period of seven years even after the termination of relationship with the customer. The detail of documents, information, methods of safe keeping, person wise duties, handling procedure, etc. shall be performed as per the functional guidelines framed under this policy.

In order to strengthen the customer due diligence and recording of customers KYC information, all the KYC information obtained subsequently by Bank shall be mandatorily updated in related field of Core Banking System (CBS) by concerned staff of the branches.

3.29 Code of conduct of Board of Directors

As an apex body of the Bank and to set the tone of the top, Board of Director of the Bank shall adhere to the following code of conduct relating to the prevention of money laundering and combating financing terrorism:

- No any board of director of the bank 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 board of director of the bank shall, by any means, support to money laundering or terrorist financing directly or indirectly, in part or in whole, unlawfully and willingly
- No any board of director of the bank shall inform/share/talk/disclose/warn, by any means, to any unauthorized persons about the bank's policies and procedures relating ML/FT/FP risk management.
- No any board of director of the bank shall inform/share/talk/disclose/warn, by any means, to any unauthorized persons about bank's consideration investigation initiated by bank or other competent authorities regarding any of its customers or other parties.

- No any board of director of the Bank shall tip off or inform/ share / disclose / warn, by any means, to any of the Bank's customer.
- Board of Director shall extend full cooperation to the legal and regulating bodies during their investigation in relation to ML/FT/FP activities.

3.30 Code of conduct of employees

As 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 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 shall, by any means, support to money laundering or terrorist financing directly or indirectly, in part or in whole, unlawfully and willingly
- No any staff of the bank shall inform/share/talk/disclose/warn, by any means, to any unauthorized persons about the bank's policies and procedures relating ML/FT/FP 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.
- No any staffs of the Bank shall tip off or inform/ share / disclose / warn, by any means, to any of the Bank's customer.
- 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/FP 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.

3.31 Speaking Up and Whistle Blowing

There shall be a speaking up mechanism instigated in the Bank such that any staff member who suspects that the Bank's code of conduct, prudent practice, and ethical standard is being/has been compromised contemplating or facilitating any act of Money Laundering /Terrorist Financing/ Proliferation Financing are allowed to escalate the case to senior management. The management shall provide adequate safeguards against victimization of whistle blower including the anonymity of the whistle blower.

3.32 Database Maintenance

The Bank shall maintain database of PEPs, sanction individual / entities, list of individual / entities involved in terrorism etc. to the extent possible depending upon the availability of such information. Sources of such information shall be the list maintained by foreign ministry / home ministry in their websites, list maintained by Nepal Rastra Bank, Financial Intelligence Unit, enforcement agencies, Nepal Banker's Association etc. The Bank may use the database maintained by world renowned agencies like Accuity Online Compliance, World Check and any other such database provider. Reliability of such database shall be ensured by the Bank itself. Further, in case of PEP database the trigger scenario shall be identified and changes thereto shall be updated at the earliest possible.

Bank may also rely on the information made available by government agencies and bodies or official website for customer identification and verification such as obtaining information on Beneficial Owner as per para 5, information of public company through website, PAN details through IRD website, verification of company account information through official website of Office of Company Registrar (OCR), etc.

3.33 Departmental Action

At each event of violation of the provisions of this policy, the Bank shall take departmental action against its staff under staff service by law, 2073.

Chapter 4: Implementation, Review, and Reinforcement Framework

4.1 Checks and Reviews/ Output Checking

Following checks and Reviews/ output checking mechanism has been set to ensure implementation of provision of Effective Board Oversight Policy of the Bank:

- Board Level Sub Committee shall review the implementation status of the directions and suggestions by Board during the subcommittee meetings.
- Audit Department shall check and review to ensure that the procedure under this policy are being properly followed, whether deviations observed has been duly endorsed by the competent authority as prescribed by this policy.
- Internal and External reporting shall be reviewed by Management, Board Level Sub Committees and should ensure the compliance framework as per the policy are being properly followed, and deviations observed has been duly endorsed to competent authority.
- Strategy Department shall review and amend the Policy on an annual basis as per provision of Corporate Governance Policy of the Bank.

4.2 Authority and Its Timeframe

Authorities required to implement the provision of this Policy shall be as provisioned in various Chapters/ Sections of this Policy which shall be valid up to next review/ amendment approval date or date of withdrawal of given authority whichever comes earlier.

4.3 Roles and Responsibilities

The Board of Directors is the apex and supreme authority of the Bank. It is responsible and accountable to frame and implement robust guidelines and frameworks for effective compliance with the laws of land and with the regulations and directives issued by the regulatory authorities. The illustrative but not exhaustive roles and responsibilities of the Board related to this Policy are as follows:

- The Board of Directors shall be responsible for approving the policies ensuring the appropriateness, sufficiency and effectiveness of the policies adopted by the bank based on the overall risk level of the bank on prevention of money laundering and financing of terrorism. Also, the board shall ensure that the Policy Framework is

comprehensive for key business and support functions, and establish a method for monitoring compliance of the same.

- The Board shall review the status of implementation of Assets (Money) Laundering Prevention Act, 2064 and (its latest amendment), Assets (Money) Laundering Prevention Rules, 2081, and the provisions contained in the Directives/Circulars issued by NRB related to AML/CFT/CFP at least on quarterly basis.
- The Board of Directors of the bank and financial institutions shall, at least on quarterly basis, discuss on the recommendation of Assets (Money) Laundering Prevention Committee on setting up and improving mechanisms to prevent customer's suspicious and abnormal transaction or money laundering and make necessary arrangement for this effect.
- The Board of Directors of the Bank shall effectively discharge its statutory responsibilities as elaborated hereinabove.
- The Board is authorized to issue appropriate instructions to the senior management regarding this Policy that it deems appropriate.
- Any amendments / cancellation or revision in this policy shall be at the sole discretion of the Board.

Assets (Money) Laundering Prevention Committee is the Board Level Committee which shall constantly monitor the nature of level of AML risk being taken by the Bank and how the risk relates to risk appetite and tolerance capacity of the Bank. The illustrative but not exhaustive roles and responsibilities of Assets (Money) Laundering Prevention Committee related to this Policy are as follows:

- The Committee should appraise the Board on adequacy and appropriateness of the current AML/CFT/CFP framework of the Bank and make suggestions and recommendations, as deemed appropriate, to the Board, for improving and strengthening existing AML/CFT/CFP framework of the Bank.
- The Committee should seek report on activities carried out by the compliance department relating to AML/CFT/CFP and discuss on the Assessment, Measurement, Monitoring and Control of various Risks relating to money laundering and financing of terrorism and make necessary recommendations to the Board, as appropriate.
- Recommend the BOD for the formulation of Policies and Structures in line with the provision of NRB Directives, Guidelines and Appropriate Practices for Management of risk relating to Money Laundering.

- The Committee should provide a quarterly report to the Board after due assessment of the activities carried out by the compliance department along with suggestion for improvement in the AML CFT and KYC practices of the bank.

Further, the Assets (Money) Laundering Prevention Committee shall perform other functions and responsibilities as prescribed under Point No. 7(5) of NRB Unified Directives No. 6/082, as amended or replaced from time to time.

Risk Management Committee is the Board level Committee which shall constantly monitor the nature of level of risk being taken by the Bank and how the risk relates to risk appetite and tolerance capacity of the Bank. The illustrative but not exhaustive roles and responsibilities of Risk Management Committee related to this Policy are as follows:

- Ensure that ML/TF/PF risks are appropriately identified, assessed, monitored and incorporated into the Bank's Risk Management Framework

Chief Executive Officer is the head of the management which shall be primarily responsible for the implementation and ensure 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:

- Circulate and implementation of the Policy approved by the Board.
- Carry out and manage the Bank’s activities in a manner consistent with the business strategy, risk appetite and other guideline provided by the board.
- The CEO shall ensure that the bank has all required procedural guideline in place to effectively achieve the objectives of this policy.
- The CEO shall promote compliance as a culture and consider AML/CFT/CFP compliance as a basic ethic of doing business.
- All the procedural guideline containing the controls, monitoring and reporting procedures will be approved by the CEO.
- The CEO shall also ensure that sufficient resources and required access to information, documents and staffs have been arranged to carry out compliance functions efficiently and effectively.
- To review on quarterly basis as to whether or not the provisions of Anti-Money Laundering Act, and rules, directive, order or policy formulated under such act are complied with.
- Other discretionary authorities shall be exercised as delegated in the Policy or by the Board from time to time.

Deputy Chief Executive Officer shall constantly monitor the nature of level of AML risk in the Bank. The illustrative but not exhaustive roles and responsibilities of Deputy Chief Executive Officer related to this Policy are as follows:

- Receive regular reports on the works performed by the Compliance Department.
- Monitor performance of compliance department on periodic basis.

ACEO are the officers or such designated officials assigned in order to achieve strategic goal in an effective and efficient manner. They are assigned with a high level strategic management role. The illustrative but not exhaustive role and responsibilities of ACEO of the Bank related to this policy are as follows:

- Achievements of strategic goals of the Bank as envisioned by Bank's Vision and Strategy complying the regulations relating to AML.
- Providing strategic oversight and guidance on the pertinent affairs across the Bank relating to AML/CFT/CFP and KYC.

CRO shall constantly monitor the nature of level of AML risk being taken by the Bank. The illustrative but not exhaustive roles and responsibilities of CRO related to this Policy are as follows:

- Receive regular reports on the works performed by the Compliance Department.
- Monitor performance of compliance department on periodic basis.
- Escalate the pertinent issue related to money laundering and combating of financing of terrorism/proliferation to the management as required.

Chief Operating Officer is the officer or such designated who shall be responsible for overall operations of the Bank. The illustrative but not exhaustive roles and responsibilities of Chief Operating Officer of the Bank related to this Policy are as follows:

- Chief Operating Officer shall be responsible for ensuring proper implementation of checks and control and monitoring and reporting procedures across the Bank relating to AML/CFP/CFP and KYC.

Information Technology Department shall be responsible for the managing core Banking system, ensuring security of information assets from internal and external threats,

responsible to automate in I-zone, ensuring reliable Management Information System designed to provide timely and forward- looking information as required by the compliance department and ensuring ready availability of the information to the management. The illustrative but not exhaustive role and responsibilities of Information Technology Department of the Bank related to this policy are as follows:

- Arrangement of necessary platform in Core Banking System as required by the compliance department to comply with the regulatory requirements.
- Provide IT support to the compliance department as and when required.
- Work in close coordination with Compliance Department for generating trigger and red flags.
- Work in close coordination with Compliance Department for creating robust Management Information System frameworks as and when required.
- Arrangement of necessary platform for proper management of KYC related information of the Bank's customer, employee, vendor etc. in the I-zone and CBS.

Data and AI Adaptation Department shall be responsible to provide timely data on KYC information of the Bank's customer, employee, vendor etc. and ensuring ready availability of the information to the management. The illustrative but not exhaustive role and responsibilities of Data and AI Adaptation Department of the Bank related to this policy are as follows:

- Work in close coordination with Compliance Department for providing KYC related data and information.
- Provide transaction related data requested by Compliance Department.
- Automate extraction of data and information of regular nature through BI links.
- Work in close coordination with Compliance Department for creating robust Management Information System frameworks as and when required.

Digital Innovation Department shall be transformation of business and organizational activities, processes, competencies and models to fully leverage the changes and opportunities of a mix of digital technologies and their accelerating impact across Bank in a strategic and prioritized way. The illustrative but not exhaustive role and responsibilities of Digital Innovation Department of the Bank related to this policy are as follows:

- Cross coordinate with related PSP/PSO for support required in transaction conducted through Digital payment channels.
- Providing Contra party details related to the digital transactions.

- Coordinate for automation of Contra party details related to the digital transactions at customer level.
- Handle application related issues if any.

Head of Central Operation Department means an officer or such designated official assigned to support Chief Operating Officer.

- The Head of Central Operation Department shall assist Chief Operating Officer for proper implementation of checks and control and monitoring and reporting procedures across the Bank relating to AML/CFT/CFP and KYC.

- Department/Business/Unit Heads shall be responsible, under the area of their control, for ensuring proper implementation of control, monitoring and reporting activities designed to prevent money laundering and terrorist financing.
- Responsible to reasonably assure that staffs under their control have required knowledge and are not involved in any money laundering and terrorist financing activities.

Audit Department shall be responsible for check and review effectiveness of this Policy. The illustrative but not exhaustive roles and responsibilities of 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 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 Bank 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 audit plan complying the provision of NRB.

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/CFP.

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

- Human Resource Management 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.
- Human Resource Management Department shall also ensure that due diligence of the employees is updated regularly (at least on annual basis) and record is maintained appropriately. AML screening also to be performed during the due diligence of employees.
- Assessment of adequate human resources requirement.
- Training to human resources in the area of AML/CFT/CFP on need basis.
- Conduct specific role based training programs on need basis relating to ML/FT/FP risks and their management as its regular activity.
- **Coordinate with the Compliance Department to identify annual AML/CFT/CPF training needs and prepare, schedule, and facilitate the implementation of the Bank's AML/CFT/CPF training program.**
- Human Resource Management Department shall obtain declaration from Head AML/CFT Compliance/AML Implementing Officer that she/he is not immediate family member of officials and top level management of related regulatory authority.

- It shall be the responsibility of every individual employee of the bank to remain vigilant to the possibility of money laundering/terrorist financing/proliferation financing risks through use of bank's products and services.
- Any staffs who come to know about the involvement of bank's staff or any of its customers in money laundering or terrorist activities must report to the higher management of the bank following standard procedure framed under this policy and shall be mandatory role of all staffs of the bank.

- All the staffs of the bank shall adhere code of conduct relating to prevention of money laundering and combating financing terrorism as specified in the clause no 3.30 of this policy.

Operation In Charge / Branch AML Implementing Officers are the officials assigned for effective management of Money Laundering and Financing of Terrorism risks in the branch level with direct reporting to the Circle AML Implementing Officer for AML/CFT/CFP related issues.

- Operation In Charge shall be responsible for ensuring proper implementation of control, and monitoring and reporting procedure across the branch under their control to prevent ML/FT/FP.
- Operation In Charge / Branch AML Implementing Officers shall act as focal point of contact for matters relating to AML/CFT/CFP.
- Liaison between Compliance Department and the Branch for AML/CFT/CFP related task/ activities.
- Responsible for executing the duties as required by various guidelines framed under this policy from time to time.
- Other major duties shall be as follow:
  - Customer Due Diligence (CDD) / Enhanced Customer Due Diligence (ECDD) related responsibility
  - Suspicious Transaction / Activity Reporting Responsibility
  - KYC Compliance Related Responsibility
  - Other roles and responsibilities of the Operation In Charge / Branch AML Implementing officers shall be covered in their job description.

Circle Head are the officials assigned for effective management of Money Laundering, Financing of Terrorism and proliferation financing risks in the province under their supervision with direct reporting to the AML Implementing Officer for AML/CFT/CFP related issues.

- The Circle Head shall be responsible and accountable for management of compliance risk in the circle under their supervisions.
- Achievements of strategic goals of the Bank as envisioned by Vision and Strategy complying the regulations relating to AML.
- Providing strategic oversight and guidance to the staffs under his / her supervision, on the pertinent affairs of the provinces.

- Circle Head shall act as focal point of contact for matters relating to AML/CFT/CFP.
- Liaison between Compliance Department and the Branch for AML/CFT/CFP related task/activities.
- Responsible for executing the duties as required by various guidelines framed under this policy from time to time.
- Providing AML/CFT/CFP related training to all the staffs under his / her supervision at least once a year.
- Other roles and responsibilities of the Circle Head shall be covered in their job description.

Departmental AML Implementing Officers are head of the department or his alternate assigned for effective management of Money Laundering, Financing of Terrorism and proliferation financing risks in the department under their supervision with direct reporting to the AML Implementing Officer for AML/CFT/CFP related issues.

- The Departmental AML Implementing Officer shall be responsible and accountable for management of KYC risk in the departments/units under their supervisions..
- Providing strategic oversight and guidance to the staffs under his / her supervision, on the pertinent affairs of the departments/units
- Departmental AML Implementing Officers shall act as focal point of contact for matters relating to AML/CFT/CFP & KYC.
- Liaison between Compliance Department for AML/CFT/CFP & KYC related task/activities.
- Responsible for executing the duties as required by various guidelines framed under this policy from time to time.
- Providing KYC related training to all the staffs under his / her supervision twice a year.
- Other roles and responsibilities of the Departmental AML Implementing officers shall be covered in their job description.

Head AML/CFT Compliance / AML Implementing Officer is the officials or such designated officials who shall act as focal point to perform tasks in accordance with the Act, these Rules and the Directives. The illustrative but not exhaustive roles and responsibilities of Head AML/CFT Compliance / AML Implementing Officer related to this Policy are as follows:

- AML Implementing Officer shall have the roles and responsibilities as specified in Assets (Money) Laundering prevention Act, Rules 2081 and Nepal Rastra Bank Directive No 19/082 AML Implementing Officer shall have all authorities mentioned hereinabove listed under authorities of compliance department.
- To ensure compliance with Assets (Money) laundering prevention Act, Assets (Money) Laundering Prevention Rules and Nepal Rastra Bank's Directive 19/082.It is to ensure that the bank does not cross the lines drawn by laws, rules and regulations.
- Devise efficient and effective AML risk management framework and recommend for its implementation to the senior management of the bank.
- Liaise with regulatory authority and enforcement authorities to carry out AML/CFT/CFP related cooperation and functions.
- Providing AML/CFT/CFP compliance related reports like suspicious transaction reports, threshold transactions reports, self-evaluation questionnaire, bank related data etc. to regulatory authority on a timely manner.
- Laise with Human Resource Department for providing trainings to the employees of the bank relating to AML/CFT/CFP and KYC and arranging AML/CFT related Skill Assessment Test (SAT) to check level of knowledge of the employees.
- Reporting to Senior Management, Assets (Money) Laundering Prevention Committee and Board regarding functioning of the compliance department.
- Cause to maintain secure record of transaction.

Any other responsibility as decided by Board and Assets (Money) Laundering Prevention Committee.

4.4 Transition Management

The Bank shall manage the transition related to the changes in this Policy as under:

- All the actions performed in accordance to the previously approved version of this policy shall be deemed to be performed in accordance to this version of the Policy.
- For transition management, implementation timeframe, if not specifically mentioned, should be as approved by DCEO or above.

Chapter 5: Miscellaneous

5.1 AML Policy for Subsidiary Companies of the Bank

Bank's subsidiary with substantial holding shall prepare and implement the AML/CFT/CFP Policy in line with the Assets (Money) Laundering Prevention Act, 2064 (with amendments); Assets (Money) Laundering Prevention Rules, 2081 and regulations as applicable from their regulators. The AML/CFT/CFP policy shall be approved by the Board of respective Subsidiary.

NIC ASIA Bank, including its substantial subsidiary (the "Group"), is fully committed to adhere to the Country's AML/CFT/CFP laws and regulations and Internal Standard as applicable. The Group AML/CFT/CFP Policy is prepared to ensure the standardize AML/CFT /CFP compliance that are very crucial. AML/CFT/CFP related Policy Paper prepared by respective subsidiaries prepared shall be in line with this group policy. Group policy may be more stringent that what is permitted by law and regulation.

1. **Group Sanction Policy:** Group adopts the policy of not entering into any business or transaction that either directly or indirectly involves or is for the benefit of any parties listed as target or subject of sanction by Ministry of Home Affairs of Nepal, United Nation (UN), United Kingdom (UK), the European Union (EU).

   The group shall neither maintain its presence nor execute any transactions in the below sanctioned geographies except otherwise mentioned specifically:

   a. Iran
   b. North Korea
   c. Myanmar (flow of fund for humanitarian assistant, legitimate NPO activity and remittance shall be allowed)

2. **Customer Acceptance Policy**: Group shall not maintain any business relationship with the following:

   - Establish or maintain dummy accounts, anonymous accounts, or accounts in fictitious names or transact in such accounts or cause to do so;
   - Maintaining accounts under pseudonyms that are not readily identifiable or numbered account;
   - Maintain relationship with shell banks & entities or other banks, entities and individual which deals with shell bank or shell entities;

- ❖ Establish an account or continue business relationship or conduct transaction with the customer who cannot provide documents, information and details required for the customer identification and verification as required by law and regulation.
- ❖ Customers who provide conflicting documents, information and details;
- ❖ Maintain relationship with customer involved in business of Arms, Defense, Military or Atomic Power.
- ❖ Maintain relationship with customer involved in unregulated charities;
- ❖ Maintain relationship with customer involved in illegal businesses such as virtual currencies, Illegal drugs, gambling, red light business / adult entertainments.

3. **Customer Due Diligence Policy:** Group companies shall adapt customer due diligence as per the regulation of related regulatory body as applicable. In case of customer posing higher risk, enhanced due diligence shall be applicable.

4. **Employee Capacity Development Policy:** Group shall ensure that AML/CFT/CFP related awareness program are conducted on annual basis and covers all the staffs.

5. **Record Management Policy:** Group shall ensure that the Customer Due Diligence related document are kept safely for at least five years from date of end of business relationship and all the transaction document for at least five years. The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

6. **Internal Audit:** Group shall ensure that the Internal Audit function or any other independent function reviews the AML/CFT/CFP and KYC framework at least once every year.

The group policy shall be communicated to all the AML Implementing Officers of the group companies for their acceptance.

5.2 Reporting Requirement to NRB and Regulatory Authority

Following report related to AML CFT and KYC should be submitted to Nepal Rastra Bank by the Bank within the time line;

Report	Period	Due Date/ Time Limit	Authority/ Submission through	Primary Responsibility	Regulation
Suspicious Transaction Report (STR) /Suspicious Activity Report(SAR)	-	Immediately	Financial Intelligence Unit, NRB through goAML	Compliance	NRB Directive 19/082 Para 16
Threshold Transaction Report (TTR)	-	Within 15 days from the date of transaction	Financial Intelligence Unit , NRB through goAML	Compliance	NRB Directive 19/082 Para 15
Card Block Report	Monthly	Within15 days of Month End	Foreign Exchange Management Department, NRB	Compliance	Point 20 Sub-point 6 (Nga-3) of Unified Directive issued by Foreign Exchange Management Department
Quarterly Risk Assessment Report (ANUSUCHI-19.2)	Quarterly	Within 15 days of Quarter End	Money Laundering Prevention Supervision Division, NRB & Financial Intelligence Unit through email (fiupolicy@nrb.org.np)	Compliance	NRB Directive 19/082 Para 4
Bank Self-Assessment Questionnaire on AML/CFT Risk Management	Annual	Within 7 days of Year End	NRB Bank Supervision Department through NRB reporting website in given format	Compliance	NRB Unified Directive ANUSUCHI 19.2
AML/CFT Risk Assessment Report	Annual	Within First Quarter End	Money Laundering Prevention Supervision Division, NRB & Financial Intelligence Unit through email	Compliance	NRB Directive 19/082 Point 9 (7)

Report	Period	Due Date/ Time Limit	Authority/ Submission through	Primary Responsibility	Regulation
			(fiupolicy@nrb.org.np)		
AML CFT Reporting Format (Off-site data collection)	Semi Annual	Within 7 days of Half Year End	Money Laundering Prevention Supervision Division Through NRB reporting website in given format	Finance and Planning	NRB Unified Directive ANUSUCHI 9.2
Risk Assessment Framework	Annual	Within 2 months of end of Financial Year	Money Laundering Prevention Supervision Division	Compliance	NRB Unified Directive 19/082 Point 9 sub-point 2.
Annual Report of Task/ Activities on AML/CFT/CFP	Annual	Within 2 months of end of Financial Year	Money Laundering Prevention Supervision Division	Compliance	NRB Unified Directive 19/082 Point 18

5.3 Review / Amendment and Interpretation

This policy shall be reviewed periodically, not exceeding one year from the date of approval / review. Any amendments / insertions shall be recommended to Board level "Assets (Money) Laundering Prevention Committee" for its recommendation to the Board for approval.

In case any confusion in the interpretation of this policy, the matter shall be referred to the Board of Directors through Board level "Assets (Money) Laundering Prevention Committee" and CEO and the decision made by the board shall be the final and binding.

5.4 Relation of Policy with Other Document

This policy must be read in conjunction with the prevailing laws of land pertaining to AML/CFT/CFP such as Assets (Money) Laundering Prevention Act, 2064 (with amendments); Assets (Money) Laundering Prevention Rules, 2081; Suspicious Transactions Reporting Guidelines and Threshold Transactions Reporting Guidelines issued by FIU; the guidelines/directives issued by the NRB and all other related acts/guidelines issued by other regulatory authorities from time to time.

In case there happens to be any contradiction with the prevailing laws and regulation currently in effect or the laws that introduced in future, the subject matters contained in this policy shall be *ab initio void* to the extent of contradiction.

5.5 Power to Formulate Appropriate Manuals/Guidelines

The CEO is authorized to approve appropriate Manuals/Guidelines/SOP required for the effective implementation of the provisions of this policy. Such Manuals/Guidelines/SOP shall be construed as the part of this policy and shall be read in conjunction with the provisions contained in this policy. There shall not be any contradiction in the Manuals/Guidelines/SOP with this policy and any contradiction in the Manuals/Guidelines/SOP with this Policy shall be *ab initio* void to the extent of contradiction. The Manual/Guidelines/SOP shall be approved by the CEO and the same shall be furnished to the Board, and Assets (Money) Laundering Prevention Committee for information.

5.6 Forms, Formats & Declarations

Forms, Formats and declarations required as per this Policy shall be as proposed by respective department which shall be reviewed and vetted by legal department and approved by CEO from time to time.

5.7 Retrospective Application

The standards set by this policy document apply to both new and existing business relationships. It is therefore necessary to initiate corrective actions on customer identification and customer due diligence, where required, for the existing accounts no matter how long the relationship has been in operation. Where significant numbers of accounts are involved, work plans for corrective actions should prioritize relationships representing higher risk.

5.8 Repeal & Saving

“Policy for prevention of Money Laundering and Combating financing of terrorism 2025" approved by the Board of Directors of the Bank vides its 715th Board Meeting dated: 22nd May 2025 and its amendment (if any) by the Board from time to time shall supersede by this policy. Except specified otherwise in this document, any amendments/ cancellation or revision in this policy shall be at the sole discretion of the Board.

Any amendment in the laws / rules / regulations / NRB Directives / Circulars affecting provisions under this policy shall have automatic effect amending such provisions under this Policy.

Annexure– I Terms of Reference of the Units under Compliance Department

1. Transaction Monitoring Unit

- Capacity management of all staffs of the Bank in terms of AML/CFT/CFP and KYC.
- Preparation of reports on agendas for Board Meetings & ALPC Committee.
- Circulation of decision of ALPC and ensuring its implementation
- Ensuring implementation of Board's Instruction to department
- Minute drafting related to Board Level and Management Level Committee
- Implementation of tactical plans and BPR of the department
- Resolution of Internal, External & NRB audit issues related to AML/CFT/CFP
- Preparation & review of policies & guidelines for AML/CFT/CFP
- Study and gap analysis on the industry & International best practices and identification of the necessary changes of implementation.
- Liaison for the response on correspondent banking
- Preparation Fortnightly News Letter
- Monitoring Lending based Transactions
- Monitoring transaction transacted through Digital Products
- Monitoring remittance and trade related transaction for identifying trade based money laundering and cross country money laundering related risk.
- Monitoring Deposit related transactions
- Monitoring other transactions from the perspective of money laundering and financing of terrorism.
- Handling suspicious activity lodged by branches
- Preparation of STR report if transaction conducted found suspicious and reporting to Financial Intelligence Unit.
- Internal and External Regulatory Reporting

goAML Data Cleansing

- Identifying the missing information or incorrect information of every account triggered in Threshold Transaction Reporting (TTR) & also the accounts of Transaction conductor.
- Updating the missing information & correcting the incorrect information identified with the help of account opening form & other documents placed in the link.
- Cleaning, compiling the accounts for which the information could not be corrected or updated for branch follow up.

Branch Follow-up

- Forwarding the accounts for which the information could not be updated by team to the respective branches for completion of missing documents & information.
- Updating the accounts as per information/data given by those branches

Threshold Transaction Reporting

- Obtain the report of TTR triggered account & transactions occurred during each day.
- Clean up the data of each TTR triggered & Transaction conductor accounts (i.e. entity & Individual) as per goAML reporting requirement.
- Generating the report after cleaning up the accounts in standard XML format.
- Uploading the generated XML report on FIU site for goAML reporting.
- Maintaining a register recording all reported transactions & also maintaining files & documents in electronic form.
- Apart from above additional tasks may be assigned by Head-Compliance/ In charge Compliance or Officiating.

2. Query Management Unit

- Receiving of Letter (Inquiry/Instructions) from Enforcement Agencies
- Recording of Inquiry/Instructions Received
- Information/Documents Gathering and Verification as per the letter and instruction received
- Execution of the instruction i.e. providing information and documents, freeze/unfreeze of the account
- Response to the inquiry/instructions
- Recording of response
- Filing and retention of records of the dispatched documents
- Risk upgradation of the account related to inquiry from enforcement agency
- Submitting list of account Risk upgraded to CAP/ Branches for ECDD

3. Screening, ECDD and KYC Management Unit

- Review of medium and high-risk accounts opened during a month on continuous basis in line compliance of Nepal Rastra Bank Directive 19.
- Review of data inputs on core banking system along with the digitized documents received during customer onboarding.
- Escalate discrepancies noted to branch as well as Centralized Account Processing Department for correction and necessary actions.

- Preparation of final report and submit report to management for information.
- Screening of customers, vendors, partners and transactions i.e. Customer onboarding, cross border transactions, remittance transactions, employee accounts, vendors etc.
- Maintain Adverse Media, PEP and Blacklisting database.