FREQUENTLY ASKED QUESTIONS On AML/CFT

1. **What is Money Laundering?**

Money Laundering is the process by which illegal funds and assets are converted into legitimate funds and assets.

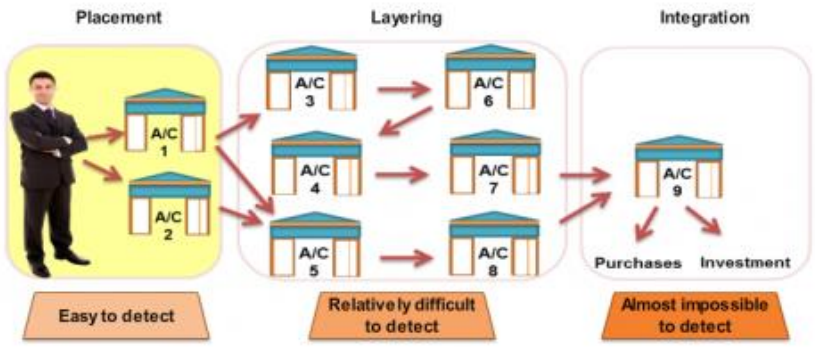
2. **What is the current scale of Money Laundering worldwide?**

Measuring the current scale of money laundering is extremely difficult. The World Bank and IMF have estimated volume of money laundering to between 3 and 5 percent of global gross domestic product (GDP) equivalent to approximately US$2.2 trillion to US$3.7 trillion annually.

3. **How does money laundering work?**

Money laundering works in following three stages.

1. **Placement**: Illegal funds or assets are first brought into the financial system. This placement makes the funds more liquid. Money launderers place illegal funds using a variety of techniques like, depositing cash into bank accounts or purchasing insurance products and using cash to purchase assets.
2. **Layering:** To conceal the illegal origin of the placed funds and thus make them more useful, the funds have to be moved, dispersed and disguised. This activity is known as "layering". At this stage, money launderers use many different techniques to layer the funds like, using multiple banks and accounts, having professionals act as intermediaries and transacting through corporations and trusts. This helps the launderers to disguise the origin of the funds.
3. **Integration:** The last stage of the money laundering process is called "integration". The "cleaned" funds can now be made available for investment in legitimate or illegitimate businesses. Thus, the original "dirty" money has achieved the appearance of legitimacy.



4. **What is Anti Money laundering (AML)?**

Anti Money Laundering (AML) refers to a set of procedures, laws and regulations designed to stop the practice of generating income through illegal actions.

5. **What is Terrorist Financing?**

Terrorism financing refers to activities that provide financing or financial support to individual terrorists or terrorist groups.

6. **What is Combating Financing of Terrorism (CFT)?**

Combating the Financing of Terrorism (CFT) involves investigating, analyzing, deterring, and preventing sources of funding for activities intended to achieve political, religious, or ideological goals through violence and the threat of violence against civilians.

7. **What is the difference between Money Laundering and Terrorist Financing?**

Money Laundering involves the disguising of fund derived from illegal activity so they may be used without detection of the illegal activity whereas terrorist financing involves the use of legally derived money to carry out illegal activities.

8. **Why is AML/CFT important?**

AML/CFT is important for following reasons:

- To protect the financial system;
- To prevent criminals from enjoying the proceeds of crimes;
- To prevent criminals to build formidable economic powers and challenge the stability

9. **Who is responsible for AML/CFT activities in financial institutions?**

Each and every individual who works in the Banks and Financial Institution is responsible for AML/CFT activities.

10. **Who enforces the Anti Money laundering regulations?**

Government of Nepal enforces the Anti Money Laundering regulations.

11. **What is Financial Information Unit (FIU)?**

Financial Information Unit (FIU) shall mean the Financial Information Unit (FIU established on April 21, 2008 pursuant to Section 9 of the Assets (Money) Laundering Prevention Act, 2008 within Nepal Rastra Bank (the Central bank) as an independent unitin order to work against the money laundering and terrorist financing activities. It is the financial intelligence unit of the State of Nepal. It is the central, national agency accountable for receiving, processing, analyzing and disseminating financial information and intelligence on suspicious money laundering and terrorist financing activities.

12. What is Shell Bank/Shell Entity?

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

13. What are the sources of illegal funds?

There are many sources of illegal funds. Major sources are as below:

- Participation in an organized criminal group, racketeering;
- Terrorism, including terrorist financing;
- Trafficking in human being s and migrant smuggling;
- Sexual exploitation including sexual exploitation of children;
- Illicit trafficking in narcotic drugs and psychotropic substance;
- Illicit arms trafficking;
- Illicit trafficking in stolen and other goods;
- Corruption and bribery;
- Fraud;
- Counterfeiting currency;
- Counterfeiting and piracy of products;
- Environmental crime;
- Murder , grievous bodily injury;
- Kidnapping, illegal restraint and hostage taking;
- Robbery and theft;
- Smuggling (including in relation to customs and excise duties and taxes);
- Tax crimes (related to direct and indirect taxes);
- Extortions,
- Forgery;
- Piracy;
- Insider taking and market manipulation

14. What is Know Your Customer (KYC)?

KYC is a process of identifying a customer trying to maintain business relationship or has already maintained such relationship or has requested for occasional transaction/s. It helps the Bank to identify and verify the customer/s; assess risk and manage it; develop risk-based,

effective, efficient and economic control system; and identify further business potential. Know Your Customer (KYC) and CDD can also be taken as a unit in certain business context.

15. What are the key elements of Know Your Customer (KYC)?

The key elements of KYC policy are:

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

16. What is customer acceptance policy?

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

- No account shall be opened in the name altering from the primary identity document, anonymous or fictitious (benami) name(s), blank names or numeric/alphanumeric characters.
- Accounts shall be opened only in the name of natural and legal person/organization, the name being the same as in the primary identity document of the person/entity. Accounts may however be opened with different account titles identifying the nature/use/purpose/type/ of account at the written request of the legal person/organization with appropriate control parameters.
- Minimum required information and documents i.e. proper identification and information pertaining to the prospective client shall be obtained prior to opening account or performing business relation of any kind, as per the AML Act, AML Rule, FIU Directives, NRB regulations/Directives and as per the product paper/policy/guidelines set forth by the Bank.
- Necessary checks/ examinations/ verifications shall be made before opening a new account so as to ensure that the identity of the customer does not match with any person with …..criminal background or with banned entries such as terrorist individual/s or terrorist organization/s etc.
- Not to open an account: Where the staff/s designated to open new accounts, find sufficient ground/s that the identity of the prospective customer/s could not be verified and/or the prospective customer/s is not disclosing the required identity, the reason for opening account, transaction frequency and volume, etc and any other such information/s deemed necessary for account opening. The refusal shall be documented properly, and shall be communicated to the HO AML compliance Officer through Branch AML Compliance Officer.
- Further, the Bank shall freeze an existing account under the situation when the designated staff/s is unable to apply appropriate customer due diligence measure/s i.e. unable to verify the identity and/or obtain document/s required as per the risk categorization, due to non-cooperation of the customer or non-reliability of the data /information furnished to the Bank. Decision for closure of such accounts shall be approved by Senior Management level official under recommendation of AML Compliance Officer at HO and also after giving due notice to the customer explaining the reason for such decision, Closure of such accounts shall be informed to the FIU in written.

- The Bank shall not establish any business relationship/s with the shell companies and the institution/s that deal with shell companies. Any identified business relationship/s with the financial and other institution/s that allow the transaction of shell bank, shall be discontinued. The bank shall not be associated with the entities located in the non-cooperative jurisdictions as identified by the FATF or those sanctioned by the agencies that the Bank refers to like, UN, OFAC, HMT, EU etc.
- Implementation of CAP should not be too restrictive resulting into denial of banking services to the general public, especially those who are financially or socially disadvantaged.

The decision to open an account for Politically Exposed Persons (PEPs) and Person in Influential Position (PlP) shall be approved by the senior Management Level official/s. Information of such account shall be provided to the AML Compliance Officer at HO

17. What are the customer identification procedures?

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

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

Natural Person/s

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

Legal Person/s

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

Legal arrangement:

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

18. When to identify or verify the customers?

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

connected with a financial transaction which can pose significant reputational or other risks to the Bank.

19. What is Customer Due Diligence (CDD)?

Customer due diligence is a process of identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information. It includes;

- Identifying customers, including beneficial owners;
- Gathering information on customers and beneficial owners and creating a customer risk profile;
- Applying established customer acceptance policies to new customers;
- Maintaining customer and beneficial owner information on an ongoing basis; and
- Monitoring customer's transactions and relationship with the customer on an ongoing basis.

20. Why is KYC/CDD important?

It allows the institutions to know and understand their customers and their transactions better, which in turn allows the institutions to intercept any fraudulent dealing.

21. When does KYC apply?

KYC will be carried out for the following but is not limited to:

- Opening a new account.(deposit/ borrowal)
- Opening a subsequent account where documents as per current KYC standards not submitted while opening the initial account.
- Opening a locker facility where these documents are not available with the bank for all locker facility holders.
- When the bank feels it is necessary to obtain additional information from existing customers based on the conduct of the account.
- After periodic intervals based on instructions received from RBI.
- When there are changes to signatories, mandate holders, beneficial owners, etc.

22. What are the types of CDD?

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

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

1. **Simplified Customer Due Diligence**

Simplified CDD is the lowest level of due diligence that can be completed on a customer. This is implied to the customer with low risk category. The customer can be categorized as low risk in the risk assessment of AML/CFT IT system conducted as per the AML Act, AML Rules and NRB Directive are met.

2. **Normal Customer Due Diligence**

Normal CDD is implied to the customers in general or in medium risk or those who do not fall under high risk or low risk. The AML/CFT IT System of the Bank provides workflow for entering, storing, updating, and retrieval of the normal CDD information**.**

3. **Enhanced Customer Due Diligence**

Enhanced CDD shall be applied to the customers categorized as high risk. ECDD includes higher degree of CDD that requires collection of additional information and documents as well as surveillance in every stage of transaction. The Bank aims to reach to the reality of the customer and transactions through ECDD process. Certain customer or transactions may need special and extended attention of the bank. Hence, a rigorous and robust additional KYC/CDD process shall be applied for ECDD customer or transactions with additional reasonable measures to verify and validate the customer's identity, understand and test the customers profile, business and account activity as well as risk associated. Prior approval shall be taken from management in account opening and high value transaction for the customer through the quickest means for high-risk category.

23. **When to update/review KYC?**

Update and review of a customer shall be based on the risk as follows, at a minimum, unless circumstances need something else or there is urgent need of changing the category of risk:

a. High risk one year
b. Medium risk three year
c. Low risk five year

24. **Who are Politically Exposed Persons (PEPs)?**

PEPs means politically exposed persons. It includes both domestic and international PEPs.

Domestic PEPs includes The President, Vice President, Ministers, Members of parliaments, Officers of the Constitutional Bodies, Judges of the different courts, senior politicians, Members of national political parties, Officers of special class of GoN, seniors executives of any institutions partially or fully owned by the government etc.

International PEPs includes head of the state or the government, senior politicians, central members of political parties, senior governments, judiciary military officials, diplomats etc.

25. Why to screen PEPs customers?

PEPs are high risk customers. So, each and every customer should be screened against PEPs list and if any customer falls under it, approval from high authority should be taken before opening the account.

26. What is STR?

STR means suspicious transaction report. Suspicious transactions are those transactions that deviate from the profile, characteristics and usual transactions pattern, transaction reasonably suspected to have been conducted with the purpose of evading the reporting and financial transaction conducted using fund alleged to be attributable to predicate offences.

Suspicious transactions should be reported within 3 days of arriving at the conclusion that the transaction is suspicious.

27. What are STR triggers?

- **Cash**: Cash transactions conducted in an unusual amount; relatively small amount but with high frequency; transactions conducted by using several different individual names for the interest of a particular person; purchase of several insurance products in cash in a short period of time or at the same time with premium payment entirely in a large amount and followed by policy surrender prior to due date and purchase of securities by cash, transfer, or checks under other person's name.
- **Economically irrational transactions**: Transactions having no conformity with the initial purpose of account opening; transactions having no relationship with the business of the relevant customer; transaction amount and frequency are different from that of normally conducted by the customer; receipts/payments of funds made by using more than one (1) account, either in the same name or a different one; fund transfers using the account of reporting entities' employee in an unusual amount; if multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate.
- **Fund Transfers:** Fund transfers to and from high-risk offshore financial centers without any clear business purposes; receipts of fund transfers in several phases and once accumulated the funds are subsequently transferred entirely to other account; receipts and transfers of funds at the same or approximately the same amount and conducted in a relatively short period (pass-by).
- **Behaviors of the Customer:** Unreasonable behaviors of the relevant customer when conducting a transaction (nervous, rushed, unconfident, etc.); unusual curiosity about internal system, control and reporting; customer/prospective customer gives false information with respect to his/her identity, sources of income or businesses; Customer/prospective customer uses identification document that is unreliable or alleged as fake such as different signature or photo; customer opens account for a short period.

28. What is TTR?

Threshold transactions includes following transactions.

1. Credit and debit transaction of **NPR 1 million or more** in the account of any person or entity particularly of cooperative, private company, NGOs either by single or multiple transactions through any mode in a day.
2. Payment of remittance of **NPR 1 million or more** by any person or entity to any person or entity through single or multiple transactions in a day.
3. Exchange transactions of **NPR 5,00,000** or more provided to any person or entity through single or multiple transactions in a day.

Threshold transactions should be reported within **15 days** of such transactions.

29. What is tipping off?

Tipping off means telling the clients that his/her account is being monitored or informing the client that there is an element of suspicion on the transaction or disclosing the information to designate authority. When an institution identifies a suspicious transaction, the customer should not be "tipped off" or informed.

30. What are the penalties for non-compliance of AML/CFT?

- To fine from NPR 1 million to **NPR 50 million** for FIs and NPR 1,00,000 to **NPR 10 million** for other Res
- To impose **full or partial restriction** on the business
- To suspend or **cancel registration/permission/license**
- To impose other appropriate **sanctions**.

31. What is risk classification of the customers?

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

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

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

32. Who are high risk customers?

- Customer identified as high risk with higher rank of risk scoring by RBA module in screening result and KYC risk profiling in the AML/CFT IT System and national, regulatory and internal risk assessment.
- All account of customers domiciled in high risk countries as categorized by FATF and updated by FIU/Home Ministry from time to time.
- All other accounts classified by FIU-NRB as high risk accounts.
- Customer or transactions related with a jurisdiction fundamentally deficient for the control of following types of crimes in general, but not limited to,:
    - Terrorism and Financing of terrorist activities,
    - Money Laundering
    - Proliferation Financing, Arms and Ammunition
    - Corruption
    - Tax / Revenue evasion
    - Narcotic Drugs and psychotropic substances
    - Human trafficking
    - Organized crime
    - Counterfeiting
- Customer or transactions related with a jurisdiction largely deficient for the control of above listed types of crimes in general or are under a kind of international monitoring
- Non face-to-face Customers or Business Transactions, particularly,
    - Cross border correspondent banking
    - Wire transfers
    - Business relation through Internet, Telephone, Fax, Postal service etc.
    - Internet Banking, ATM Transaction, Mobile Banking
    - Transaction through instruction / request by Fax/wire
    - Transaction through Wire or prepaid card, etc.
- Politically exposed persons (PEPs) both domestic and foreign PEPs their family member and person associated with them.
- Antique dealers (individuals and entities), Money service bureaus, Dealers in arms, Casinos, Bullion dealers including sub dealers &jewelers.
- Business of precious herbs and medicines.
- Export/import trade, Travel agencies, Cooperatives, and company service providers, real Estate agents, Dealers in vehicles.
- All accounts of Trusts, NGOs, Charities, Charities and Organizations receiving domestic or foreign donations and accounts operated by Power of Attorney holders may be classified as High Risk.
- STR reported customer
- Customer under investigation or prosecution or convicted
- Customer with suspected Beneficial Owner.

33. Who are low risk customers?

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

- Salaried employees/pensioners whose salary structure is well defined.
- People belonging to lower economic strata of the society whose accounts show small balances and low turnover.
- Current account and saving account having annual turnover less than NPR 1 Lakh.
- Government departments and Government owned companies, Regulators, Financial Institutions, Statutory Bodies, etc.
- All deposit and borrower accounts pertaining to the Government of Nepal, Governmental bodies/Corporations/Companies/Organizations, Joint ventures with Government, Regulators, Financial Institutions, and Statutory Bodies may be classified as low risk account.
- All borrower accounts other than those classified as high risk and medium risk.

34. What type of transactions are non face to face transactions?

Non face to face transactions include but not limited to;

- business relationships concluded over the Internet or by other means such as through the post;
- services and transactions over the Internet;
- use of ATM machines;
- telephone banking;
- transmission of instructions or applications via facsimile or similar means; and
- making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid or re-loadable or account-linked value cards.

35. Who is beneficial owner?

Beneficial Owner means the natural person/s who ultimately own or control a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person, entity or arrangement.

36. Why to identify beneficial owners?

The term Beneficial Owner is important to understand because a person in whose name an account is opened with an institution may not necessarily be the person who ultimately controls or is entitled to the funds or investments. The distinction is important because the focus of anti-money laundering guidelines is on the person who has the ultimate level of control or entitlement.

37. How long the transactions record of the customers should be kept?

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