Global IME Bank

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

Revised: January 2023

Contents

VERSION CONTROL

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

APPROVAL SHEET

Prepared By:	Kalyan Babu Tiwari AML/CFT Unit	
	Suresh Prakash Chataut AML/CFT Unit	
	Aashish Raj Pandey Money Laundering Reporting Officer	

Supported By:	Sulochan Wagle Strategy Department	
	Sulav Hari Joshi Chief of Country Operations	
	Shanta Siwakoti Chief Marketing Officer	
	Anil Joshi Chief-Information Technology Officer	
	Buddhi Akela Chief Risk and Compliance Officer	
	Bhawani Dhakal Chief Operation Officer	
	Kalyan Bikram Pande Chief Business Officer	

Recommended By:	Surendra Raj Regmi Deputy Chief Executive Officer	
	Mahesh Sharma Dhakal Sr. Dy. Chief Executive Officer	

Approved by:	Ratna Raj Bajracharya Chief Executive Officer	

ABBREVIATIONS

AML	Anti-Money Laundering
ALPA	Asset (Money) Laundering Prevention Act, 2064
APG	Asia/Pacific Group on Money Laundering
BOD	Board of Directors
CDD	Customer Due Diligence
CCO	Chief Compliance Officer
COCO	Chief of Country Operations
CEO	Chief Executive Officer
COO	Chief Operating Officer
CFO	Chief Finance Officer
CFT	Counter-Financing of Terrorism
ECDD	Enhanced Customer Due Diligence
EU	European Union
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GoN	Government of Nepal
HMT	Her Majesty's Treasury, United Kingdom
HNE	High Net Worth Entity
HNI	High Net Worth Individual
HRD	Human Resource Department
KYC	Know Your Customer
KYE	Know Your Employee
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
ML/TF	Money Laundering and/or Terrorist Financing
NRB	Nepal Rastra Bank
NRN	Non-Resident Nepali
OFAC	Office of Foreign Assets Control
PAN	Permanent Account Number
PEP	Politically Exposed Person
Rules	Asset (Money) Laundering Prevention Rules 2073

STR	Suspicious Transaction Report
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TBML	Trade Based Money Laundering
TF	Terrorist Financing
The Policy	Anti-Money Laundering / Counter Financing of Terrorism Policy of the Bank
TOR	Terms of Reference
TTR	Threshold Transaction Report
UN	United Nations
VAT	Value Added Tax
WMD	Weapons of Mass Destruction

CUSTOMER IDENTIFICATION

1.1 Customer identification indicators

1. Customer identification is collection and verification of customer information before providing any services. Customer Identification procedure is to be carried out at following cases[1]:
   a. While establishing business relationship

   b. While opening an account

   c. While carrying out occasional transaction in foreign currency equivalent to or more than NPR 0.1 million by non-accountholders[2].

   d. During wire transfers (cross-border transfers).

   e. When the Bank needs to reconfirm the already availed information of a customer availed for customer identification due to doubt in authenticity or adequacy of such information provided.

   f. When the Bank has a suspicion of money laundering or terrorist financing and needs to reconfirm.

   g. At each transaction of high-risk customers and politically exposed persons.

2. Customer Identification procedure is to be carried out at following cases in addition to the above cases.
   a. If there is complex business structure of a legal person, the Bank has to identify the ownership and control structure in each layer of ownership of a legal person and also identify the natural person(s) (beneficial owner) who ultimately control the legal entity[3].

   b. When there is doubt of involvement of person other than family member as a beneficial owner in the transaction of natural person[4].

   c. When the customer's profile does not match with the volume and number of transactions

   d. When accepting cash deposit of more than NPR 0.1 million in an account from any person other than concerned account operator. In such case, the Bank must obtain identification document/details of the depositor (or third-party conductor) along with purpose of deposit[5].

[1] Asset (Money) Laundering Prevention Act, 2008 Clause 7(KA)
[2] Provision of the law further clarified by Unified Directive 2078, Directive no. 19 clause 2(3)
[3] Unified Directive 2078, Directive no. 19 clause 2(2)
[4] Unified Directive 2078, Directive no. 19 clause 2(4)
[5] Unified Directive 2078, Directive no. 19 clause 2(5)

1.2 Know Your Customer

Know your customer (KYC) helps the Bank to establish the legitimacy of a customer's identity and identify risk factors. KYC involves knowing a customer's identity, their financial activities and the risk they pose. It involves collection of information and documents of a customer, address verification and identification of the reasons behind establishing a relationship or conducting transactions.

1.3 Collection of information

The Banks need to obtain necessary information in establishing the identity of a new customer and continuing relationship with existing customer as well as the purpose of the intended nature of banking relationship. The information collected from the customer at the time of opening account and updating the same shall be treated confidential and shall not be disclosed to any parties unless allowed by law of the land.

1. For new customer
   a. In case of natural and legal persons, the Bank shall have to obtain information as per annex 1. The information thus collected shall be the profile of the customers and act as the basis for customer due diligence.

      The accounts of natural persons, where simplified due diligence is applicable, limited information to be obtained as per annex 1.

   b. The Bank must have a clear understanding of the purpose or intended nature of business of the customer while establishing any relationship with the Bank. For this, the Bank must obtain written disclosure regarding purpose or intended nature of business of the customers.

2. For existing customer
   a. The Bank shall obtain updated information and documents related to a customer in the due course of business / transactions.

   b. The Bank must ensure that the purpose of the customer in establishing any relationship with the Bank has not changed. If any information has changed, the Bank shall have to obtain updated KYC information and update the data / information in the system.

   c. The Bank shall ask the customer for the KYC information and documents that have changed, or might have changed, or that is additional to the existing information/documents available to the Bank. The Bank shall obtain updated information and documents as per the customer's statement / declaration.

3. Collection of KYC information:
   a. The Bank shall collect KYC information of its customers through
      i. duly filled KYC form (simplified KYC form or standard KYC form as applicable) of the Bank by face-to-face meeting or
      ii. e-KYC / video KYC or
      iii. any other means as appropriate and approved by the Bank.

1.4 Collection of documents

1. In case an account is to be opened,
   a. account should be opened only in natural person's or legal person's name exactly as written in government issued identification / registration document[6]. However, the business name can be assigned as per the Article of Association or Memorandum of Association / Constitution etc. as Alias name in the system along with the registration name such that the registration name can be searched/identified and is reported in various transactional reports.

   b. for natural person's accounts, thumb print impression of the account holder(s) and mandatee/power of attorney must be obtained.[7] The thumb print impression of minor is not required while opening account of minors.

   c. for legal person's accounts, thumb print impression only of the account operator(s) must be obtained.[8]

2. Bank shall have to obtain all necessary documents required for establishing relationship with a customer (including related persons and beneficial owners). The documents required, in general, while opening of accounts are mentioned in annex 2. The product specific documents described in a product paper by the Bank in addition to the document mentioned herein shall also to be obtained as appropriate.

3. In case of beneficial owners, the Bank shall have to obtain the following documents from the customer:
   a. In case of company: the list of shareholders certified by Office of Company's Registrar (शेयर लागत) for identification of beneficial owners.

   b. In case of trusts/foundations: details of settlor, trustee, guardian, and beneficiary that control them as per trust deed or similar document.

   c. In case of partnership firm: partnership deed that discloses details of all partners.

   d. In case of other firms/entities: registration document that discloses the ownership structure of the firm.[9]

   e. In case of natural persons: Declaration whether a person is acting on his/her own behalf.

4. The identification documents submitted by the customer must be clear and readable. If the details in original document are not clear, readable or seems doubtful, the Bank shall have to obtain any one of the below mentioned identification documents as a supplement:

Identification Document (Supplement)	Applicable to
1. Citizenship certificate	Nepali
2. Voter's card issued by Government of Nepal	Nepali
3. Valid identity card issued by Government of Nepal	Nepali
4. Valid driving license issued by Government of Nepal	Nepali

[6] In line with clause 12(iii) of "Guidelines for Suspicious Transactions Reporting (STR), July 2021" issued by FIU, Nepal and in goAML Operational Guidelines for BFIs (Updated January 2022).
[7] As per Asset (Money) Laundering Prevention Rule, 2009 clause 4 (4)
[8] As per Asset (Money) Laundering Prevention Rule, 2009 clause 4 (4)
[9] As per Asset (Money) Laundering Prevention Rule, 2009 clause 6 (3)

5. PAN Card issued by Government of Nepal	Nepali
6. Valid passport	Nepali, Indian, NRN
7. NRN Card	Non-Resident Nepali
8. Registration certificate issued by Embassy of India in Nepal	Indian
9. Aadhar Card issued by Government of India	Indian
10. Voter's card issued by Government of India	Indian
11. Valid passport with valid visa	Foreigners except Indian

5. The Bank may ask for any additional documents based on the nature of business, nationality, risk category, income, profile etc. of the customer.

1.5 Identification of related persons

1. Proprietor, partners, board of directors, executive / management committee members, chief executive officer, and account operators shall be termed as related persons to a legal person as appropriate.

2. In case of offices/bodies under/ owned by Government of Nepal, bodies established under special Act, companies under ownership of Government of Nepal, financial institutions licensed by Nepal Rastra Bank, insurance companies licensed by Insurance Board which has offered public shares, United Nations or offices, specialized bodies and international organizations under United Nations and foreign embassy, only authorized account operators shall be termed as related persons[10].

3. The Bank shall have to obtain the following details of the natural persons for the identification of related persons:
   a. Full name
   b. Date of birth
   c. Nationality
   d. Family details - spouse, father, mother and grandfather
   e. Permanent and current address
   f. Identification details
   g. Declaration as PEP and convicted under criminal activities
   h. Telephone, mobile, and email. If not available, customer declaration to be obtained.
   i. Designation
   j. Resident country

1.6 Identification of beneficial owner

The Bank shall have to follow the below specified procedure for identification of Beneficial owner.

1. The Bank shall have to obtain the following details of the natural persons who are identified as beneficial owners.
   a. Full name
   b. Date of birth
   c. Nationality
   d. Family details – spouse, father, mother and grandfather
   e. Permanent and current address
   f. Identification details
   g. Declaration as PEP and convicted under criminal activities

[10] Unified Directive 2078, Directive 19, clause 2(7)

h. Location Map of the current resident
i. Income and /or work-related details including expected annual income
j. Resident country
k. Share ownership in case of legal person

2. Following measures shall have to be applied to identify beneficial owners of legal entities[11]:

   a. By identifying natural person(s) who ultimately owns 10 percent or more shares or capital of the legal person.

   b. The natural person who holds the position of senior managing official in case no natural person holds 10 percent or more shares or capital of the legal person

   c. The natural person who can exercise significant control over the company.

      i. A person who can hire or terminate a member of senior level management

      ii. A person who can appoint or dismiss Directors

      iii. Senior managers who have control over daily/regular operations of the person / arrangement (e.g., CEO, CFO, or a Managing Director)

3. In case the beneficial owner has changed, the Bank shall obtain the adequate information and documents required to identify and verify new beneficial owner.

1.7 Identifying politically exposed persons

1. PEPs shall be identified through any one or all of the below mentioned mechanism:
   a. Checking the customer's name (name screening) using database adopted by the Bank through system adopted by the Bank. (Please refer section 2.2.1).

   b. Obtaining declaration from the customer if they are PEP, or family members of PEP, or PEP associates during on-boarding and periodic reviewing.

   c. Obtaining declaration from PEP whether their family members maintain any account with the Bank while conducting enhanced due diligence.

   d. Obtaining any valid documents evidencing that the person is a PEP.

   e. Using publicly available information of the customer, where it is possible for the Bank to verify such information through independent sources.

2. Once the PEP is identified, the PEP must be categorized as domestic PEP, foreign PEP or international PEP.

3. PEP shall remain as PEP till 5 years from the date of cessation from the prominent public function.

[11] As per Asset (Money) Laundering Prevention Rule, 2009 clause 6 (2)

1.8 Identifying high net worth customers

1. The Bank shall identify High Net Worth Individual (HNI) where total account balance is NPR 50 million and more in all of the accounts – current, savings, call, margin and fixed – maintained with the Bank at the end of each fiscal year.

2. The Bank shall identify High Net Worth Entity (HNE) where total account balance is NPR 200 million and more in all of the accounts – current, savings, call, margin and fixed – maintained with the Bank at the end of each fiscal year.

1.9 Address verification

Address verification is a process to ensure that a person lives where they claim to reside. It also ensures that address is accurate and up to date.

1. In case of individual customers categorized under low risk, current address verification is not necessarily required.

2. In case of individual customers categorized under medium and high risk, current address verification is to be made through any or all of the below mentioned measures:

    a. Matching the address mentioned in account opening / KYC form with address mentioned in the identification document submitted by the customer. Any Identification document issued by Government of Nepal (federal, provincial or local level government) or by government owned public enterprises / institutions and constituent bodies where address has been disclosed shall only be accepted for this purpose.

    b. In case the location of the customer cannot be identified through location map or identification document, address verification is to be made through one of the following measures

        i. Matching the address mentioned in account opening / KYC form with the most recent copy of the utility bill. The utility bill may be addressed to another person's name with whom the customer is living within a same premise.

        ii. Matching the address mentioned in account opening / KYC form through physical verification of the location. The physical verification can be made by any officials of the branch except for support level staffs. If the physical verification is made, a brief report or remarks regarding the observations of such visits is to be maintained in the file along with account opening documents.

        iii. In case of individual customers are staffs of Government of Nepal categorized under high risk, current address verification is not required to be made through physical verification of the location.

3. For accounts of individuals opened online and for customer onboarded through video KYC, current address verification shall have to be performed in an appropriate manner or as described in the respective product papers.

4. In the event that the address verification cannot be performed due to any reasons whatsoever, approval from COO or any other person delegated by COO is to be obtained.

5. Irrespective of the risk, the current address must be physically verified in case of domestic entities suspectable of being shell entities.

1.10 Document verification

1. The Bank has to verify the copy of the documents submitted by the customers with original documents.

2. The Bank may, as deemed necessary, also supplement the identity of the customer through available external sources such as: Inland Revenue Office (PAN): https://ird.gov.np/pan-search.

RISK MANAGEMENT

2.1 Screening

Name Screening is one of the methods used for risk assessment of the customers of the Bank. It is to be carried out on sanctions, PEP, adverse media, and internal lists of the Bank. Name screening is designed to identify targeted individuals or entities during on-boarding or the lifecycle of the customer relationship with the Bank to adopt proper risk identification and categorization of customers.

2.1.1 Name screening

1. Name screening is to be carried out based on the name as per government issued valid identity documents for individuals or registration certificate for entities in following circumstances:

    a. During establishing relationship with a customer with or without opening a deposit account with us.

    b. During periodic and event driven review of customers

    c. In case of international fund transfers initiated through SWIFT by the Bank.

2. Name screening is to be performed irrespective of the customer risk profile and is to be done in real time.

3. The process of name screening in branches is to be overseen by Operations In-charge. In case of departments at Corporate Office and Province Offices, the department heads or province heads to ensure name screening is properly conducted in their offices / departments.

4. The name screening is to be conducted against names appearing on sanction list, politically exposed persons list, adverse media list and internal negative list. Such list is to be arranged by the Bank by maintaining database internally and/or by subscribing the database. Internal negative list shall be prepared by the department handling correspondence / letters received from Nepal Rastra Bank and other authorities.

5. The Bank has adopted to comply with the sanction list issued by the UN, OFAC, EU, HMT, Australian list and list published by Ministry of Home Affairs of Nepal. AML/CFT Unit shall be responsible to ensure that the list is updated in the system. For this coordination from Information Technology Department and Digital Banking Department shall be sought.

6. Central Operations and province offices overseeing the branches shall monitor that the name screening is being performed by the branches properly.

7. In case a person/entity is under Sanction list, the Bank cannot establish any relationship with the customer. Please refer 3.4 for the procedure to be followed in case a name matches in the sanction list.

8. In case a person/entity is under PEP list, the Bank can establish a relationship with the customer.

9. Adverse media screening is conducted to assess the customer's risk profile by checking unfavorable information discovered across various public sources / domain. A proper adverse media check can expose a person's or an entity's involvement in money laundering, terrorist financing, financial fraud, organized crime etc. In case a customer is identified under adverse media list, the Bank can establish a relationship with the customer.

    a. The Bank shall refer the third-party database (Accuity) which report on a broad spectrum of global and national events.

    b. The Bank shall consider only the predicate offence or the financial crime such as money laundering, terrorism/terrorist financing, bribery and corruption, organized crime, drug trafficking, human trafficking, wildlife trafficking, proliferation and proliferation financing, and tax evasion.

    c. The Bank shall consider all stages of news - allegation, investigation, charges and conviction made to a customer in conducting adverse media screening.

10. An internal negative list shall be developed by the Bank based on the instruction received from various investigative, governmental, regulatory and constitutional bodies to block / release of accounts. In case the name of a person/entity matches with the Internal Negative list, the Bank cannot establish any relationship with the customer until the name is removed from such list.

2.1.2 Batch name screening

1. Batch name screening shall be conducted based on the data maintained in the core banking system (Finacle) against third party Accuity Database. The batch name screening shall be based upon the records of full name and profession details available in Finacle and Accuity database.

2. Batch name screening of all customers under sanction list shall be conducted by AML/CFT Unit:

    a. The batch name screening against sanctioned list is to be carried out on the subsequent month of end of each quarter.

    b. While conducting batch name screening against sanction list, any name that appears similar by 98% or more shall be rechecked with available documents and information to ascertain whether the person is under sanction list.

c. The procedure to be followed in case a name matches under Sanction list shall be as per 3.4.

3. Batch name screening of all customers under PEP list shall be conducted by AML/CFT Unit:

   a. The batch name screening against PEP list is to be carried out annually – within the first month subsequent to the end of a fiscal year.

   b. While conducting batch name screening against PEP list, any name that matches 100% shall be provided to Central Operations.

   c. Central Operations have to check for the correctness of the result within next 15 working days.

   d. The procedure to be followed in case a name matches under PEP list shall be as per 3.2.

4. Once the batch name screening is conducted and names are verified to the extent possible, the result shall have to be notified to AML/CFT Management Committee through AML/CFT Implementation Report.

2.2 Customer due diligence parameters

The Bank shall take risk-based approach in the identification, assessment, understanding and mitigation of ML/TF risk by considering influencing factors such as geography or country, customers (including occupation, profession, and type), product or service availed, nature of the transaction, and delivery channels in conducting customer due diligence. The parameters followed by the Bank for customer due diligence shall be as under:

1. For new customers
   a. Name screening of customer
      i. Name screening of accountholder and related person (owners, directors, beneficial owners, signatories, mandatee/person having power of attorney etc.) shall be conducted as per 2.1.1. The name screening shall result to “no match”, or match with “sanction”, “PEP” or “Adverse Media”.

      ii. The screening shall also be based on customer’s self-declaration as PEP in the KYC form which needs to be examined whether such person can be categorized as PEP as per 1.7 (1) (d) and 1.7 (1) (e) above. If a person declares as “associated with a PEP”, the customer is to be considered as a PEP.

      iii. If a person declares as “involved in financial crime”, the customer is to be considered as a high-risk customer.

   b. Geography
      i. The nationality of the customer shall be matched with high-risk jurisdictions (countries) list published by FATF.

      ii. The need for FATCA reporting shall also be assessed by inquiring about US Green Card / US citizen for individuals and whether any US company owns share of 10% and more in case of legal person.

iii. In case of Nepali citizen and entities registered in Nepal, the district mentioned in permanent address shall be checked with the districts categorized as high, medium, or low risks based on the crime rates data available. The crime rate of different districts is presented in annex 3

c. Customers (including occupation, profession, and type),

i. To identify whether the introducer of the customer in opening an account is a staff of the Bank or other accountholder or the account is opened based on government's requests for distribution of subsidy and other such incentives.

ii. To ensure that the accounts are operated by the accountholder and his/her family members, the Bank shall check whether mandatee / power of attorney has been provided to persons other than unseparated family members. In case of sole proprietorship firms, the Bank shall ensure that the accounts are operated by the accountholder or his/her unseparated family members.

iii. Bank to ensure that all required documents have been obtained and that the customer fully cooperated in providing documents and information sought by the Bank.

iv. The Bank to ensure the customer's involvement in businesses considered as high-risk by the Bank. Involvement in high-risk business shall not include the customer working as an employee.

v. The Bank to identify the primary occupation of the individual customer. In case of entities, the Bank needs to check whether the type of business is high risk business as defined by the Bank. The high, medium and low risk businesses categorized by the Bank shall be as per annex 4.

vi. The Bank needs to confirm whether there are any beneficial owners. In case of companies, the recent shareholding list (शेयर लागत) from Office of Company's Registrar shall be obtained to ensure whether any natural person holds 10% or more share of the entity.

d. Nature of product or service availed

i. The Bank shall have to identify whether the customer requires current, savings or fixed deposit accounts/product.

ii. The Bank shall have to identify whether the customer intends to avail or has been availing funded or non-funded or both loans with the Bank.

e. Nature of the transaction

i. The customer needs to declare estimated annual transaction during opening of an account with the Bank. The Bank, based on profile of the customer, needs to analyze such declaration and to ensure whether the customer is highly overstating or underrating this information. The Bank official conducting customer due diligence needs to justify the basis of analysis if there are substantial differences – estimation of the Bank official is 5 times more / less than what the customer declared.

ii. In case of an account opened for receiving remittance, the Bank official needs to ensure that the customer receives remittance through formal channels.

f. Delivery channels
   i. The Bank needs to state whether a customer has been met in person (face-to-face). Meeting through video KYC shall be considered as face-to-face meeting.

2. For existing customers
   a. Name screening of customer
      i. Name screening of accountholder and related person (owners, directors, beneficial owners, signatories, mandatee/person having power of attorney etc.) shall be conducted as per 2.1.1. The name screening shall result to "no match", or match with "sanction", "PEP" or "Adverse Media".

      ii. The screening shall also be based on customer's self-declaration as PEP in the KYC form which needs to be examined whether such person can be categorized as PEP as per 1.7 (1) (d) and 1.7 (1) (e) above. If a person declares as "associated with a PEP", the customer is to be considered as a PEP.

      iii. If a person declares as "involved in financial crime", the customer is to be considered as a high-risk customer.

   b. Geography
      i. The nationality of the customer shall be matched with high-risk counties list published by FATF.

      ii. The need for FATCA reporting shall also be assessed by inquiring about US Green Card/ US citizen for individuals and whether any US company owns share of 10% & more in case of legal person.

      iii. In case of Nepali citizen and entities registered in Nepal, the district mentioned in permanent address shall be checked with the districts categorized as high, medium, or low risks based on the crime rates data available. The crime rate of different districts is presented in annex 3

   c. Customers (including occupation, profession, and type),
      i. The Bank needs to ensure that the identification documents obtained by the Bank as per 1.4 (2) above is valid.

      ii. To ensure that the accounts of individuals are operated by the accountholder and his/her family members, the Bank shall check whether mandatee / power of attorney has been provided to persons other than unseparated family members. In case of entities where there is only one signatory assigned in the account by the customer, the Bank shall check that the accounts are operated by the accountholder or his/her unseparated family members.

iii. The customer needs to provide his/her primary occupation where s/he is involved most of the time including source of income. In case of entities, the Bank needs to check whether the type of business is high risk business as defined by the Bank. The high-risk business and low risk businesses as per business type shall be as per annex 4

iv. The customer needs to confirm whether there are any beneficial owners. In case of entity, the declaration or the recent shareholding list (शेयर लागत) from the Office of the Company's Registrar whichever is applicable shall be obtained to ensure whether any natural person holds 10% or more share of the entity.

d. Nature of product or service availed
   i. In the case the customer had any account with the Bank, the risk grading at the time and past transaction behavior needs to be checked.

   ii. In case of entity, the detail whether it has availed non-funded facility from the Bank needs to be checked.

   iii. In case of an account opened for receiving remittance, the Bank official needs to ensure that the customer receives remittance through formal channels.

e. Nature of the transaction
   i. The Bank shall have to check whether high frequency of transactions made in cash by persons other than the accountholder in the last fiscal year. The MIS report shall be used for this.

f. Delivery channels
   i. The Bank need to state whether a customer has been met in person (face-to-face) in the review period. Meeting through video KYC shall be considered as face-to-face meeting.

3. All the above parameters for both new and existing customers while conducting CDD shall be used for appropriate risk grading. In the basis of risk associated with the customers, the Bank shall apply the appropriate due diligence mechanism as:

   a. Simplified Due Diligence
   b. Standard Due Diligence
   c. Enhanced Due Diligence

2.2.1 Simplified Due Diligence

Simplified due diligence is the lowest level of due diligence that can be conducted of a customer. This is appropriate where there is little opportunity or risk of Bank's services or customer becoming involved in ML/TF activities.

1. Simplified due diligence shall be applicable in the following cases

   a. in establishing relationship with customers for local level programs organized for social and economic benefit of Nepali citizens upon

approval from the Nepal Rastra Bank[12]. However, such approval shall not be required if such programs are for a period of 3 months or less[13].

b. Accounts opened under "खोलौ बैंक खाता अभियान, २०७६" for Nepali citizen who have no bank accounts opened previously.[14]

c. Any special purpose scheme of accounts offered by the Bank to encourage Nepalese citizen to establish saving habit as part of its financial inclusion.

d. Any account where transaction is less than or equal to NPR 0.1 million in a fiscal year.

e. Accounts opened for distribution of social security allowance, elderly allowance and other such benefit payments by the Government of Nepal and where other transactions are restricted by the Bank.

2. The Bank shall categorize such customers under low risk and put a tag in the system to identify customers where simplified due diligence is performed.[15]

3. In conducting simplified due diligence, the Bank shall
   a. Obtain the name of grandfather, father and mother of the customer. It shall not be compulsory for the Bank to obtain the details of customer's spouse, children, brothers and sisters, daughter -in-law and mother-in-law.

   b. The permanent address to be as per the identification document submitted and current address need not to be verified.

   c. Obtain primary identification document (citizenship, passport, voter's card, or license).

4. Simplified due diligence shall not be applied in the below cases[16]:
   a. If a customer is a foreign national

   b. Customer of the countries that are largely non-compliant with international standards on combating of money laundering and terrorist financing or customers having transactions at such territories or countries.

   c. Customer listed to Stock Exchange of the countries that are largely non-compliant with international standards on combating of money laundering and terrorist financing.

[12]Asset (Money) Laundering Prevention Rule, 2009 clause 9(2)
[13] Provision of the law further clarified by Unified Directive 2078, Directive no. 19 clause 7(4)
[14] Unified Directive, 2078 Directive 19 Clause 7(ka)
[15] Unified Directive 2078, Directive 19 clause 7(2)
[16]Asset (Money) Laundering Prevention Rule, 2009 Clause 9(3)

d. Legal entities or legal arrangements, if the details of their beneficial owners are not publicly available

e. PEP or family member of PEP or close associate of PEP or customer having PEP as beneficial owner.

f. Customer posing high risk or customers suspected of being involved in money laundering or terrorist financing activities.

g. Account where annual transaction is more than NPR 0.1 million.

2.2.2 Standard Due Diligence

1. In majority of cases, standard due diligence is the level of due diligence that shall be used. These are generally situations where there is a potential risk but it is unlikely that these risks will be realized.

2. The standard customer due diligence shall be conducted in cases where customers are identified as low risk customer but simplified customer due diligence cannot be applied. Such customers shall include:
   a. Ministries and departments of Government of Nepal

   b. Public enterprises where the share of Government of Nepal is more than 50% of total equity.

   c. Regulators and statutory bodies.

   d. Bank and financial institutions regulated by NRB and insurance companies regulated by Insurance Board of Nepal as their ownership structure/details, shareholding pattern, controlling interest, beneficiary details are published and easily available.

   e. Employees whose salary structures are well defined.

   f. Pensioners

   g. Government /community-based school/college/universities

   h. UN Agencies and Mission of United Nations

   i. Accounts opened for distribution of social security allowances / supports/ reliefs by the Government.

3. The standard customer due diligence will be conducted for customers availing letter of credit and bank guarantee having following threshold:

   a. Sum of all LC facilities availed by a customer in a fiscal year is less than NPR 100 million or equivalent

   b. Sum of all guarantees availed in a fiscal year is less than NPR 150 million or equivalent.

4. The standard customer due diligence will be conducted for medium risk customers.

2.2.3 Enhanced Customer Due Diligence

Enhanced CDD is required for certain types of customers and some transactions or activities where the Bank considers that the level of ML/TF risk involved is high (high-risk customers). Enhanced customer due diligence involves inquiring for additional information regarding identifying of a customer, address and income source.

1. Enhanced CDD shall be carried out for establishment of banking relationship or continuing existing relationship with the following customers:

    a. Cash intensive business with annual credit turnover (in a fiscal year) in cash above NPR 100 million.

    b. Legal persons involved in dealing of high value goods or precious metals or mining of precious stones. Such customers include jewelry businesses, business of precious metals, art and antique dealers.

    c. Casino/ Gambling house, night clubs.

    d. Money Service Business (MSB) which includes remittance company (excluding agents) and exchange houses (including money changers).

    e. Trusts, Charities, Non-Profit Organizations which includes religious charities, religious institutions, charitable foundation Non-Governmental Organizations, International Non-Governmental Organizations receiving donations.

    f. Private/Personal Investment Company (PIC) that is often established in an offshore jurisdiction with tight secrecy laws to protect the privacy of its owners.

    g. Companies issuing bearer shares

    h. Embassies, Consulates Missions

    i. Legal persons having complex business ownership structure with more than 2 layers of ownership structure.

    j. Offshore Entity/Offshore Banks

    k. Entity where total account balance is NPR 200 million or more in all of the accounts – current, savings, call, margin and fixed – maintained with the Bank at the end of each fiscal year.

    l. Entity account operated by single person (mandatee) who is not the owner or family members of the owner.

    m. Real estate business involved in land plotting, building residential houses for sale or building commercial complex, constructing apartments and involved in land development. It shall not include

construction companies or individuals that are hired or employed by real estate businesses.

n. Correspondent Banks

o. Trade Finance customers having following threshold:

   i. Sum of all LC facilities availed by a customer in a fiscal year is NPR 100 million and above or equivalent

   ii. Sum of all guarantees availed in a fiscal year is NPR 150 million and above or equivalent

p. Involvement of PEP as a shareholder holding 10% or above shares, or as acting as a member of Board of Director, Chief Executive Officer, partner (for partnership firm), signatory, mandatee, or beneficial owner.

q. Politically exposed Persons (PEPs), their family members and their associates.

r. Individual whose total account balance is NPR 50 million or more in all of the accounts – current, savings, call, margin and fixed – maintained with the Bank at the end of a fiscal year.

s. Individual account operated by mandatee who is not the family member of account holder.

t. Individual who is owner of the High Risk categorized legal entity.

u. Citizen of high-risk jurisdictions (countries) list published by FATF.

v. True match of customer with person/entity in the adverse media list as outlined in 2.1.1 (9)

2. While conducting enhanced customer due diligence, the Bank shall undertake following measures[17].

a. To examine the purpose and background of large or complex transactions having no apparent economic or legal motives.

b. To identify the background of transactions and purpose of the customer through all reasonable means possible.

c. To continuously monitor the customer or the person having control on a transaction to ensure whether such customer or transaction is unnatural or suspicious or identify the transaction that needs to be further monitored or examined.

d. Obtain or collect information of the customer, beneficial owners and related persons.

[17] Asset (Money) Laundering Prevention Rule, 2009 Clause 8(1)

e. Obtain additional information with regard to business relation, transaction and background, nature and purpose of the same.

f. To obtain approval from Chief Operating Officer or any other official designated by Chief Operating Officer as per 3.2, for establishing new or continuing existing business relationship.

g. Transaction amount shall be as per the declaration made in the account open form / updated KYC form.

h. To inspect or verify the documents obtained through other means.

i. To continuously update customer's KYC information

j. To apply all reasonable measures to identify the sources of fund or wealth of customers by obtaining customer's declaration or if possible, by obtaining documents evidencing sources of funds/wealth.

k. To maintain proper records of the due diligence and provide such records to authorized authorities including auditors.

2.3 Risk scoring and ratings

1. Based on customer due diligence parameters, the Bank shall provide the risk score to its customers through risk based CDD mechanism and based on such scores, customers shall be categorized under high risk, medium risk and low risk customers.

2. The Bank shall identify inherent risk by analyzing the risk factors: Customer, Country, Geography and Products & services offered. These risk factors shall be further classified to the below mentioned parameters in assisting the derivation of inherent risk:

SN	Risk Factors	Parameters for CDD
1	Customer	Name screening of customer
		Customer (occupation, profession, and type)
		Nature of the transaction
2	Country	High Risk Countries
3	Geography	Areas within the country where illegal activities are high
4	Product and service Offered	Nature of product or service availed
		Delivery channels

3. The risk assigned to each parameter and risk scored shall be as per annex 5.

4. The risk scoring and ratings shall be provided automatically once all details are mentioned in the CDD form currently developed in excel spreadsheet until it is digitally prepared and integrated with the account open module of the Bank.

2.4 Use of third party

The Bank may rely on the KYC information and documents collected / CDD conducted by third party provided that the criteria set out below are met. However, the ultimate responsibility for CDD measures remains with the Bank relying on the third party.

1. That the copies of identification data and other relevant documents relating to the CDD requirements will be made available from the third party upon request without delay.

2. That the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements similar to that of the Bank.

3. The Bank shall provide AML training prior to the appointment of and periodically to the third-party agents.

2.5 Internal controls

The Bank shall ensure that the process and practices to manage the inherent risks identified are proper. For this, the Bank shall rely on internal audit and internal compliance testing. The Bank shall assess the effectiveness of AML/CFT program through:

1. Observations and comments with regard to AML/CFT matters made by Internal Audit Department during its visits to branches and departments.

2. Observations and comments with regard to AML/CFT matters made during external and regulatory audits.

3. Ensuring proper implementation of AML/CFT program through internal questionnaire, onsite visits and incident reporting received from various branches and departments. Onsite/offsite visits shall be conducted (as appropriate) by the AML/CFT Unit to check/monitor the activities and to create awareness in aspects relating to AML/CFT.

2.6 Wire Transfers

1. All wire transfers must be made after obtaining the below mentioned minimum information for proper identification and verification of customer irrespective of the currency and amount[18]:
   a. Originator's full name

   b. Account Number of originator and where account does not exist, unique reference number that is sufficient for identification of transaction

   c. Address of the originator and where the same is not available, date of birth and place of birth or citizenship number or national identification number or customer identification number.

   d. Name and account number of beneficiary and where account does not exist, unique reference number that is sufficient for identification of transaction.

   Originator here also refers to the beneficial owner of the originator.

2. In relation to the wire transfer, following points shall have to be considered and taken care of:

   a. Information and details as mentioned above shall also be applicable in case of wire transfer through batch file.

[18] Asset (Money) Laundering Prevention Act, 2008, Clause 7 (THA)

b. In case the Bank acts as an intermediary or beneficiary bank, it should ensure that originator's information is retained with the transfer.

c. In case such information is not retained with transfer, the Bank shall have to seek the same from ordering bank or intermediary.

d. If such information is not received from ordering bank or intermediary, such payment shall have to be withheld, return or accept till the required information is received.

e. While making payment of wire transfers, customer identification procedure has to be applied for beneficiary.

f. In case of having agent in relation to wire transfer, it should be ensured that such agent should have implemented the program for anti-money laundering and combating of financing of terrorism and implementation of the same shall have to be regularly monitored.

g. Requirement of originator's information is not necessary in following transactions:
    i. Wire transfer, resulted on account of purchase of goods or services through debit card, credit card or prepaid card where details of the transaction are recorded in the card.

    ii. Interbank transfers and settlements, where both the originator and beneficiary are banks or financial institutions.

    iii. If the Bank is satisfied with existing customer identification and verification of the customer and does not envisage any money laundering or terrorist financing risk associated with him/her in case of originator or beneficiary being existing customer of the Bank.

CUSTOMER ACCEPTANCE

3.1 General guideline for accepting a customer

The customer acceptance procedure shall have to be followed by the Bank to identify the circumstances under which a new relationship would be accepted and a current relationship would be continued in a risk-based approach by understanding and mitigating risk.

Customer shall be onboarded or the existing relationship shall be continued under the following circumstances:

1. Where the Bank is able to confirm the true identity of the customer by collecting all relevant information and documents so that accounts are not opened under anonymous or fictitious names.

2. Where the customer are not shell banks/company/firms.

3. In case of legal persons, such persons must have registered under the law of the land (except allowed by regulator or legal body for specific purpose).

4. Where the customer acting on behalf of another customer to open an account have legal right to do so.

5. Entities/persons not listed in the sanctioned lists of UN, OFAC, EU, HMT, Australian list and list published by Ministry of Home Affairs of Nepal.

6. By verifying the identity of the customer as per the customer identification procedure where customer profile can be created, customer due diligence can be conducted and risk category can be assigned.

7. Where the customer is fully cooperative in providing required documents and information such that the documents and information are reliable and can be verified with an independent source. The bank shall restrict opening of accounts or stop continuing business relationship (block of all transactions / closure of accounts) with a customer who is reluctant to provide documents, and information mandatorily required to identify and access ML/TF risk associated with the customer[19].

8. Where the customer does not deal with crypto currency.

9. Where the transactions with the Bank are not related with purchase or sale of arms.

10. The customers not involved in activities prohibited under law of the land.

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

3.2 Accepting high-risk customers

1. The Bank shall accept business relationship with a high-risk customer by conducting enhanced due diligence.

2. The Bank needs to obtain approval from Chief Operating Officer or any other person delegated by Chief Operating Officer before starting or continuing a business relationship with a high-risk customer[20].

    a. The branches need to process approval from High-Risk Customer Approval System.

    b. Approvals provided digitally by using High-Risk Customer Approval System shall construed as valid approvals.

3. The Bank shall obtain information regarding the source of income, identify family, close associates and beneficial owners of a PEPs, through an Enhanced Due Diligence Form as mentioned in annex 6 that needs to be filled up by the Bank staffs by obtaining information from the customer.

4. In the event of an existing customer or beneficial owner of an existing account thereafter becoming PEP, branch which is maintaining their account should contact the customer and obtain additional details required for completing Enhanced Due Diligence.

3.3 Accepting correspondent banking relationship

1. The correspondent banking relationship should be established by
    a. Obtaining sufficient information required for establishing correspondent relationship. For this The Wolfsberg Group Wolfsberg Correspondent Banking Due Diligence Questionnaire of the correspondent bank or AML questionnaire of the Bank should be obtained and periodically analyzed to assess the AML controls and related risk of such banks.

    b. Assessing the AML/CFT policies, procedures, systems and controls, and decide that they are adequate and effective

    c. Obtaining senior management approval to establish the relationship

    d. Documenting the respective responsibilities of the respondent and correspondent, including in relation to AML and CFT matters;

    e. Ensuring whether the respondent bank is regulated and supervised (at least for AML and CFT purposes) by a regulatory or governmental authority, body or agency equivalent to the Regulator in each foreign jurisdiction in which it operates;

2. The Bank must be satisfied that the respondent bank
    a. will have conducted CDD for its customers and verified the customers' identities.

    b. will conduct ongoing monitoring for the customers. For this Treasury Department shall monitor the transaction from / to such respondent bank.

[20] Asset (Money) Laundering Prevention Rule, 2009 clause 8(CHA)

c. will be able to provide the Bank, on request, the documents, data or information obtained in conducting CDD and ongoing monitoring for the customers.

3. If the respondent is a subsidiary of another legal person
   a. the parent's company's jurisdiction (or country) (if different)

   b. whether it is regulated and supervised (at least for AML and CFT purposes) by a regulatory or governmental authority, body or agency equivalent to the Regulator in each jurisdiction in which it operates;

   c. whether each foreign jurisdiction in which it operates has an effective AML/CFT regime

   d. its ownership, control and management structure (including whether it is owned, controlled or managed by a PEP)

4. The Treasury & International Banking Department of the Bank must conduct enhanced ongoing monitoring of the volume and nature of the transactions conducted if the respondent bank is in a high-risk jurisdiction.

5. The Bank must review the relationship and the transactions conducted at least annually by considering RMA.

3.4 Sanctioned parties

Sanctioned countries are the countries against whom the political and economic trade restrictions are put in place to prevent terrorism, the proliferation of weapons, violation of international treaties, money laundering, drug trafficking, and destabilization of sovereign nations.

1. The Bank shall not carry out any transactions related with countries by any means at/with the countries that fall in “Call for Action” list of Financial Action Task Force (FATF) under the list of “High Risk and other monitored jurisdictions”. For the list, please refer the link: http://www.fatf-gafi.org/countries/#high-risk. At present, Democratic People’s Republic of Korea (North Korea) and Iran fall under “Call for Action” of Financial Task Force.

2. The Bank shall strictly prohibit transaction with the sanctioned parties under UN, OFAC, EU, HMT, Australian list and list published by Ministry of Home Affairs of Nepal.

3. Branches before opening any new account shall have to check the name of proposed customer as 2.1.1 to ensure that the name of the proposed customer does not appear in the sanction lists.

4. In case the customer is not sanctioned, the branch may open accounts.

5. In case of exact match, the Bank shall not open account. And the name of proposed customer (sanctioned individual or entity), the same should immediately be reported to MLRO who shall inform the Chief Risk and Compliance Officer.

6. AML/CFT Unit shall ask for the confirmation from the account maintaining branch regarding services availed by such customer. Based on the reply received AML/CFT Unit shall block the accounts and ensure all services availed by the customer are restricted.

3.5 Combating of Financing of Terrorism

1. The AML/CFT Unit of the Bank shall update the list of terrorist individual, group or organization either by regularly visiting the website of Ministry of Home Affairs or through third party database that incorporates sanction list published by UN.

2. During screening, if a new customer is found to be enlisted in the list of terrorist individual, group or organization,

   a. The branches and departments shall not establish relationship with the customer and report to AML/CFT Unit.

   b. The branches and departments shall be responsible to provide additional details and documents as asked by AML/CFT Unit.

3. In case any existing customer of the Bank is found to be enlisted in the list of terrorist individual, group or organization, the Bank should immediately freeze the assets of such persons.

   a. AML/CFT Unit shall freeze accounts including joint accounts, lockers, debit/credit cards, mobile banking services, internet banking services, QR code services and any Bank products and services, restricting any financial transactions in the same day such persons are identified.

   b. Freeze of account and other facilities shall be executed without prior notice to customers.

   c. AML/CFT Unit shall have to provide the information to Financial Intelligence Unit, Nepal within three days in the form of STR/SAR[21].

   d. Upon the name delisted by Ministry of Home Affairs, AML/CFT Unit shall allow financial transactions removing all restrictions in accounts and services as mentioned in “a” above.

3.6 Downstream correspondent banking (or nesting)

Downstream correspondent clearance (or nesting) refers to the use of a bank's correspondent relationship by a number of underlying banks or financial institutions through their relationships with the correspondent bank’s direct customer. The underlying respondent banks or financial institutions conduct transactions and obtain access to other financial services without being direct customers of the correspondent bank.

The Bank shall not allow downstream correspondent banking services to any respondent bank.

3.7 Payable-through Accounts or Pass-through Accounts

The Bank shall not allow its customers to directly access the correspondent account to conduct business on their own behalf. Also, the Bank shall restrict the customer of respondent banks to have direct access to the vostro account.

[21] Asset (Money) Laundering Prevention Act, 2008 Clause 29Chha (5)

MONITORING AND REVIEW

4.1 Transaction monitoring program

A strong transaction monitoring program is crucial for the Bank towards implementation of effective anti-money laundering and countering terrorist financing. The transaction monitoring program shall include all functions of the Bank to participate equally in identifying and investigating transactions and behaviors of customers that creates alerts regarding suspicious activity

The monitoring of transactions shall be based on customer behavior, transaction pattern, and profile of the customers

1. observed by the front-line business units,

2. through a set of rules in the AML system and MIS reports by AML/CFT Unit, and

3. through checks and audits conducted by the Bank.

4.2 Monitoring by branches

Branches shall have to be vigilant for any unusual/ suspicious transactions/activities by the customers. Regarding the transactions carried out in the branch premises, the branches need to:

1. Provide special attention to the size, frequency or patterns of transactions that may indicate unusual or suspicious activity.

    a. Large or frequent cash transaction, either deposits or withdrawals.

    b. Unexpected number of transactions and movement of fund in an account.

    c. Large number of individuals depositing fund into the same account

2. Closely examine the transactions of customers to ensure that the transactions are consistent with the customer's profile.

3. Examine the legitimacy of source of funds if found suspicious.

4. Be more vigilant in each transaction carried out by PEPs

5. Provide attention to the customers who

    a. Visit only during rush hours and demands prompt service

    b. Inquire about AML controls adopted by the Bank

    c. Want to maintain more than one mandatee in the account

    d. Are reluctant to provide normal information when opening an account

e. Use of safe deposit lockers at multiple times (more than 6 times) in a month except in festive seasons.

f. Has opened account at a place other than the permanent/registered, office/work, or current address of the customer.

g. makes unusually large cash payments in relation to business activities which would normally be paid by cheques / digital means.

h. Frequently transact on amount less than NPR 1 million.

6. In case any transaction or activity of the customer seems suspicious, same has to be immediately reported to AML/CFT Unit by any staff of the branch as per annex 9 for further analysis.

4.3 Monitoring of transactions

As a first line of defense, the front-line business functions that are involved in remittance related, transaction banking related, wire transfers related, trade related and loans related transactions of their customers shall have to monitor the transactions carried out by their customers and report suspicious transactions to AML/CFT Unit at Corporate Office as per Annex 9.

The following triggers are indicative and minimum. The concerned departments/ functions are free to build their own additional triggers or modify the parameters of the below mentioned triggers as per their discretion so as to strengthen the AML/CFT program of the Bank.

4.3.1 Remittance transactions related

Following triggers shall assist the Bank to identify such transactions.

1. Provide special attention where remittance in smaller volume or the purpose of remittance received is not clear to the receiver:
   a. a number of transactions is made by the same counter-party (sender) in amounts less than NPR 0.1 million to multiple customers

   b. there is high frequency of remittance received in an account in a month in amount less than NPR 0.1 million

   c. Customer does not appear to know the sender of fund and its intended purpose for remittance above NPR 1 million.

2. Closely examine the any transaction in which the nature, size or frequency appears unusual where:
   a. the remittance received in excess of NPR 0.1 million is immediately withdrawn in cash.

   b. the remittance received is transferred to multiple accounts within the Bank or to other banks through the use of digital channels.

   c. the purpose of remittance is difficult to understand or is vague. Or the sender uses foreign language (excluding English) in disclosing the purpose of remittance.

d. An under-aged person receiving funds from many legal/natural persons and/or from different locations

3. Provide special attention to the customers who received remittance from
   a. the countries which is abnormal given the market size, restricted due to security concern or where Nepali laborers/migration is nominal.

   b. high-risk jurisdiction country generally known for money laundering and terrorist financing

4.3.2 Transaction banking related

The transaction related with transaction banking might be used for layering of funds, investment in cryptocurrency, for legalizing the funds earned by evading tax. Following triggers shall assist the Bank to identify such transactions.

1. Examine the transactions of customers to ensure that the transactions are consistent with the customer's profile.
   a. Use of cards, mobile banking, internet banking, or QR banking does not consummate with the deposit product or scheme of any account.

   b. Withdrawal of funds at different ATMs.

   c. Settlement of outstanding credit card amount by cash deposit by person other than the card holder.

   d. Settlement of outstanding credit card amount by depositing significantly excess funds.

2. Any transaction in which the nature, size or frequency appears unusual
   a. Cards used by fully utilizing transaction limits each day.

   b. Cash withdrawals from a credit card in the last three consecutive months

   c. Withdrawals of fund from cards issued by foreign banks/companies using the Bank's ATM for an amount exceeding the Bank's transaction limit set for its own cards.

3. Be vigilant with the customer exhibiting following transactions:
   a. Transfer of funds to a single wallet account by more than 10 accountholders of the Bank in a day.

   b. Receipt of funds to a same account of the Bank from multiple wallets.

   c. Deposits of fund in eCom cards by non-accountholder.

   d. Use of eCom cards in high-risk jurisdiction for purchase of goods

   e. Use of a same POS issued by the Bank for the sales transaction of a same amount (in total) from a credit card (onus and offus both) in three consecutive months.

4.3.3 Wire transfers and trade related

Trade related transactions are used in an attempt to legitimize the illicit origins through the misrepresentation of the price, quantity or quality of imports or exports. The following triggers aims to help the Bank with the challenges of detecting trade-based money laundering.

1. The wire transfers of fund for trade related activities are made through two different channels – SWIFT (commonly known as T.T) and letter of credits. SWIFT transfers are made through branches supervised by Central Operations; hence the following triggers shall be monitored by Central Operations regarding SWIFT transfers.
    a. Multiple transfers sent to common beneficiary by an applicant within a short period of time.

    b. Multiple transfers sent by an applicant on the same day to different beneficiary.

    c. Identification details used when conducting international transfers – different beneficiaries having same address or phone number or email.

    d. Transfers sent to a same beneficiary for purchase (import) of same goods on the basis of multiple invoices where there are variances in unit price.

2. Central Trade Operations that look after international trade shall remain alert regarding various risks related to documents - inconsistencies, discrepancies, missing documents to identify the trade-based money laundering.
    a. Be vigilant with the customer exhibiting changes in current patterns followed by a customer:
        i. Abnormal shipping routes in comparison to the practice previously followed by the applicant or by others known to the Bank.

        ii. Letter of credit by placing 100% cash margin in cases except mandatorily required by the policy of the Bank or by regulators.

        iii. Letters of credit are frequently amended.

        iv. Significant discrepancies in description, value, quality or quantity of goods apparent on official documents (invoices, bills of lading, etc.).

    b. Any transaction in which the nature, size or frequency appears unusual
        i. A customer suddenly starts to trade in high volumes of high value goods.

        ii. A customer unexpectedly changing its transaction from established sector to a new sector.

iii. Trading in products that do not fit with the company's consistent line of business.

iv. Any transaction where identification of beneficiary Is not provided by the applicant raising suspicions towards hiding the true counter-parties, or that it deals with shadowy "trade" partners.

c. Provide special attention where there is:
   i. Over-invoicing: The exporter submits an inflated invoice to the importer, generating a payment that exceeds the value of the shipped goods. Greater value is transferred from the importer to the exporter.

   ii. Under-invoicing: The exporter submits a deflated invoice to the importer, shipping goods with greater value and transferring that value to the importer.

   iii. Multiple-invoicing: The exporter invoices multiple times for the same shipment, transferring greater value from the importer to the exporter.

   iv. Over or under shipment: The exporter ships more goods than previously agreed to with the importer, thereby transferring greater value to the importer. Alternatively, the exporter ships fewer goods than agreed, transferring greater value to the exporter.

   v. Falsely described goods and services: misrepresent the quality or type of goods or services

   vi. The products imported / exported that can be used for dual use i.e., for military or civilian purposes.

4.3.4 Credit related

Account monitoring of credit clients shall be done by respective relationship officers/relationship managers.

The Bank shall remain alert and vigilant when:

a. Customers repay problem loans unexpectedly

b. Customers make prepayment of loans or make large transaction settlement by cash.

c. High risk customers make prepayment of loans within a short period of time.

d. Borrowing request that are inconsistent with the customer's profile.

e. The source of the customer's equity contribution is unclear.

4.4 Monitoring by AML/CFT Unit

Transaction monitoring by AML/CFT Unit shall be based upon a set of transaction monitoring scenarios/rules to determine if a transaction might be suspicious through an automated AML software to enact these rules.

1. AML/CFT Unit needs to set up the rule in the AML software and based on such rules, the AML software will analyze transaction information automatically, flagging suspicious transactions for analyst review.

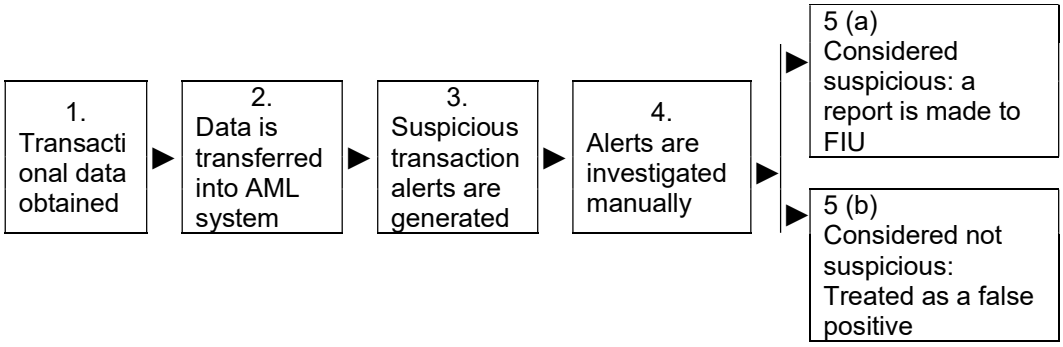
2. In setting up the rule/scenarios in the AML software, the parameters and rules shall be as decided by management level AML/CFT Committee.

3. The rules shall be used in a risk-based approach i.e., based on an assessment of risk, and implementation of a due diligence process that takes into account the risk profile of the customer.

4. AML/CFT Unit shall have to continuously optimize the rule sets based upon patterns of alerts received from the AML system so that alerts are received only on patterns that are at risk for money laundering / terrorist financing:
   a. The number of alerts generated by the AML software that do not meet the criteria for review (or false positives) are reduced

   b. Avoid to have too many risk scenarios that increases the risk of duplicate cases being generated from different scenarios for the same threat.

5. The workflow for the handling alerts generated by AML/CFT Unit shall be as illustrated hereunder.



6. AML/CFT Unit may also conduct transaction monitoring through various MIS reports of the Bank, information provided by the branches, observation made by the internal and external / statutory auditors with regard to the AML/CFT matters.

4.5 Review of KYC information

Review of the customer information is to be conducted in order to detect any suspicious transactions, reassess the level of risk associated with a customer; and determine whether transactions or activities are consistent with the customer information that the Bank has obtained.

4.5.1 Periodic review of KYC information

1. KYC information of the customers has to be updated and Customer Due Diligence to be reviewed for every customer on regular basis by branches / departments as applicable as under:

For high-risk customers	At least once a year
For medium risk customers	At least once in every five years
For low-risk customers	At least once in every six years

The time limits prescribed above would apply from the date of opening of the account or the last verification of KYC whichever is later.

2. During updating of KYC information, only the information and documents of a customer that have changed, are likely to change have to be obtained[22].

3. In addition to periodic updating, KYC information of the customers has to be updated immediately under circumstances mentioned in 1 above.

4. Updating KYC information may include all measures for confirming the identity, address and other particulars of the customer that the Bank may deem reasonable and necessary based on the risk profile of the customer.

5. In case KYC information of the customer cannot be updated in spite of all efforts, separate list of data of such customers have to be prepared by the branches.

4.5.2 Ongoing Monitoring

Ongoing monitoring consists of scrutinizing transactions undertaken throughout the course of a business relationship and Keeping documents, data or information up-to-date and relevant. The ongoing monitoring shall be conducted by first line and second line of defense as applicable.

1. Ongoing due diligence is to be carried out by considering the following triggers:
   a. High volume transactions or activity appear to be different than the expected pattern of transactions, the expected activity for a particular customer or the normal business activities for the type of product or service that is being delivered.

   b. In all transactions of high-risk customers where an apparent economic or visible lawful purpose for the transactions or activity cannot be established. The purpose may be established based on an existing customer profile or requesting additional information from a customer.

   c. Transactions conducted outside of the normal course of business or where the method of payment/receipt is not usual business practice.

   d. Transactions conducted are unusual in themselves

[22] Unified Directive 2078, Directive 19 clause 8 (4)

i. Where no rational or logical explanation can be provided by the customer.
ii. loss-making transactions where the loss is avoidable
iii. dealing with money or property when there are suspicions of tax evasion

2. Ongoing monitoring may involve both real time and post event monitoring. Real time monitoring will focus on transactions and activity when information or instructions are received from a customer, before or as the instruction is processed. Post event monitoring may involve end of day, weekly, monthly or annual reviews of customer transactions and activity.

3. The ongoing monitoring of transactions or activity may also be conducted either by customer facing employees, or by an independent reviewer. In any case, the examiner must have access to all customer records.

4.6 Correspondent banking relationships

Correspondent banking relationships are recognized globally as being vulnerable to exploitation for money laundering and terrorism financing purposes as correspondent banks often have limited information about the nature or purpose of the underlying transactions, particularly when processing electronic payments.

AML/CFT Unit shall conduct review of correspondent banking relationship from ML/TF risk perspective at least once a year. For this, AML/CFT Unit shall review The Wolfsberg Group Wolfsberg Correspondent Banking Due Diligence Questionnaire of the correspondent bank or AML questionnaire of the Bank to assess the AML controls and related risk of such banks.

Treasury and Correspondence Department shall be responsible to update the information and documents as applicable in line with Corresponding Banking Policy (January 2020 of the Bank).

4.7 Relationships with remittance companies

Several features of the remittance companies make them an attractive vehicle through which criminal and terrorist funds can enter the financial system, such as the simplicity and certainty of remittance transactions, worldwide reach, the cash character of transactions etc. Remittance Department shall conduct review of relationship with such companies.

4.8 Introduction of New Technology

New technologies for AML/CFT refer to an innovative skills, methods, and processes that are used to achieve goals relating to the effective implementation of AML/CFT requirements or innovative ways to use established technology-based processes to comply with AML/CFT obligations.

New technologies seek to improve the speed, quality, or efficiency and cost of some AML/CFT measures, compared to the use of traditional methods and processes. Many of these new technologies' capabilities and implications are still largely unknown. That said, it is essential to understand their current capabilities and potential impact on AML/CFT.

In implementing technologies that affect AML/CFT program of the Bank, Information Technology and Digital Banking Department shall:

1. Ensure Privacy and Data Protection when implementing new technologies.

2. Identify explicit, well-defined uses of new technologies for AML/CFT supervision and examination

3. Understand the risks and benefits associated with new technologies, and appropriate risk-mitigation measures that preserve their benefits

4. The AML/CFT solution has explainability and transparency of processes and outcomes; oversight by humans; strong cybersecurity; and alignment with technical standards and best practices.

RECORD KEEPING AND REPORTING

The Bank shall maintain records in an efficient, secured and cost-effective manner so that identification and retrieval of records by branches/ offices of the Bank are facilitated to meet the operational, business, legal, statutory and decision/policy making requirements in the course of the pursuit of the Bank's mission.

5.1 Record keeping

1. The Bank shall have to maintain records, as under, accurately and securely for minimum five years after the termination of business relationship or from the date of transaction or from the date of occasional transaction[23]:
   a. All documents and records related to identification and verification of customer and beneficial owner,

   b. All documents, records and conclusion of the analysis of customer or beneficial owner and transaction,

   c. All documents, details and records related to accounting and business relation of the Bank

   d. All documents, details and records relating to domestic and foreign transactions,

   e. All documents, details and records of attempted transactions,

   f. All other documents, details and records as prescribed by regulators.

2. The documents specified in Annex 2 of this Policy, shall be retained/preserved, as the case may be, in physical form (Hard Copy) and/or electronic/digital form (Soft Copy in E-kagaj/DMS/any other platform used by the Bank) or both.

3. The preservation of documents should be such as to ensure that there is no tampering, alteration, destruction or anything which endangers the content, authenticity, utility or accessibility of the document.

4. The documents must be accessible at all reasonable times.

5. The Bank shall maintain record of documents for a period as mentioned in the Record Management and Retention Guideline of the Bank or for five years whichever is longer. Any documents that are not mentioned in the Record Management and Retention Guideline of the Bank shall have to be maintained for a minimum period of five years from the date of end of relationship.

6. It is imperative that factual information such as names, citizenship numbers, registration numbers, etc. recorded in the system is accurate.

[23] Asset (Money) Laundering Prevention Act, 2008 Clause 7(DA)

7. All spellings and transcriptions in the accounts should be accurately recorded in system.

5.2 Reporting to Financial Intelligence Unit (FIU)

In line with Asset (Money) Laundering Prevention Act, 2008 and provisions in Unified Directive, AML/CFT Unit is obliged to provide the following reports to the Financial Intelligence Unit (FIU-Nepal).

SN	Name of Report	Deadline
1	Threshold Transactions Reports (TTRs)	Within 15 days of transaction
2	Suspicious Transactions Reports (STRs/SARs)	Within three days or earlier
3	Quarterly risk assessment report (Annexure-19.2)	within 15 days from the end of each quarter

5.2.1 Threshold Transactions Reports (TTR)

1. A Threshold Transaction Report is a report that the Bank is required to file with FIU for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through or to the financial institution which involves a transaction in currency of NPR 1 million (NPR 0.5 million in case of foreign currency exchange) and above.

2. The Bank needs to segregate TTR into three sub categories viz. TTR-Cash, TTR-Cross Border and TTR-FCY Exchange and submit it to FIU through goAML software.

3. The nature of transaction that needs to be reported shall be as mentioned in Unified Directive.

5.2.2 Suspicious Transactions Report (STR)

Suspicious Transactions are financial transactions in which there are reasonable grounds to suspect that, the funds involved are related to the proceeds of criminal activity[24].

1. The Bank shall make a suspicious transaction report to the FIU within three days or earlier in case of following circumstances in relation to any customer, transaction or property[25].

   a. If it suspects or has reasonable grounds to suspect that if the property is related to ML/TF or other offence, or

   b. If it suspects or has reasonable grounds to suspect that the property is related or linked to, or is to be used for, terrorism, terrorist, terrorist acts or by terrorist organization or those who finance terrorism.

2. The Bank shall submit the suspicious activity report to FIU if the activity of the customer is suspicious and actual transaction has not taken place and in case of attempted transaction[26].

3. Suspicious Activity arises from suspicion relating to general behavior of the person in question which creates the knowledge or belief that he or she may be involved in illegal activities out of which proceeds might be

[24] Guidelines for Suspicious Transactions Reporting (STR), January, 2020
[25] Asset (Money) Laundering Prevention Act, 2008 clause 7(DHA) (1)
[26] Asset (Money) Laundering Prevention Act, 2008 7(DHA) (2)

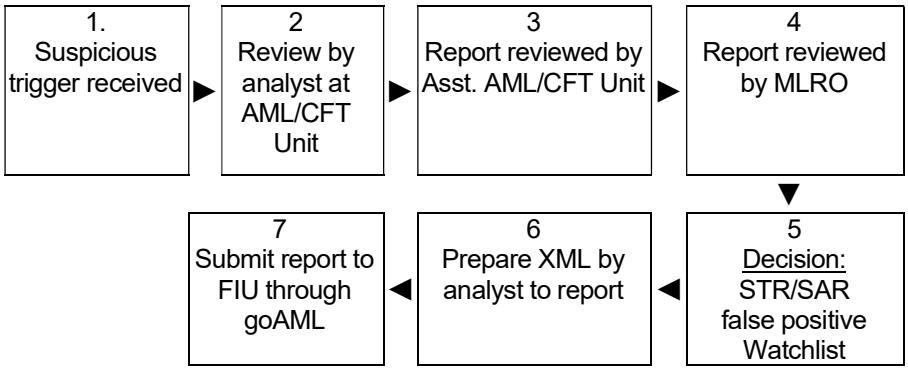
generated. Any suspicious attempted transaction also falls in this category.

4. The triggers that help to identify suspicious transactions shall be as guided by "Guidelines for Suspicious Transactions Reporting (STR), July 2021" issued by FIU, Nepal and any update thereon.

5. Submission of the information/ report of suspicious transaction and activity by any staff of the Bank shall be kept confidential. The Bank shall take due care in ensuring that customers are neither told nor inferred that the Bank is looking at their transactions / activity with suspicion.

6. Branches /Departments are required to report all suspicious transactions and activity to the Manager-AML/CFT, AML/CFT Unit, Corporate Office, immediately by mentioning Customer name, account no. and reasons for considering the transaction suspicious as per annex 9.

7. The analyst in AML/CFT Unit analyzes the suspicious activity in the format as per annex 7 where the transactions shall be preliminarily analyzed based on proximity of branch from business/current address of the customer, type of transaction (cash, digital, and clearing), trend of withdrawals and deposits and transaction conducted from account maintaining branch/ other branches. Upon this, the decision to file suspicious transaction/activity, hold as watchlist for a certain period of time due to lack of adequate information / documents, or mark as false positive is taken and a report is prepared. In the course of analysis, the analyst may seek information, details or documents from the concerned employees/branches/offices/ department through phone, email or any other suitable means, which the concerned shall have to respond promptly. Once the report is prepared, it shall be further assessed by an authorized official of AML/CFT Unit and then by Manager-AML/CFT for making final decision. The workflow for STR/SAR shall be as under:



8. The Bank shall follow the Suspicious Transaction Reporting & Suspicious Activity Reporting (STR/SAR) Guidelines issued from time to time by FIU for filing STR/SAR.

9. Manager-AML/CFT shall act as compliance officer to report STRs and to deal with FIU on matters relating to STRs.

5.2.3 Quarterly risk assessment and review report

Quarterly Risk Assessment and review report in the prescribed format shall be prepared and submitted by AML/CFT Unit to FIU and Supervision Department of Nepal Rastra Bank within 15 days from the end of each quarter.

5.3 Reporting to Nepal Rastra Bank

Following reports shall have to be prepared and submitted to supervision Department of Nepal Rastra Bank.

SN	Name of Report	Deadline
1	Self-assessment questionnaire on AML/CFT risk management	Within 15 days of year end
2	ML/TF risk assessment report	Within first quarter end
3	Quarterly risk assessment report (Annexure-19.2)	Within 15 days of quarter end
4	Offsite data collection (NRB14)	Within 15 days of half year end

5.4 Reporting to Management/ Board level committees

1. AML/CFT Unit shall have to put up implementation report concerning status of compliance of AML/CFT guidelines as per the ALPA, ALPR, NRB Directives and Bank's policy at least at the quarterly meetings of management level AML/CFT Committee and board level Asset (Money) Laundering Prevention Committee.

2. Upon requirement, AML/CFT Unit shall put up the report of compliance status of AML/CFT guidelines to these committees at any time.

ROLE AND RESPONSIBILITIES

Role and responsibilities of various authorities in regard to AML/CFT in the Bank shall be as under:

6.1 Board of Directors

1. Board of the Directors of the Bank shall oversee the formulation of the internal policy for compliance of AML/CFT provisions as per Asset (Money) Laundering Prevention Act, 2008 Asset (Money) Laundering Prevention Rule, 2009, and NRB Directives applicable to the Bank.

2. The BOD shall carry out the review of the report submitted by Asset (Money) Laundering Prevention Committee with regard to AML/CFT and activities carried out thereon.

6.2 Asset (Money) Laundering Prevention Committee

1. Asset (Money) Laundering Prevention Committee constituted in line with NRB Directives. This committee shall oversee AML/CFT implementation status of the Bank and further report at least once in every three months for review of the same to BOD.

2. The committee shall provide necessary suggestion, feedbacks, instructions to the Management for compliance of AML/CFT provisions in the Bank and enrichment of compliance status and compliance culture.

3. The Terms of Reference (TOR) of the Committee shall be as per Unified Directive, Directive 6 issued by NRB on Corporate Governance.

6.3 AML/CFT Committee

1. AML/CFT Committee shall supervise and guide all of the Bank functions regarding implementation of AML/CFT Policy and guidelines of the Bank.

2. It shall analyze the gap if any in regard to compliance to AML/CFT provisions and provide suggestion, feedback and instruction for the compliance of the same.

6.4 Chief Risk Officer

1. CRO shall have to monitor operating effectiveness of mitigating controls and conduct assessment of the residual risk, which considers the effectiveness/status of the controls against the ML/TF risks of the Bank.

2. CRO to communicate the Bank's risk appetite so that the residual risk can be maintained within the Bank's risk appetite.

3. CRO shall communicate to the top management and the Board level committee towards managing the ML/TF risk. CRO shall ensure reports on the status of AML/CFT Policy are placed to the Board through Asset (Money) Laundering Prevention Committee.

6.5 Chief Compliance Officer

1. Chief Compliance Officer, a senior management level official and shall be responsible for effective implementation of the policies and guidelines/manuals, in all areas within the Bank.

2. CCO shall ensure that any policies, product papers, manuals, guidelines/ procedures and other documents are in line with AML/CFT Policy of the Bank.

6.6 Chief Operating Officer

1. COO shall be responsible for establishing proper implementation mechanism of checks/control as per this Policy across the Bank.
   a. Develop forms/formats as required

   b. Develop operational procedure for implementation of AML/CFT Policy

2. COO shall provide appropriate instructions and guidance to the Branches/offices/ Departments to follow and comply with the process system as required to comply in relation to AML/ CFT policies of the Bank and NRB Directive.

6.7 Manager-AML/CFT

1. Manager-AML/CFT shall act as focal person to comply with the obligations pursuant to the Bank's AML/CFT policy and shall directly report to Chief Risk and Compliance Officer.

   MLRO shall have access to any customer / transaction records, financial documents; and right to ask and obtain any information from the concerned staffs of the Bank and to perform any task to implement the provision laid down by ALPA, Rules and NRB Directive[27]. The MLRO may take specialized service from the heads of all other departments as required[28].

2. The Bank shall report name, address, qualification, contact number, email address etc. of the Manager-AML/CFT to FIU-Nepal and Bank Supervision Department of NRB and report all such details of new incumbent in case of change[29].

3. The Bank shall ensure following functions, rights and duties:
   a. Drafting policy, procedures and guideline for effective compliance of AML/CFT provisions.

   b. Analyzing and investigating the information related to suspicious and unusual activities received from departments, officials and employees.

   c. Seeking for and obtaining the service of experts from any department/officials and/or necessary data, information, details or documents from concerned employee of the Bank.

4. Monitoring the compliance of the AML/CFT provisions as stipulated the Bank's AML/CFT policy.

[27] Asset (Money) Laundering Prevention Act, 2008 – Chapter 3, Clause (7)(TA)(4)
[28] Unified Directive, 2078, directive no. 19/078 clause 18 (3)
[29] Unified Directive, 2078, Directive 19 Clause 18 (2)

5. Recommending for departmental punitive action to the officials or employees who do not submit data, information, details, records or documents sought in the course of fulfilling the obligations[30].

6. Interaction with Branch/Department AML Officer in Branches / Offices / Departments for ensuring full compliance with the Policy.

7. Communicate and respond to the inquiry received from FIU as per the provision in law.

8. Ensuring submission of periodical reports related to AML/CFT to BOD through Asset (Money) Laundering Prevention Committee[31].

9. Performing other AML/CFT related functions as prescribed by FIU and the management of the Bank.

6.8 Branch / Department AML Officer

1. Each Department/Province Office/ branch will designate an official as Branch/Department AML Officer who would ensure compliance of AML/CFT policy in their department/office/branch.

2. Branch/Department AML Officer shall be the focal person for the respective department/office/branch and shall have the responsibility of ensuring compliance to AML/CFT provisions while establishing any business relation at their Department/Office/branch from AML/CFT perspective.

3. Branch/Department AML Officer shall report to the AML/CFT Unit.

4. Branch/Department AML Officer shall monitor customer activities/ transactions on ongoing basis, carry out customer due diligence and enhanced due diligence as required.

5. Branch/Department AML Officer shall carry out investigation/ analysis in relation to any suspicious activity detected by them or reported by others at their branch/ office/department so as to report the same to AML/CFT Unit.

6.9 Province Head

1. Head-Province Office shall ensure compliance with the AML/CFT measures at province office

2. Head-Province Office shall monitor the AML/CFT compliance status of the branches under the province.

3. Head-Province Office shall have to ensure prompt reporting of suspicious transactions at the province office to the AML/CFT Unit.

4. During branch visit, Head-Province Office shall verify compliance status of AML/CFT measures of the branches and suggest appropriate actions to the branches for improving compliance of AML/CFT matters.

[30] Unified Directive, 2078, Directive 19 Clause 18 (5)
[31] Unified Directive, 2078, Directive 19 Clause 18 (6)

5. Head-Province Office shall coordinate with AML/CFT Unit and/or Human Resources Department for conducting trainings on AML/CFT matters.

6.10 Branch managers and department heads

1. Branch Manager and department heads shall ensure that AML/CFT provisions as per prevailing rules and regulations and Bank's internal policy and procedures are complied with at the branch/department.

2. Branch Manager and department heads shall ensure that the relevant KYC information/documents are obtained from the customers so as to identify and verify the customer.

3. Branch Manager and department heads shall ensure proper due diligence has been carried out and provisions of AML/CFT guidelines have been complied with before establishing business relation.

4. Branch Manager and department heads shall ensure that the transactions of the customers are being monitored and all unusual/ suspicious transaction/ activity have been reported. Branch manager and department heads shall ensure that the branch/department is capable of providing any information and reports sought by AML/CFT Unit on priority basis

5. Branch Manager and department heads shall analyze the observations of internal audit, all other inspection reports pertaining to AML/CFT measures of the branch/department and initiate appropriate corrective actions if required.

6.11 Customer Service Desk staff and relationship officers/managers

1. To verify customer details / profile.

2. To exercise required and proper due diligence of the customer.

3. To adhere to the provisions of the Bank's policy and guideline in relation to opening of account/establishing a relationship.

4. To comply with the guidelines issued by the Bank from time to time in respect of establishing relationship / opening and conduct of account.

6.12 Internal Auditor

1. Internal audit shall focus on an assessment of the design of policies, procedures, controls, and systems to ensure that they meet the regulatory requirements, and are in line with best practices and with the risk appetite of the Bank.

2. Internal audit shall also review the implementation of the Bank's policies and procedures by the first line of defense, to ensure that the controls designed by management are implemented in practice and that the controls are effective in mitigating the risk.

3. Internal audit shall also cover the oversight and checks carried out by the second line of defense.

4. Whilst preserving independence, internal audit should work together with management and the relationship between the two should be built on mutual

trust. For this discussing findings and remediation plans during the course of the audit shall be made with AML/CFT Unit from time to time.

6.13 All Employees of the Bank

1. It is the responsibility of each and every staff of the Bank to understand the AML/CFT provisions applicable to their area of operation.

2. Comply with AML/CFT policy and procedures.

3. Be alert at all times due to possibility of money laundering and reporting all suspicious or unusual transactions.

MISCELLANEOUS

7.1 Capacity Enhancement program for Board Members & Top Management

The Bank shall arrange knowledge sharing programs on AML/CFT for capacity enhancement of Board members, top management and shareholders having 2% or more share of paid-up capital.[32]

7.2 Know your employee

Human Resource Department shall conduct code of conduct of every employee as per Personnel Policy Guidelines and Know Your Employee (KYE) procedure and maintain up-to-date information of each employee. The HRD shall also monitor the transaction of the employees and report to MLRO upon observing suspicious nature of activities related to ML/TF for reporting to FIU wherever required.

7.3 Employee training

1. Ongoing employee training shall be conducted so that staff members are adequately trained in AML/CFT policy and procedures. All employees shall be provided with AML/CFT training at least once a year through appropriate means.

2. Human Resources Department shall have to conduct AML/CFT trainings at regular intervals as per their training calendar. AML/CFT Unit shall provide necessary inputs in regard to content of the training program. External as well as internal resource persons shall be utilized for training based on the assessment of training need.

3. Both onsite/offsite visits shall be conducted by the AML/CFT Unit to check/monitor the activities and to create awareness in aspects relating to AML/CFT. Feedback of onsite visits shall be submitted to the Chief Compliance Officer for review.

4. More extensive training including foreign training shall also be provided to staff in the AML/CFT Unit and other AML/CFT relevant staff. The training shall be conducted in coordination with Training and Development, Human Resource Department.

5. Records of all training given to staff shall be kept including the date and nature of the training along with names of the resource person and staff attending the training by Human Resource Department.

7.4 Failure to Comply

1. Concerned staffs who fail to comply with the AML/CFT policy and guideline, report unusual and suspicious transactions shall be warranted disciplinary action in accordance with the prevailing act, regulations and internal policy of the Bank.

2. All staffs are encouraged for whistle blowing of any wrongdoing or sense of wrongdoing activity that is associated with corruption or unethical behavior

[32] Unified Directive, 2078 Directive 19 clause 18 (7)

causing loss to the Bank or non-compliance, through Branch/Department AML/CFT Officer or directly to MLRO.

7.5 Not to be Liable for Providing Information

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

7.6 Tipping Off

1. Information provided to the regulator or information disseminated by any staff/representative while working in normal course of work or at the time of providing information to authorized investigating unit shall not be disclosed to anybody except mandatory disclosure as per the prevailing act, Law etc.

2. Employee who tips off the customer that their account is under surveillance shall be punishable as per the prevailing act/law/rule/regulation and the Bank's policy and procedures.

3. Tipping off shall be considered under following act performed by any staff of the Bank:
   a. Inform/warn the customer about the suspicion.

   b. Talk/disclose with other employees and friends/ family.

   c. Discuss in unrelated meeting.

4. In the course of obtaining information/details from the customer in regard to any suspicious activity/ transaction, concerned staff should use proper discretion to evade the risk of realizing the same by the customer.

7.7 Penalty for Non-adherence of AML/CFT Policy/ Guideline/ Act/Rule

1. Penalties may be imposed to the Bank as well as concerned staff of the Bank as per the provisions of Asset (Money) Laundering Prevention Act, 2064 and NRB Directive for non-compliance of the provisions related to AML/CFT. Therefore, employees shall strictly comply with the Policy and Guidelines prescribed herein while performing the assigned job.

2. The concerned staff shall be punishable as per the prevailing law and the internal regulation of the Bank if any penalty imposed to the Bank by the regulator due to violation of AML Act/Rule. Manager-AML/CFT shall have the authority to recommend suitable action for such staffs failing to adhere with this Guideline.

7.8 Prevention and Cancellation

1. This Guideline is intended to supplement AML/ CFT Policy of the Bank and Asset (Money) Laundering Prevention Act, 2008, Asset (Money) Laundering Prevention Rule, 2009 and prevailing directives issued by NRB. The provision of the Act/Directives shall prevail if any Act/Directive contradicts with this Guideline.

2. The directives/circulars/guidelines issued by NRB from time to time on AML/KYC-Due Diligence shall prevail and be regarded as the integral part of this Guideline.

3. The interpretation and elaboration of the provisions in this Guideline, where necessary, shall rest on CEO after recommendation from CCO.

4. CEO may waive any provision or clause of this Guideline in exceptional cases subject to condition that such waiver does not violate any Act, Rules or NRB Directives.

7.9 Amendment

This guideline shall be revisited annually under the supervision of CRO subject to the prevailing rules and regulations of the country and of the regulator. This Guideline shall supersede previously issued internal circulars issued by AML/CFT Unit related to AML/CFT issues. Furthermore, this Guideline shall be amended as and when required due to change in national and international norms, practices, regulations on AML/CFT with approval of CEO as per the recommendation of the AML/CFT Committee.

GLOSSARY

Alert

A review based on underlying red flags that requires analyst attention. Within know-your customer procedures, alerts are potential discrepancies that are flagged, either manually or through an automated system, based on defined red flags and underlying typologies.

AML/CFT Implementation Report

A collection of information about the current status of AML/CFT program of the Bank.

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

AML/CFT is a term used in the financial and legal industries to describe the legal procedures/controls that requires financial institutions and other regulated entities to prevent, detect, and report ML/TF activities.

Asia/Pacific Group on Money Laundering (APG)

Asia/Pacific Group on Combating Money Laundering - a FATF-style regional body for the Asia/Pacific region, which defines regional AML/CFT policy in accordance with 40 FATF Recommendations.

Asset

Anything an individual or legal entity owns that has a monetary value. Fixed assets are those items, such as buildings and equipment, that will be used over a period of time; current assets include raw materials, cash, and any money other parties owe to the individual or legal entity.

Asset Freezing

The prevention of a person targeted by sanctions from accessing or using his or her bank account and other financial assets. Asset freezing is also referred to as blocking an asset.

Batch Screening

The process of screening the Bank's existing customer base and other associated entities, such as Directors, Proprietor, Beneficial Owner, Signatory, with Automated Screening Tools on a periodic basis.

Bearer Share

Negotiable instruments that accord ownership in a corporation to the person who is in physical possession of the bearer share certificate, a certificate made out to "Bearer" and not in the name of an individual or organization.

Beneficial Owner

The term beneficial owner is the natural person who ultimately owns or controls an account through which a transaction is being conducted or the natural persons who have significant ownership of, as well as those who exercise ultimate effective control over, a legal person or arrangement.

Beneficiary

The person (natural or legal) who benefits from a transaction, such as the party receiving the proceeds of a wire transfers. In case of trust, the beneficiaries are the people who benefit from the trust

Cash Deposits

Sums of currency deposited in one or more accounts at a financial institution.

Cash-Intensive Business

Any business in which customers usually pay with cash for the products or services provided, such as restaurants, coin-operated machines or car washes. Some money launderers run or use cash-based businesses to commingle illegally obtained funds with cash actually generated by the business.

Complex business structure

A company that does not have immediate transparency of ownership and/or control.

Correspondent Banking

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 hundreds of 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 wire transfers of funds, check clearing services, payable-through accounts and foreign exchange services.

Counterparty

The other side of a transaction—the seller where one's customer is the buyer, or vice versa.

Criminal Proceeds

Any property derived from or obtained, directly or indirectly, through the commission of a crime.

Cross Border

Used in the context of activities that involve at least two countries, such as wiring money from one country to another or taking currency across a border.

Crypto/Virtual Currency

A medium of exchange that operates in the digital space that can typically be converted into either a fiat (e.g., government issued currency) or it can be a substitute for real currency.

Customer Due Diligence

A set of internal controls that enable a financial institution to establish a customer's identity, predict with relative certainty the types of transactions in which the customer is likely to engage, and assess the extent to which the customer exposes it to a range of risks (i.e., money laundering and sanctions). As such, they constitute an essential part of sound risk management.

Customers

Customers of the bank shall denote:

a) A person or entity that maintains an account with the Bank and/or has business relationship with the Bank.

b) A person on behalf of whom an account is maintained i.e., beneficial owner.

c) Any person or entity connected with the financial transaction that may impose significant reputational or other risks to the Bank.

Delivery Channels

The ways in which products and services are provided by the Bank to its customer.

Designated Non-Financial Businesses and Professions

FATF recommends certain standards apply to non-financial businesses and professions, including specifically: casinos, real estate agents, dealers in precious metals and precious stones, trust and company service providers who prepare or carry out certain duties on behalf of their clients

Domestic PEPs

PEPs located in the same country as the financial institution of which it is a client and has a domestically located position.

Dual-Use Goods

The products or technology that can be used for either military or civilian purposes. Most often, in diplomatic and political platforms, these are goods that can serve multiple uses at one time. An example is missile technology, which can be used for both scientific research and military action.

Due Diligence

The investigation and examination of a company or group, conducted in the process of preparing for a business transaction. Due diligence should be completed before entering into any financial transaction or business relationship.

Enhanced Customer Due Diligence

ECDD calls for additional measures aimed at identifying and mitigating the risk posed by higher risk customers. It requires developing a more thorough knowledge of the nature of the customer, the customer's business and understanding of the transactions in the account

than a standard or lower risk customer.

European Union

The modern EU was founded in the Treaty of Maastricht on European Union, signed in 1992 and effective in 1993. The EU is a politico-economic union of member states located primarily in Europe.

Event-Triggered Monitoring

An internal control used to mitigate sanctions risks. Event-triggered monitoring occurs whenever relevant information about an existing customer change, therefore requiring an interim review of information prior to a scheduled review.

False Positive

A hit identified during the screening process as a possible alert, but when reviewed, is found not to be a match to a target named on a sanctions list.

Financial Action Task Force

FATF was chartered in 1989 by the Group of Seven industrial nations to foster the establishment of national and global measures to combat money laundering. It is an international policy-making body that sets anti-money laundering standards and counter-terrorist financing measures worldwide.

Financial Intelligence Unit

Financial Intelligence Unit (FIU) 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 ML and TF activities to the Investigation Department, other relevant law enforcement agencies and foreign FIUs. The FIU was established on 21 April, 2008 under the section 9 of the Asset (Money) Laundering Prevention Act, 2008 with the Nepal Rastra Bank as an independent unit.

Financing of Terrorism

Financing of Terrorism involves the solicitation, collection or provision 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.

First Line of Defense

Within the governance structure of a sanctions compliance program, the first line of defense (also referred to as the "front line") includes relationship managers and other customer-facing employees who are closest to the customers and counterparties during the onboarding and contracting phase of relationships. The first-line defense is responsible for ensuring that adequate information is obtained so that effective screening of customers and their owners and controllers can be performed. In general, the first-line defense owns and manages the collection of SDD information.

Foreign PEPs

PEPs on behalf of a government that differs from the government's public position in which the financial institution is located.

Freeze

To prevent or restrict the exchange, withdrawal, liquidation, or use of assets or bank accounts. Frozen property, equipment, funds or other assets remain the property of the natural or legal person(s) that held an interest in them at the time of the freezing and may continue to be administered by third parties. The courts may decide to implement a freeze as a means to protect against flight.

goAML

The goAML application is a fully integrated software solution developed specifically for use by Financial Intelligence Units and is one of United Nations Office on Drugs and Crime 's strategic responses to financial crime, including money-laundering and terrorist financing.

Inherent Risk

The level of sanctions risks that exists before controls are applied to mitigate them. There are four main inherent risk categories: customers, products and services, countries, and delivery channels. Inherent risk is linked to the risk assessment process, which evaluates the effectiveness of an institution's risk controls. Inherent risk considers the likelihood and impact of noncompliance prior to considering any mitigating effects of risk management processes.

Integration

The integration phase, often referred to as the third and last stage of the classic money laundering process, places laundered funds back into the economy by re-entering the funds into the financial system and giving them the appearance of legitimacy.

International PEPs

PEPs on behalf of an international organization (such as World Bank, IMF, UN etc.).

Jurisdiction

The country (or countries, in the case of dual citizenship) in which an individual is a legal citizen.

Know Your Customer

Know Your Customer is the process of establishing the identity of customer, understanding the nature of customers' activities and qualify that the source of funds is legitimate and assessment of money laundering risks associated with customers.

Layering

This is the second stage where the origins of the funds are concealed by moving them around in a series of complex bank transfers or financial transactions to distance the money from its illegal source.

Material change

A material change is an event, activity, or situation that the Bank identifies during interactions with its customer (or via ongoing customer due diligence and account monitoring) that could change the level of ML/TF risk.

Money Laundering

Money laundering refers to financial activities designed to conceal the proceeds, sources or nature of the illicit activities in making the money generated appear to have come from a legitimate source.

Money Laundering Reporting Officer (MLRO) (Manager-AML/CFT)

A term used in various international rules to refer to the person responsible for overseeing a firm's anti-money laundering activities and program and for filing reports of suspicious transactions with the national FIU. The MLRO is the key person in the implementation of anti-money laundering strategies and policies.

Money Services Business

A person (whether a natural or legal person) engaged in dealing in foreign exchange, check cashing, providing or selling prepaid access, money transmission where it exceeds the applicable regulatory threshold, at which point the person is generally deemed to be a financial institution subject to AML obligations.

Monitoring

An element of an institution's anti-money laundering program in which customer activity is reviewed for unusual or suspicious patterns, trends or outlying transactions that do not fit a normal pattern. Transactions are often monitored using software that weighs the activity against a threshold of what is deemed "normal and expected" for the customer.

Multiple Accounts

The act of opening several bank accounts by criminals using stolen or fake identities or accounts belonging to legitimate customers who have allowed criminals to use their account for illegitimate reasons.

Name Screening

The process of matching an internal record (i.e., customer, counterparty, related account party) against a sanctioned list record, either manually or through an automated screening tool. Name screening may also include batch name screening, which allows a firm to screen its entire customer base using automatic screening tools on a periodic basis.

Nested Account

The use of a bank's correspondent relationship by a number of underlying banks or financial institutions through their relationships with the correspondent bank's direct customer. The underlying respondent banks or financial institutions conduct transactions and obtain access to other financial services without being direct customers of the correspondent bank.

Non-Governmental Organization

Not for profit organizations that are not directly linked to the governments of specific countries, and perform a variety of service and humanitarian functions, including bringing citizen concerns to governments, advocating for causes and encouraging political participation.

Non-Profit Organizations

These can take on a variety of forms, depending on the jurisdiction and legal system, including associations, foundations, fund-raising committees, community service organizations, corporations of public interest, limited companies and public benevolent institutions.

Office of Foreign Assets Control

The agency within the US Department of the Treasury responsible for administering and enforcing economic sanctions issued as part of US foreign policy and by international organizations like the United Nations against targeted foreign countries. It often works in consultation with other agencies, such as the Department of State, to oversee national security goals. A core component of the agency's responsibilities is the creation and maintenance of the Specially Designated Nationals (SDN) list.

Offshore

Literally, away from one's own home country—if one lives in Europe, the U.S. is "offshore." In the money laundering lexicon, the term refers to jurisdictions deemed favorable to foreign investments because of low or no taxation or strict bank secrecy regulations.

Originator

The account holder or, where there is no account, the person (natural or legal) which places the order with the financial institution to perform the wire transfer.

Payable Through Account

Transaction account opened at a depository institution by a foreign financial institution through which the foreign institution's customers engage, either directly or through subaccounts, in banking activities and transactions in such a manner that the financial institution's customers have direct control over the funds in the account.

Payment Screening

A method of screening that focuses on screening payment messages. Unlike name screening, payment screening takes place with current customers and is performed before a payment or message is processed. Payment screening relies on payment messages using predefined templates, codes, and acronyms to describe certain information. The information provided in these predefined templates is typically provided by a third party; therefore, the firm has little, if any, control over how the data is presented.

Placement

The first phase of the money laundering process: The physical disposal of proceeds derived from illegal activity.

Politically Exposed Person

A PEP is an individual who has been entrusted with prominent public functions in a foreign country, such as a head of state, senior politician, senior government official, judicial or military official, senior executive of a state-owned corporation or important political party official, as well as their families and close associates. Various country regulations will define the term PEP, which may include domestic as well as foreign persons.

Predicate Crimes

"Specified unlawful activities" whose proceeds, if involved in the subject transaction, can give rise to prosecution for money laundering. Most anti-money laundering laws contain a wide definition or listing of such underlying crimes. Predicate crimes are sometimes defined as felonies or "all offenses in the criminal code."

Private Investment Company

Also known as a Personal Investment Company, a PIC is a type of corporation that is often established in an offshore jurisdiction with tight secrecy laws to protect the privacy of its owners. In some jurisdictions, an international business company or exempt company is referred to as a private investment company.

Proliferation Financing

Proliferation Financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials that would contribute to the Weapons of Mass destruction proliferation (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Red Flag

A warning signal that should bring attention to a potentially suspicious situation, transaction or activity.

Regulatory Agency

A government entity responsible for supervising and overseeing one or more categories of financial institutions. The agency generally has authority to issue regulations, to conduct examinations, to impose fines and penalties, to curtail activities and, sometimes, to terminate charters of institutions under its jurisdiction.

Related persons

Proprietor, partners, board of directors, executive / management committee members, chief executive officer, and account operators of a firm, company and trust as appropriate.

Remittance Services

Remittance services are businesses that receive cash or other funds that they transfer through the banking system to another account. The account is held by an associated company in a foreign jurisdiction where the money is made available to the ultimate recipient.

Residual risk

This is the assessed ML/TF risk after AML/CFT controls and measures have been put in place.

Respondent Bank

A bank for which another financial institution establishes, maintains, administers or manages a correspondent account.

Risk Appetite

The amount of risk that a firm is willing to accept in pursuit of value or opportunity. A firm's risk appetite reflects its risk management philosophy and comfort level for undertaking business in situations in which there could be an elevated sanctions risk. In turn, risk appetite influences the firm's culture and operating style and guides resource allocation. An organization's risk appetite is determined through the risk-assessment process and formalized in a Risk Appetite Statement or Framework. A business should determine its risk appetite based on the resources it has to invest in controls, staffing, and measures to protect its reputation. Firms can have an overarching risk appetite (i.e., enterprise-wide) and/or have risk appetites defined on a more granular level (e.g., by department).

Risk Assessment

A tool that allows a business to identify and assess the extent to which it may be exposed to risks. In global banking, risk assessments form the foundation of a sound sanctions compliance program.

Risk-Based Approach

The assessment of the varying risks associated with different types of businesses, clients, accounts and transactions in order to maximize the effectiveness of an anti-money laundering program.

Sanctions

Sanctions are punitive or restrictive actions taken by individual countries, regimes, or coalitions with the primary purpose of provoking a change in behavior or policy.

Sanctions List

A document or database listing individuals, legal entities, and countries with whom it is illegal to do business.

Second Line of Defense

In general, the second line exists to ensure that CDD procedures and processes applied by the first line are designed properly, firmly established, and applied as intended. The second-line defense reviews the effectiveness of controls used to mitigate ML/FT risks;

provides information to the first line; and investigates possible noncompliance with sanctions restrictions.

Settlors

Persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trust's assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes done with the assets.

Shell Bank

Bank that exists on paper only and that has no physical presence in the country where it is incorporated or licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.

Shell Company

A company without active business or significant assets. Shell companies are legal, but people sometimes use them illegitimately—for instance, to disguise business ownership.

Smurfing

A commonly used money laundering method, smurfing involves the use of multiple individuals and/or multiple transactions for making cash deposits, buying monetary instruments or bank drafts in amounts under the reporting threshold. The individuals hired to conduct the transactions are referred to as "smurfs".

Specially Designated Nationals and Blocked Persons List (SDN List)

A list of individuals and companies, published by OFAC, that are owned, controlled by, or acting on behalf of a targeted country. The list also includes groups and people, such as terrorists or drug traffickers, who are associated with a specific crime as opposed to a country.

Structuring

Illegal act of splitting cash deposits or withdrawals into smaller amounts, or purchasing monetary instruments, to stay under a currency reporting threshold. The practice might involve dividing a sum of money into lesser quantities and making two or more deposits or withdrawals that add up to the original amount. Money launderers use structuring to avoid triggering a filing by a financial institution. The technique is common in jurisdictions that have compulsory currency reporting requirements.

Suspicious Activity

Irregular or questionable customer behavior or activity that may be related to a money laundering or other criminal offense, or to the financing of a terrorist activity. May also refer to a transaction that is inconsistent with a customer's known legitimate business, personal activities, or the normal level of activity for that kind of business or account.

Suspicious Transaction Report

A government filing required by reporting entities that includes a financial institution's account of a questionable transaction. Many jurisdictions require financial institutions to report suspicious transactions to relevant government authorities such as its FIU on a suspicious transaction report (STR), also known as a suspicious activity report or SAR.

Suspicious Transactions

Suspicious Transactions are financial transactions in which there are reasonable grounds to suspect that, the funds involved are related to the proceeds of criminal activity.

Terrorist Financing

The process by which terrorists fund their operations in order to perform terrorist acts.

Third Line of Defense

The third-line defense is the internal audit, which involves independent reviews of the controls applied by the first two lines of defense. It independently evaluates the risk management and controls of the bank through periodic assessments, including the adequacy of the bank's controls to mitigate the identified risks. It also evaluates the effectiveness of the staff's execution of the controls, the effectiveness of the compliance oversight and

quality controls, and the effectiveness of the training.

Tipping Off

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

Trade-Based Money Laundering

The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize the illicit origins.

Trust

Arrangement among the property owner (the grantor), a beneficiary and a manager of the property (the trustee), whereby the trustee manages the property for the benefit of the beneficiary in accordance with terms set by the grantor.

Trustee

A person (natural or legal) that holds the assets in a trust fund separate from the trustee's own assets. The trustee invests and disposes of the assets in accordance with the settlor's trust deed, taking into consideration any letter of wishes.

Typology

Refers to a money laundering method and is a term used by FATF.

United Nations

An international organization that was established in 1945 by 51 countries committed to preserving peace through cooperation and collective security. The United Nations contributes to the fight against organized crime with initiatives such as the Global Program against Money Laundering (GPML), the key instrument of the UN Office of Drug Control and Crime Prevention in this task. Through the GPML, the UN helps member states to introduce legislation against money laundering and to develop mechanisms to combat this crime. The program encourages anti-money laundering policy development, monitors and analyzes the problems and responses, raises public awareness about money laundering and acts as a coordinator of joint anti-money laundering initiatives with other international organizations.

Unusual Transaction

Transaction that appears designed to circumvent reporting requirements, is inconsistent with the account's transaction patterns or deviates from the activity expected for that type of account.

Wire Transfer

Electronic transmission of funds among financial institutions on behalf of themselves or their customers. Wire transfers are financial vehicles covered by the regulatory requirements of many countries in the anti-money laundering effort.

Wolfsberg Group

Named after the castle in Switzerland where its first working session was held, the Wolfsberg Group is an association of global financial institutions, including Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse Group, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank and UBS. In 2000, along with Transparency International and experts worldwide, the institutions developed global anti-money laundering guidelines for international private banks. Since then, it has issued several other guidelines on correspondent banking and terrorist financing, among others

Annex1 Collection of information

For natural persons

Y = Is to be compulsorily obtained **N** = Not required **O** = Is to be obtained if applicable

Particular	Nepali	NRN	Indian	Foreigner (non- Indian)	Remarks
Personal Details					
Full Name	Y	Y	Y	Y	
Gender	Y	Y	Y	Y	
Date of birth	Y	Y	Y	y	
Nationality	Y	Y	Y	Y	
Residence Country	Y	Y	Y	Y	
Family Details					
Name of father and mother	Y	Y	Y	Y	
Name of grandfather	Y	Y	Y	Y	
Name of spouse	O	O	O	O	
Name of father-in-law or Mother-in-law	O	N	N	N	For married woman only
Name of sons and daughters	O	O	O	O	
Transaction Details					
Estimated yearly transaction amount	Y	Y	Y	Y	
Estimated yearly number of transaction	Y	Y	Y	Y	

	Residing in Nepal				Residing abroad				
	Nepali	NRN	Indian	Foreigner (non-Indian)	Nepali	NRN	Indian	Foreigner (non-Indian)	Remarks
Permanent address									
Tole/Street	Y	Y	Y	Y	Y	Y	Y	Y	
House No	O	O	O	O	O	O	O	O	
Muni/Rural Muni	Y	O	O	O	Y	O	O	O	
Ward No	Y	O	O	O	Y	O	O	O	
District	Y	O	O	O	Y	O	O	O	
State	Y	O	O	O	Y	O	O	O	
Country	Y	Y	Y	Y	Y	Y	Y	Y	
Current address									
Tole/Street	Y	Y	Y	Y	Y	Y	Y	Y	
House No	O	O	O	O	O	O	O	O	

Muni/Rural Muni	Y	Y	Y	Y	O	O	O	O	
Ward No	Y	Y	Y	Y	O	O	O	O	
District	Y	Y	Y	Y	O	O	O	O	
State	Y	Y	Y	Y	O	O	O	O	
Country	Y	Y	Y	Y	Y	Y	Y	Y	
Identification details									
Type of ID	Y	Y	Y	Y	Y	Y	Y	Y	
ID Number	Y	Y	Y	Y	Y	Y	Y	Y	
Issue Date	Y	Y	Y	Y	Y	Y	Y	Y	
Expiry Date	O	O	O	O	O	O	O	O	
Visa Expiry Date	N	N	O	Y	N	N	O	O	
Issuing Authority	Y	Y	Y	Y	Y	Y	Y	Y	
Issuing Place	Y	Y	Y	Y	Y	Y	Y	Y	
Issuing Country	Y	Y	Y	Y	Y	Y	Y	Y	
NRN Card	N	Y	N	N	N	Y	N	N	
Permanent Account Number (PAN)	O	O	O	O	O	O	O	O	

If any of these persons are related persons, transaction details and PAN is not to be obtained.

For legal persons

Y = Is to be compulsorily obtained **N** = Not required **O** = Is to be obtained if applicable

	Sole proprietor / partnership	Company	Club / NGO	Cooperatives	Trust	School / college	INGO	Consumer committee
Name of entity	Y	Y	Y	Y	Y	Y	Y	Y
Address of registered office								
Tole/Street	Y	Y	Y	Y	Y	Y	Y	Y
House No	O	O	O	O	O	O	O	O
Muni/Rural Muni	Y	Y	Y	Y	Y	Y	Y	Y
Ward No	Y	Y	Y	Y	Y	Y	Y	Y
District	Y	Y	Y	Y	Y	Y	Y	Y
Province	Y	Y	Y	Y	Y	Y	Y	Y
Country	Y	Y	Y	Y	Y	Y	Y	Y
Address of the business								
Tole/Street	Y	Y	Y	Y	Y	Y	Y	Y
House No	O	O	O	O	O	O	O	O
Muni/Rural Muni	Y	Y	Y	Y	Y	Y	Y	Y
Ward No	Y	Y	Y	Y	Y	Y	Y	Y
District	Y	Y	Y	Y	Y	Y	Y	Y
Province	Y	Y	Y	Y	Y	Y	Y	Y
Country	Y	Y	Y	Y	Y	Y	Y	Y
Type of business	Y	Y	Y	Y	Y	Y	Y	Y

Phone number	Y	Y	Y	Y	Y	Y	Y	Y
Email	O	O	O	O	O	O	O	O
Jurisdiction	Y	Y	Y	Y	Y	Y	Y	N
Number of branches	Y	Y	Y	Y	Y	Y	Y	N
Place of major branches	Y	Y	Y	Y	Y	Y	Y	N
Expected transaction amount	Y	Y	Y	Y	Y	Y	Y	Y
Expected Annual Transaction Number	Y	Y	Y	Y	Y	Y	Y	N
Documents as per the product paper	Y	Y	Y	Y	Y	Y	Y	Y

Any other documents that the bank may deem necessary on case-to-case basis needs to be obtained.

Annex 2 Collection of documents

A. For individuals

Y = Is to be compulsorily obtained **N** = Not required **O** = Is to be obtained if applicable

Particular	Nepali	Minor	NRN	Indian	Foreigner (non- Indian)	Refugee	Remarks
Recent passport size photograph	Y	Y	Y	Y	Y	Y	
Voter's card	Any One	N	N	N	N	N	
Driver's license		N	N	N	Y	N	
citizenship certificate		N	Any one	N	N	N	
Passport		N		Any one	N	N	
Registration certificate issued by Embassy of India in Nepal	N	N	N		N	N	
Non-Resident Nepali Card	N	N	Y	N	N	N	
Birth Certificate / Certificate of minor	N	Y	N	N	N	N	
Refugee identity card	N	N	N	N	N	Y	
Valid Visa	N	N	N	N	Y	N	
Permanent Account Number (PAN) / Value Added Tax (VAT)	O	O	O	O	O	N	
Income source documents	O	O	Y	O	O	O	
Staff identity card	O	N	N	N	N	N	Mandatory for persons working in GoN, public enterprises, limited companies, schools, colleges, and universities under subsidy by GoN

B. For legal persons

Y = Is to be compulsorily obtained **N** = Not required **O** = Is to be obtained if applicable

SN	Documents	Sole proprietor / partnership	Company	Club / NGO	Cooperatives	Trust/Foundation	School / college	INGO	Embassy	Consumer committee
1	Registration	Y	Y	Y	Y	Y	Y	Y	N	O
2	License and permits	O	O	O	O	O	O	N	N	N
3	PAN / VAT	Y	Y	Y	Y	Y	Y	Y	N	N
4	Personal Details of									
	Proprietor	Y	N	N	N	N	N	N	N	N
	Partner	Y	N	N	N	N	N	N	N	N
	Signatories	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Board of directors /Management committee/ executive committee members	N	Y	Y	Y	Y	Y	Y	N	N
	Chief Executive officer	N	Y	Y	Y	Y	Y	Y	N	N
	Shareholders holding 10% or more shares	N	Y	Y	N	N	N	N	N	N
	Trustee/Settlors/Comptroller	N	N	Y	N	N	N	N	N	N
	Country representatives	N	N	N	N	N	N	Y	N	N
5	Passport size photo of									
	Proprietor	Y	N	N	N	N	N	N	N	N
	Partner	Y	N	N	N	N	N	N	N	N
	Signatories	Y	N	Y	Y	Y	Y	Y	N	Y
	Board of directors	N	Y	N	Y	N	N	N	N	N
	Chief Executive Officer	N	Y	Y	Y	Y	Y	Y	N	N
	Country representatives	N	N	N	N	N	N	Y	N	N
6	Identity documents as per “A. For individuals” above									
	Proprietor	Y	N	N	N	N	N	N	N	N
	Partner	Y	N	N	N	N	N	N	N	N
	Signatories	Y	N	Y	Y	Y	Y	Y	N	Y
	Board of directors	N	Y	N	Y	N	N	N	N	N
	Chief Executive Officer	N	Y	Y	Y	Y	Y	Y	N	N
	Country representatives	N	N	N	N	N	N	Y	N	N
7	Documents disclosing address of									
	Members	N	N	N	N	Y	N	N	N	N
	Signatories	N	N	N	N	N	N	Y	Y	N
	Board of directors /Management committee/ executive committee members	N	N	N	N	N	N	Y	N	N
	Chief Executive officer	N	N	N	N	N	N	Y	N	N
	Country representatives	N	N	N	N	N	N	Y	N	N

SN	Documents	Sole proprietor / partnership	Company	Club / NGO	Cooperatives	Trust/Foundation	School / college	INGO	Embassy	Consumer committee
8	Financials									
	Audited Financials	Any one	Y	Y	Y	Y	Y	Y	N	N
	Management prepared financials		N	N	N	N	N	N	N	N
	Tax Clearance, tax paid voucher	Y	Y	O	Y	Y	Y	Y	N	N
9	Regulating documents									
	Partnership deed	Y	N	N	N	N	N	N	N	N
	Article of association & Memorandum of association	N	Y	N	N	N	Y	N	N	N
	Constitution / Bylaws	N	N	Y	Y	Y	N	Y	N	O
	Trust deed	N	N	N	N	Y	N	N	N	N
10	Minutes									
	Minute with decision for opening account and authority to operate account	Y	Y	Y	Y	Y	Y	Y	N	N
	Minute for establishing branch / sister organization along with authority to operate account	N	N	N	N	N	N	O	N	N
	Minute with decision for opening account and authority to operate account	N	N	N	N	N	N	N	Y	Y
11	Agreements									
	Agreement with Social Welfare Council	N	N	N	N	N	N	O	N	N
	Agreement with GoN	N	N	N	N	N	N	O	N	N
12	Others									
	Letter from embassy	N	N	N	N	N	N	N	Y	N
	Recommendation letter from local level government to open the bank account along with details of account operators	N	N	N	N	N	N	N	N	Y
	Declaration that the account shall be used for the purpose of establishment of consumer committee	N	N	N	N	N	N	N	N	Y

Annex 3 Risk assigned to districts

SN	District	SN	District	SN	District	SN	District
	HIGH RISK	10	Sarlahi	15	Salyan	37	Doti
1	Kathmandu	11	Kapilbastu	16	Gulmi	38	Bajura
2	Morang	12	Surkhet	17	Baglung	39	Darchula
3	Sunsari	13	Udayapur	18	Khotang	40	Dadeldhura
4	Rupandehi	14	Kavrepalanchok	19	Ramechhap	41	Kalikot
5	Jhapa	15	Mahottari	20	Dolakha	42	Jajarkot
6	Kailali	16	Nawalparasi East	21	Dailekh	43	Jumla
7	Kaski		**LOW RISK**	22	Solukhumbu	44	Rukum East
8	Dhanusa	1	Nawalparasi West	23	Parbat	45	Rasuwa
9	Chitawan	2	Bardiya	24	Rolpa	46	Mugu
10	Siraha	3	Dhading	25	Arghakhanchi	47	Humla
11	Parsa	4	Tanahu	26	Bhojpur	48	Mustang
	MEDIUM RISK	5	Sindhupalchok	27	Okhaldhunga	49	Dolpa
1	Lalitpur	6	Ilam	28	Lamjung	50	Manang
2	Banke	7	Sindhuli	29	Rukum West		
3	Dang	8	Syangja	30	Taplejung		
4	Makawanpur	9	Palpa	31	Dhankuta		
5	Bara	10	Nuwakot	32	Myagdi		
6	Saptari	11	Gorkha	33	Terhathum		
7	Kanchanpur	12	Panchthar	34	Baitadi		
8	Rautahat	13	Sankhuwasabha	35	Bajhang		
9	Bhaktapur	14	Pyuthan	36	Achham		

Annex 4 Risk assigned to business

HIGH-RISK BUSINESS

1. Art and antique dealers	6. Charity organization	11. Casino/ gambling & night club
2. Embassy/consulate	7. INGO	12. Jewelry & precious metal
3. Money changer	8. NGO	13. Private investment company
4. Political organizations	9. Real estate companies	14. Remittance company licensed by NRB
5. Religious organizations	10. Offshore bank/entity	

LOW-RISK BUSINESS

1. Government entities
2. Bank and financial institutions
3. Government owned entities
4. Insurance companies

Annex 5 Risk scoring and ratings

	Parameters	Result	Risk	Score	Override as
1	Name screening				
i	Screening ID	Sanction	High	10	High
		PEP	High	10	
		Adverse Media	High	10	
		False Match	Low	1	
ii	Self-declaration as PEP	True	High	10	
		False	Medium	3	
iii	Citizen from sanction country	True Match	High	10	High
		False Match	Low	1	
iv	Family member	False match	High	10	
		True Match	Medium	3	
v	Ownership layer (for entities only)	True match	High	10	High
		False Match	Medium	3	
A	Screening score	Maximum of i to vi			
2	Geography				
i	Nationality	High Risk Countries	High	10	High
		Nepal	Low	1	
		Others	Medium	3	
ii	District	High Risk Areas	High	10	
		Medium Risk Areas	Medium	3	
		Low Risk Areas	Low	1	
B	Screening score	Average of i and ii			
3	Occupation & income				
i	Occupation	Self-employed	High	10	
		Business, House wife, Unemployed	Medium	3	
		Agriculture, Salaried	Low	1	
ii	Type of business	High Risk Business	High	10	High
		Medium risk Business	Medium	3	
		Government owned Business	Low	10	Low
iii	Income source	Investment	High	10	
		Business, Family income, Remittance	Medium	3	
		Agriculture, Insurance, Job, Pension, Rent	Low	1	
C	Screening score	Average of i to iii			
	Customer				
	Introducer	Walk in customer	High	10	
		Other Accountholder	Medium	3	
		Staff of the Bank	Low	1	
		Local Bodies	Low	1	
ii	Helpful	Yes	Medium	3	
		No	High	10	
iii	High Risk Business	Yes	High	10	High
		No	Medium	3	
iv	Face-to-face	Yes	Low	1	

		No	High	10	
D	Screening score	Average of i to iv			
4	Transaction				
i	Trans. Amount	Entity:			
		Transaction in cash of more than NPR 100 million	High	10	High
		Total account balance is NPR 200 million or more in all of the accounts	High	10	High
		Individual			
		Total account balance is NPR 50 million or more in all of the accounts	High	10	High
		Difference of 5x in estimated annual transactions declared by customer and estimated by staff	High	10	High
		Sum of all LC facilities availed by a customer in a fiscal year is NPR 100 million and above or equivalent	High	10	High
		Sum of all LC facilities availed by a customer in a fiscal year is less than NPR 100 million or equivalent	Medium	3	
		Sum of all guarantees availed in a fiscal year is NPR 150 million and above or equivalent	High	10	High
		Sum of all guarantees availed in a fiscal year is less than NPR 150 million or equivalent.	Medium	3	
ii	Matches profile	Yes	Low	1	
		No	High	10	
iii	Source identifiable	Yes	Low	1	
		No	High	10	
iv	Remittance	Yes	Low	1	
		No	High	10	
E	Screening score	Average of i to iv			
	Total risk	Average of A to E			

Interpretation

1. 10 or more High Risk
2. Below 10 up to 3: Medium Risk
3. Below 3: Low Risk

Annex 6 ECDD Form

ENHANCED CUSTOMER DUE DILIGENCE - INDIVIDUALS
(TO BE FILLED BY THE BRANCH)

Date: **Account no.:** **Account name:**

SN	Question	Comments
1.	Is the customer a PEP? [ ] Yes, Self > Reason for considering as PEP: _____ [ ] Yes, Related with PEP> Relation: _____ [ ] No	 If yes, go to 2 If no, go to 3
2.	Is the customer still in prominent position for PEP? [ ] Yes [ ] No, left the position/retired but 5 years has not elapsed [ ] No, left the position/retired but 5 years has elapsed	 If 5 years has been elapsed, the account-holder is not a PEP.
3.	Do the accountholder's family members maintain account with any of our bank branches? [ ] Yes [ ] No Name A/C no. Relation a. _____ _____ _____ b. _____ _____ _____ c. _____ _____ _____ d. _____ _____ _____ If yes, are these (above) accounts categorized as PEP (as associated PEP)? [ ] Yes [ ] No	 If yes, Mention account numbers and name Change risk grade to High Risk of all of these accounts if the risk rate is not High Risk
4.	Indicate source of fund (There might be one or many sources) a. Agriculture [ ] Large [ ] Small scale farming [ ] Sales proceeds to wholesales [ ] Sales proceeds personally b. Business profits Business registered year _____ B.S. (or _____ A.D.) Type of goods / services offered _____ Business owned by self or family member? [ ] Yes [ ] No c. Family income Person who earns for the family Name: _____ Relation _____ His/her occupation _____ His/her estimated yearly income NPR _____ His/her account with the bank: Account no. _____Risk Assigned _____ Branch _____ [ ] Do not have account at any branch of our Bank	 Change risk grade to High Risk if maintained otherwise

	d. Insurance agent commission Name of insurance company _____ Year of involvement _____ years e. Investment earnings [ ] Trading of shares [ ] Real estate [ ] Others_____ Years of involvement: _____ year f. Job / Salaried Works in [ ] Government of Nepal [ ] Pvt. / Ltd. Company [ ] Renowned firm [ ] Small / local firms Confirmation taken with organization involved: [ ] Yes, through _____ [ ] No Years of experience in the current office _____ year Monthly Salary NPR _____ g. Pension Pension paying office: _____ Monthly pension in NPR _____ h. Remittance (including sponsorship) [ ] Domestic[ ] International [ ] Receives from family members Name: _____ Relation _____ [ ] Receives from persons who are not family members Name: _____ Relation _____ i. Rent [ ] From own property [ ] From family owned property [ ] Sublet	If confirmation is not taken, it is to be obtained through phone, visits, letters/documents or other means as appropriate Sublet: to rent out a property in which the accountholder is not an owner but tenant)
5.	Address verification has been made through [ ] Resident/office visits: Visits made by staff / agent: Name of staff: _____ Employee ID: _____ Date of site visit: _____	Mention Staff name and Staff ID in case visits has been made by staff. Mention name of the agent if visited by third party agent.
6.	Beneficial owner is other than the accountholder [ ] Yes [ ] No	If Yes, obtain KYC of the beneficial owner and record in Finacle by creating Customer ID and E-kagaj

ECDD conducted by:	ECDD verified by:
Name Staff ID: Signature:	Name of Operations In-Charge Staff ID: Signature: OI to ensure that scanned copy of this form is uploaded in E-kagaj after signing.

ENHANCED CUSTOMER DUE DILIGENCE - ENTITIES
(TO BE FILLED BY THE BRANCH)

Date: **Account no.:** **Account name:**

SN	Question	Comments
1.	Purpose of account open [ ] Loan [ ] Business transactions	
2.	The entity is expected to receive payment from abroad [ ] Yes; name of country (s) _____ [ ] No	If yes, ensure that these are not sanctioned countries.
3.	Entity registration is valid: [ ] Yes, Registration expiry date.: _____ [ ] No	
4.	Entity requires licenses and permits: [ ] Yes Type of License taken: _____ Permit / license issuing authority: _____ Permit / license expiry date: _____ [ ] Not required	
5.	Address verification has been made through [ ] Resident/office visits: Visits made by staff / agent: Name of staff: _____ Employee ID: _____ Date of site visit: _____	Mention Staff name and Staff ID in case visits has been made by staff. Mention name of the agent if visited by third party agent.
6.	The entity has its own website with complete information about its shareholders, products and services offered by it. [ ] Yes web site address: _____ [ ] No	

ECDD conducted by:	ECDD verified by:
Name: Staff ID:	Name of Operations In-Charge Staff ID:
Signature:	Signature:
	OI to ensure that scanned copy of this form is uploaded in E-kagaj after being signed.

Annex 7 Suspicious alert assessment form

Suspicious Alert Assessment Form

DATE PREPARED | PREPARED BY | SOURCE OF STR | WAS UNDER WATCHLIST > REVIEW DATE>

PROFILE

ACCOUNT NAME | ACCOUNT NO. | CUSTOMER ID

ACCOUNT SCHEME | TYPE: INDIVIDUAL | ACCOUNT OPEN DATE | DATE OF BIRTH

PROFESSION / BUSINESS AREA | GENDER | ID NO. | ID TYPE | ID ISSUE DATE

HAS OTHER ACCOUNTS WITH THE BANK > | RISK | COUNTRY | PROVINCE | DISTRICT

ASSUMPTIONS & DECLARATION

MIN THRESHOLD | AVG TRANSACTIONS | YEARLY TRANS NO. (CUST) | NO. OF BRANCHES | YEARLY TRANS (CUST)

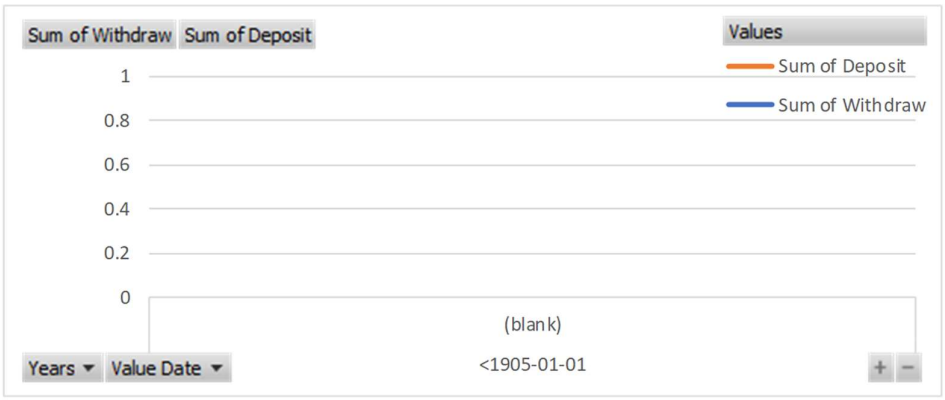
PROXIMITY | RISK

BRANCH / SOL | PLACE OF RESIDENCE/WORK IS NEAR TO BRANCH >

TRANSACTION TO | FROM *0 Days* | RISK

		NO.	TOTAL TRAN	AVERAGE TRAN	BRANCH THRESHOLD	
A. CASH	DR	-	NPR	NPR	-	-
	CR	-	NPR	NPR	-	-
B. CLEARING	DR	-	NPR	NPR	-	-
	CR	-	NPR	NPR	-	-
C. TRANSFERS	DR	-	NPR	NPR	-	-
(ALL CHANNELS)	CR	-	NPR	NPR	-	-
D. TRANSFERS	DR	-	NPR	NPR	-	-
(DIGITAL CHANNELS)	CR	-	NPR	NPR	-	-
TOTAL TRANSACT	DR	-	NPR	NPR	-	-
(A+B+C)	CR	-	NPR	NPR	-	-

TRANSACTION TREND



RISK

IS NORMAL

NATURE OF TRANSACTION TO FROM *0 Days* RISK

	DEPOSIT		WITHDRAWALS	
	No.	Amount	No.	Amount
FROM ACCOUNT SOL	0	NPR .00	0	NPR .00
FROM OTHER SOL	0	NPR .00	0	NPR .00
FROM DIGITAL CHANNEL	0	NPR .00	0	NPR .00

IS NORMAL

SUMMARY

PROXIMITY	TYPE OF TRANSACTION	TRANSACTION TREND	NATURE OF TRANSACTION

ACTION TO BE TAKEN

DESCRIPTIONS

NAME OF ACCOUNTHOLDER

SUMMARY

ANALYSIS OF EXAMINATION:

POSSIBLE LINKAGE:

LINKED PERSONS/ACCOUNTS:

RELATED ACCOUNT NUMBERS:

SUSPECTED BENEFICIARY:

OCCUPATION/BUSINESS IN CASE OF ENTITY :

ESTIMATED YEARLY INCOME:

ESTIMATED MONTHLY SALARY:

OTHER RELEVANT INFORMATION:

PERSON AND TRANSACTION TREE OR MAP:

GENERAL INDICATOR

DESCRIPTION (AS PER NRB STR GUIDELINE)

INDICATOR 1

INDICATOR 2 (OPTIONAL)

TOTAL SUSPICIOUS AMOUNT

TRANSACTION REPORTED

TRAN ID	**TRAN ID**	**TRAN ID**
TRAN DATE	**TRAN DATE**	**TRAN DATE**
AMOUNT	**AMOUNT**	**AMOUNT**

Date	Year	Dr.	Dr.	Cr.	Cr.	Closing

WITHDRAW

	Date	Cheque/Voucher No.	Payee	Amount	Remarks
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Annex 8 Category of domestic PEPs

1. House of representative
   a. Speaker
   b. Deputy Speaker
   c. Member of House

2. National Assembly
   a. Chairman
   b. Deputy Chairman
   c. Member of House

3. Province Assembly
   a. Speaker
   b. Deputy Speaker
   c. Member of House

4. President

5. Vice President

6. Ministries
   a. Prime Minister
   b. Deputy Prime Minister
   c. Ministers
   d. Chief Minister

7. Member of Judicial Council

8. Judiciary
   a. Chief Justice
   b. Justice of Supreme Court
   c. Justice of High Court
   d. Registrar of Supreme & High Court
   e. Head of Other Judicial Body and Tribunal (Special Court, Administrative Court, etc.)

9. Commission for the Investigation of Abuse of Authority (CIAA)
   a. Chief Commissioner
   b. Commissioner

10. Office of Auditor General
    a. Audit General
    b. Deputy Audit General

11. Public Service Commission
    a. Chairperson
    b. Executive Member

12. Office of Attorney General
    a. Attorney General
    b. Deputy Attorney General

13. Financial Comptroller General Office
    a. Financial Comptroller General
    b. Joint Financial Comptroller General
    c. Deputy Financial Comptroller General

14. National Human Rights Commission
    a. Chairperson
    b. Commissioners

15. Election Commission Nepal
    a. Chief Election Commissioner
    b. Election Commissioner

16. National Natural Resources and Fiscal Commission
    a. Chairperson
    b. Members.

17. National Women Commission
    a. Chairperson
    b. Members.

18. National Dalit Commission
    a. Chairperson
    b. members

19. Indigenous Nationalities Commission
    a. Chairperson
    b. Members.

20. National Inclusion Commission
    a. Chairperson
    b. Members.

21. Madhesi Commission
    a. Chairperson
    b. Members.

22. Tharu Commission
    a. Chairperson
    b. Members.

23. Muslim Commission:
    a. Chairperson
    b. Members.

24. Nepalese Ambassador/Counselor of foreign Countries

25. Nepal Army
    a. Chief of Army
    b. Lieutenant General
    c. Major General
    d. Brigadier General
    e. Colonel

26. Nepal Police
    a. Inspector General of Police
    b. Additional Inspector General of Police
    c. Deputy Inspector General of Police
    d. Senior Superintendent of Police

27. Armed Police
    a. Inspector General – IG
    b. Additional Inspector General – AIG
    c. Deputy Inspector General – DIG
    d. Senior Superintendent - SSP

28. Head of National Investigation Department

29. Director General of Department of Money Laundering Investigation

30. Director General of Department of Revenue Investigation

31. Nepal Rastra Bank
    a. Board of Directors
    b. Governor
    c. Deputy Governor
    d. Executive Director

32. Beema Samiti (Insurance Board)
    a. Board of Director
    b. Executive Director

33. National Cooperative Development Board
    a. Executive Committee Member

34. Security Board of Nepal
    a. Board of Director
    b. Executive Director

35. Nepal Stock Exchange
    a. Board of Director
    b. Chief Executive Officer

36. Nepal Electricity Authority
    a. Board of Directors
    b. Managing Director

37. Nepal Telecommunication Authority
    a. Board of Director
    b. Chairman

38. Civil Aviation Authority of Nepal
    a. Board of Directors
    b. Director General

39. Universities
    a. Chancellor
    b. Vice-Chancellor
    c. Registrar

40. Nepal Medical Council
    a. President
    b. Registrar

41. Nepal Nursing Council
    a. President
    b. Registrar

42. National Examination Board
    a. Board of Director

43. Nepal Engineering Council
    a. Chairman
    b. Registrar

44. Nepal Bar Council
    a. Chairman
    b. Registrar

45. The Institute of Chartered Accountants of Nepal
    a. President
    b. Vice President

46. Council for Technical Education and Vocational Training
    a. Chairperson
    b. Vice Chairperson

47. Employee Provident Fund
    a. Board of Directors
    b. Administrator

48. Citizen Investment Trust
    a. Board of Director
    b. Executive Director

49. Nepal Airlines Corporation
    a. Board of Director
    b. Managing Director

50. Nepal Water Supply Corporation
    a. Board of Director
    b. General Manager

51. Rastriya Beema Sansthan
    a. Board of Directors
    b. Administrator

52. Nepal Oil Corporation
    a. Board of Directors
    b. Managing Director

53. Department of Mines and Geology
    a. Director General

54. National Trust for Natural Conservation
    a. Board of Trustee

55. Department of Archaeology
    a. Director General

56. Department of National Parks and Wildlife Conservation
    a. Director General

57. Department of Livestock Services
    a. Director General

58. Department of Agriculture
    a. Director General

59. Department of Food Technology and Quality Control
    a. Director General

60. Department of Cottage & Small Industries
    a. Director General

61. Inland Revenue Department
    a. Director General

62. Salt Trading Corporation Limited
    a. Board of Director
    b. Chief Executive Officer

63. Nepal Telecom
    a. Board of Director
    b. Managing Director

64. Nepal Tourism Board
    a. Board of Director
    b. Chief Executive Officer

65. National Planning Commission
    a. Vice Chairman
    b. Member of the Executive Committee

66. Nepal Law Commission
    a. Chairperson
    b. Vice Chairperson
    c. Members of the Commission

67. Nepal Bureau of Standards & Metrology
    a. Director General

68. National Trading Limited
    a. Director General

69. Nepal Food Corporation
    a. Board of Director
    b. Director General

70. Office of the Company Registrar
    a. Registrar

71. Department of Industry
    a. Director General

72. Department of Electricity Development
    a. Director General

73. Department of Custom
    a. Director General

74. Department of Cooperative
    a. Registrar

75. Department of Commerce Supplies and Consumer Protection
    a. Director General

76. Rastriya Banijya Bank/Nepal Bank/Agricultural Development Bank
    a. Board of Director
    b. Chief Executive Officer

77. Dairy Development Corporation
    a. Board of Director
    b. Director General

78. Lumbini Sugar Industries
    a. Board of Director
    b. Director General

79. Herbs Production & Processing Co. Ltd.
    a. Board of Director
    b. General Manager

80. Nepal Aushadhi Limited
    a. Board of Director
    b. General Manager

81. Udayapur Cement Industries Ltd.
    a. Board of Director
    b. General Manager

82. Agriculture Input Company Limited
    a. Board of Director
    b. Managing Director

83. Nepal Ban Nigam Limited
    a. Board of Director
    b. Director General

84. Deposit and Credit Guarantee Fund
    a. Board of Director
    b. Chef Executive Officer
    c. Department of Transport Management
    d. Director General

85. Cultural Corporation
    a. Director General

86. Gorkhapatra Sansthan
    a. Board of Director
    b. Director General

87. Nepal Academy
    a. Chanellor
    b. Vice Chancellor

88. Janak Education Material Center Limited
    a. Board of Director
    b. General Manager

89. Nepal Television
    a. Board of Director
    b. General Manager

90. Medical Education Commission
    a. Chairperson
    b. Co-Chairperson
    c. Vice Chairperson

91. Mayor / Chairman of rural municipality

92. Deputy mayor / Deputy Chairman of rural municipality

93. Joint Secretary, Secretary and Chief Secretary of Government of Nepal

Annex 9 Suspicious transaction / activity reporting form

SUSPICIOUS TRANSACTION / ACTIVITY REPORTING BY BRANCH / DEPARTMENT FORM
(to be emailed to MLRO)

1. Date
2. Branch / Department
3. Reporting staff ID
4. Customer Name
5. Has account with the bank
   a. ☐ Yes > Account no. ____ Customer ID ____
   Is account of your branch? ☐ Yes > KYC Status ____
   ☐ No > Branch ____
   b. ☐ No > ID type ____ ID No. ____
   Mobile number ____
6. Account of business owned by the customer maintained in bank ☐ Yes > Account no. ____ ☐ No
7. Is customer loan client? ☐ Yes ☐ No
8. How suspicion noticed / found
9. Reasons for Suspicion
10. Suspicious Amount NPR ____
11. Other comments if any: