नेपाल राष्ट्र बैंक

बैंक तथा वित्तीय संस्था नियमन विभाग

केन्द्रीय कार्यालय
बालुवाटार, काठमाडौं।
फोन नं.: ४४१९८०४/५
Web Site: www.nrb.org.np
पोष्ट बक्स:७३

पत्र संख्या : बै.वि.नि.वि./नीति/सूचना/७/०७९/८०

मिति: २०७९/०८/१८

सूचना

इजाजतपत्रप्राप्त बैंक तथा वित्तीय संस्थाहरु तथा पुर्वाधार विकास बैंक,

AML/CFT सम्बन्धी जोखिम मुल्यांकन गर्न सहज हुने उद्देश्यले यस बैंकबाट इजाजतपत्रप्राप्त बैंक तथा वित्तीय संस्थाहरु तथा पुर्वाधार विकास बैंकका लागि ML/TF Risk Assessment Guidelines for Bank and Financial Institution, 2022 जारी गरिएको व्यहोरा सम्बन्धित सबैको जानकारीको लागि यो सूचना प्रकाशित गरिएको छ।

कार्यकारी निर्देशक

ML/TF Risk Assessment Guidelines for Bank & Financial Institutions, 2022

NEPAL RASTRA BANK

November 2022

Contents

<u>Note:</u> For the purpose of this guideline, Financial Institutions include- A Class Commercial Banks, B Class Development Banks, C Class Finance Companies, D Class Microfinance Institutions and Infrastructure Development Bank

Abbreviations

AML/CFT	Anti-money Laundering/Countering Financing of Terrorism
APG	Asia Pacific Group on Money Laundering
CDD	Customer Due Diligence
DNFBPs	Designated Non-Financial Businesses and Professions
ECDD	Enhanced Customer Due Diligence
FATF	Financial Action Task Force
FIU	Financial Information Unit
HNI	High Net-worth Individual
KYC	Know Your Customer
ML/TF	Money Laundering/ Terrorist Financing
NRA	National Risk Assessment
NRB	Nepal Rastra Bank
PEP	Politically Exposed Person
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report

1. Introduction

1.1 This guideline is designed to assist to conduct money laundering and terrorism financing risk assessment (hereinafter referred as 'risk assessment') under the Asset (Money) Laundering Prevention Act, 2008 (hereinafter referred as 'the Act') and Unified Directive issued by NRB.

1.2 FATF Recommendation 1 of the 40 Recommendations requires financial institutions or DNFBPs to conduct ML/TF risk assessment of their business.

1.3 Risk assessment is the first step that must be taken before developing AML/CFT program. It involves identifying and assessing the inherent risks reasonably expected by financial institutions in terms of ML/TF perspective. Once risk assessment is completed, then only a program that minimizes or mitigates those risks can be implemented.

1.4 Risk assessment and AML/CFT program should reflect a risk-based approach that allows some flexibility in the steps to meet AML/CFT obligations. A risk-based approach does not restrict financial institutions from engaging in transactions/ activities or establishing business relationships with higher-risk customers. Rather, it is expected to effectively manage and prioritize responses to ML/TF risks.

1.5 Risk assessments guides financial institutions in optimal allocation of the available resources towards the AML/CFT efforts and thereby implement risk-based approach to AML/CFT program effectively and efficiently. The nature and extent of the ML/TF risk assessment should commensurate with the nature and size of the business.

1.6 On the basis of the risk assessment, financial institutions should formulate policies, procedures and control measures to mitigate and manage the identified risk in an effective manner. Financial institutions should not only monitor the implementations of the control measures adopted, but also enhance the measures regularly.

1.7 The risk assessment process should be initiated only after financial institutions familiarize themselves with the NRA, the Mutual Evaluation Report, AML/CFT National Strategy, typologies envisaged by FIU (through guidelines or annual

reports) and guidelines issued by the NRB. This would assist financial institutions to comprehend the national level risk in their institutional risk assessment.

1.8 Predicate offences are the crimes underlying ML/TF activities. Financial institutions should understand the various types of predicate offences mentioned in the annexure of the Act.

1.9 As a reporting entity, financial institutions have a number of obligations under the Act and Unified Directive in relation to risk assessment. In addition to requirements of Section 7D of the Act, risk assessment must fulfill following requirements.

- Risk assessment must identify the risk of ML/TF that financial institutions may reasonably expect to face during their business;
- Risk assessment must enable financial institutions to determine the level of ML/TF risk involved in relation to relevant obligations under the Act;
- Risk assessment should be done for each group or type of customers, business relationships, product or services, delivery channel and geographical location offered by financial institutions within its business;
- Risk assessment must be submitted to NRB within stipulated time through stipulated process, after review from the board;
- Risk assessment must be used to develop AML/CFT program; and
- Risk assessment must identify deficiencies, make necessary changes and be reviewed to ensure it is up to date.

1.10 When conducting risk assessment, it is expected that both adequacy and effectiveness are explored. Adequacy is defined as how compliant risk assessment is with the various obligations of the Act. Effectiveness is defined as how well the practical application of the risk assessment meets the obligations of the Act.

1.11 The contents of this guideline and the examples provided herein are neither intended to, nor should be considered as an exhaustive treatment of the subject and the NRB may revise this guideline by revoking, varying, amending or adding to its content.

2. Objectives

This guideline aims at:

- Outlining the recommended steps involved in conducting ML/TF risk assessment;
- Providing general information about risks related with the customers, products, services, delivery channels and geographical locations;
- Assisting financial institutions to develop policies, procedures and control measures that enable them to effectively manage and mitigate the inherent risks that have been identified; and
- Guiding financial institutions to frame a process to systematically check and assess the adequacy of the control system.

3. Role and Responsibilities of Board and Senior Management

3.1 The ultimate responsibility to identify and assess ML/TF risks and take measures to mitigate them is borne by the Board and the senior management of financial institutions. Board and senior management's initiation and commitment to the prevention of ML/TF risks are vital aspects while implementing a risk-based approach to combat ML/TF risks.

3.2 The Board should encourage regulatory compliance and ensure that employees abide to internal procedures, policies, practices and processes aimed at risk mitigation and control. Role and responsibilities of the Board includes:

- approving and reviewing appropriate policies for ML/TF risk management;
- determining the financial institution's risk appetite on Customer Acceptance;
- establishing internal controls; and
- being in active engagement with the senior management.

3.3 Board should ensure that senior management is taking necessary steps to identify, measure, monitor and mitigate the ML/TF risks including implementing strategies to mitigate those risks.

3.4 Senior management is, in turn, responsible for establishing and communicating a strong awareness of, and need for effective internal controls, policies and procedures within the organization.

4. Identification of Risk

4.1 In the assessment of ML/TF risks, financial institutions must address their "inherent risks". These are the ML/TF risks present before applying controls and mitigations. Financial institutions may focus to assess their "residual risks" (risks after controls and mitigations) as part of their risk assessment. However, NRB will expect that risk assessment deals with inherent risk. If risk assessment covers residual risk, financial institutions will need to document and demonstrate how residual risk is computed.

4.2 In order to identify the risk effectively, financial institutions must, at a minimum, assess the products and services, delivery channels, types of customers, and geographical locations.

4.3 The nature, size and complexity of business activities can be guiding factors to determine how susceptible is financial institutions towards ML/TF. For instance, the bank with huge transactions in cash, cross border transaction or transactions of complex nature are more vulnerable towards the ML/TF risk than those financial institutions with nominal transactions of such nature. In the process of identification of risk, financial institutions must analyze the scope and segmentation (i.e. volume/ threshold of transaction etc.) of the customers in performing the transactions across multiple products to circumvent the detection.

4.4 Use of quantitative data will help figure out what parts of the business are vulnerable to ML/TF activities. For instance, financial institutions may have identified a higher-risk product, but without knowing number and varieties of those products that financial institutions have provided to customers, and place of domicile (and other relevant factors), this will result in a flawed assessment of risk.

4.5 The FATF, the APG, and other international AML/CFT agencies also publish documents in relation to the various methods and trends used for ML/TF (also called typologies). Review of such typologies should be done for proper assessing of ML/TF risk.

4a. Products and Services

4a.1 The products and services offered by financial institutions may have varying degree of ML/TF risks. Some of the products may foster higher degree of anonymity, use

of larger volume of cash or involvement of third party agents compared to other products. Thus, during the assessment process, financial institutions must be heedful of the transaction volume, average transaction size, exposure to foreign transactions, level of cash activity, complexity and transparency of the products and services offered by them.

4a.2 In addition, financial institutions should also be watchful about the engagement of third party agents in the delivery of the products and services to the customer. The frequency of the transactions together with the size/value of the transactions is crucial factor to be considered in monitoring the movement of the illicit funds through the banking channels.

4a.3 The ability to hide amongst other transactions and conduct frequent transactions is a key factor for those seeking to undertake money laundering or the financing of terrorism. Financial institutions should always be careful of the transparency in the offered products and services. The products and services should be transparent in terms of the anonymity offered as well as the obscure ownership.

4a.4 Additionally, prior to introducing new products, financial institutions should assess the potential ML/TF risks associated with same, to ensure that the appropriate mitigating mechanism is in place.

4a.5 Some of the products and services for risk assessment are listed below:

- Deposit account services- interest bearing and non-interest bearing accounts;
- Lending activities, particularly loans secured by cash collateral and marketable securities, immediate prepayment of loans and other ;
- Electronic banking: mobile banking, internet banking, card services, fund transfer services, quick response code services and point of sale banking;
- Wire transfer services/ Money Value Transfer Services (MVTS): domestic and international wire transfers/ MVTS, both inward and outward;
- Services provided to third-party payment processors or senders;
- Trade finance services;
- Correspondent banking services;
- Foreign exchange services - buy and sell of foreign currency;
- Safe deposit vault services;

- Depository services; and
- Market maker for government securities.

4a.6 When considering whether the products and services offered by financial institutions could be exploited for ML/TF purposes, following questions can be considered:

- Does the product/service allow for anonymity?
- Does the product/service disguise or conceal the beneficial owner of the customer?
- Does the product/service disguise or conceal the source of wealth or funds of the customer?
- Does the product/service allow payments to third parties?
- Does the product/service commonly involve receipt or payment in cash?
- Has the product/service been identified in the NRA, FIU or NRB guidance material, or any Sector Risk Assessments as presenting a higher ML/TF risk?
- Does the product/service allow for the movement of funds across borders?
- Does the product/service enable significant volumes of transactions to occur frequently?
- Does the product/service allow the customer to engage in transactions with minimal oversight by the financial institution?
- Does the product/service have an especially high transaction or investment value?
- Does the product/service have unusual complexity?
- Has there been an immediate prepayment of loan or other unusual activity?
- Does the product/service, particularly internet banking, let the users residing outside the country to make transfer of funds from the account?

4a.7 A number of other factors can contribute to the ML/TF risk of products and services. It will be the responsibility of financial institutions to identify those factors as part of their risk assessment.

4b. Customer Types

4b.1 All the customers of financial institutions may be equally posing vulnerability towards the ML/TF. However, the nature of the business, occupation, expected transaction volume may pose customer specific risk.

4b.2 Some categories of customers pose a higher risk of ML/TF than others, especially when combined with higher-risk products/services and jurisdictions. Financial institutions need to determine the breakdown of their customer base; assessing where the customers originate from or the types of transaction they are performing, in line with how they use the products/services of the financial institution, etc.

4b.3 It is essential that financial institutions exercise judgment when assessing customer types, as opposed to treating or defining all members of a specific category of customer as posing the same level of risk.

4b.4 At the end of the assessment, financial institutions should be able to assign category of their customers as high, medium or low risk.

4b.5 Some examples of customers types and entities are detailed below:

- Foreign financial institutions, including banks and foreign money services providers (e.g., money changers, and money remitters);
- Non-bank financial institutions (e.g., money services businesses; casinos; brokers/dealers in securities);
- Senior political figures and their immediate family members and close associates of PEPs- domestic, foreign or international;
- Foreign corporations, particularly offshore corporations (such as domestic shell companies and Private Investment Companies (PIC) and international business corporations (IBC) located in higher-risk geographic locations;
- Cash-intensive businesses (e.g., petrol pumps, restaurants, retail stores);
- Non-governmental organizations and charities (foreign and domestic);
- Professional service providers (e.g., attorneys, accountants, or real estate brokers);
- Housewives;
- Students; and
- Minors.

4b.6 Financial institutions needs to evaluate following questions when assessing both its new and existing customers:

- Are they a trust or other legal person?
- Have the beneficial owners been identified?
- Are they specified in the Act or Rules or NRB as requiring enhanced due diligence?
- Are they involved in occasional or one-off activities/transactions above a certain threshold?
- Do they use complex business structures that offer no apparent financial benefits?
- Are they PEP?
- Are they in a cash-intensive business?
- Are they involved in businesses associated with high levels of corruption?
- Do they have an unexplained or hard to verify source of wealth and/or source of funds?
- Do they conduct business through, or are introduced by, gatekeepers such as accountants, lawyers, or other professionals?
- Are they a non-profit organization?
- Are they HNI?
- Have they been identified in the NRA or by FIU as presenting a higher ML/TF risk?
- Are they large borrowers?
- Are there any unusual debit/credit transactions, especially spending money in extravagant activitites?

4c. Delivery Channels

4c.1 The vulnerability to ML/TF is affected by the mode of on-boarding the customers and delivering the products and services. When identifying the risk associated with delivery channels, financial institutions should consider the risk factors related to the extent that the business relationship is conducted on a non-face to face basis,

any introducers or intermediaries used and the nature of their relationship. This should be performed during further transactions carried with the customer.

4c.2 The assessment of vulnerability towards ML/TF from the delivery channels must be based on the identification of number of delivery channels used in the business transactions and the use of delivery channels by various products and services. This would provide financial institutions with clearer picture of the areas the money launderer can exploit the products and services with multiple delivery channels to conceal the actual nature of transaction.

4c.3 Financial institutions can assess:

- Whether the customer is physically present for identification purposes.
- Do financial institutions have non-face-to-face customers (via post, telephone, internet or intermediaries)?
- Are products/services provided via internet?
- Do financial institutions have indirect relationships with customers (via intermediaries)?
- Are products/services provided by means of agents or intermediaries?
- Are products/services provided to overseas jurisdictions?
- How often are the non-account holders operating as conductors?

4d. Geographical locations

4d.1 Geographical location risk may arise because of the location of a customer and the origin or destination of transactions of the customer. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to money laundering and terrorism financing.

4d.2 It is important to identify geographical location which may pose a higher degree of risk and assist financial institutions to understand and evaluate the specific risks associated with doing business in, opening and servicing accounts, offering products and services and/or facilitating transactions involving certain geographic locations.

4d.3 Geographic risk alone does not necessarily determine a customer's or transaction's risk level. Financial institutions have to ensure that they understand the links

between their customers and the different jurisdictions they operate in, transact with or originate from, so that an effective assessment of the risk can be undertaken.

4d.4 The geographically risky location can be categorized as international and domestic. Domestic geographical location risk can be identified based on:

- the exposure of the business based upon frequency of transaction; ;
- access to customs;
- level of predicate offences in the jurisdiction;
- level of transparency;
- level of financial access and literacy; and
- negative report of public media.

International higher risk geographic locations generally include:

- Jurisdictions or countries monitored for deficiencies in their regimes to combat ML/TF by international entities;
- Offshore financial centers;
- Countries with ineffective AML/CFT measures;
- Countries with high level of organized crime;
- Countries with high prevalence of bribery and corruption; and
- Other countries identified by financial institution as higher-risk because of its prior experiences or other factors (e.g., legal considerations, or allegations of official corruption).

4d.5 To assist in the determination of a country's geographic risk, various sources of information can be used. These include:

- FATF list of high-risk and non-cooperative jurisdictions;
- FATF mutual evaluation reports;
- Basel AML Index;
- United Nations Office on Drugs and Crime reports;
- Transparency International Corruption Perceptions Index;
- Trusted and independent media sources; and
- United Nations sanctions, embargoes or similar measures.

4d.6 Based on the analysis of above factors, financial institutions will be able to identify the geographic breakdown associated with its customers/transactions, put in place adequate monitoring systems and measures to address the risks.

4d.7 Financial institutions may consider checking if countries are subject to United Nations sanctions, embargoes or similar measures.

5. Risk assessment of financial institutions

5.1 Once the ML/TF risks have been identified, financial institutions must determine the level of that risk.

5.2 Financial institutions should analyze for the various situations that currently arise in their business or are likely to arise in the near future. For instance, risk assessment should consider the impact of new products, services or customer types, as well as new technology. In addition, ML/TF risks will often operate together and represent higher risks in combination.

5.3 For proper management of ML/TF risks of financial institutions, it should identify all the possible threats that can arise during the operation and also assess the vulnerability towards the threats.

5.4 Upon identifying the risks, financial institutions needs to adequately assess the ML/TF risk exposure, which would enable them to evaluate the likelihood of adverse effects arising from that risk and the potential impact of that risk on the realization of objectives.

5.5 The process of risk assessment can be divided into a series of activities or stages:

a. Identification;
b. Analysis; and
c. Evaluation.

5.6 Firstly, the process of identification in the context of an ML/TF risk assessment starts by developing an initial list of potential risks or risk factors financial institutions face when combating ML/TF. The threats and vulnerabilities drive the identification process. Ideally at this stage, the identification process should attempt to be comprehensive; however, it should also be dynamic in the sense that new or previously undetected risks identified may also be considered at any stage in the

process. Financial institutions should identify customers, products, services, transactions, and geographical locations specific risk for the entity.

5.7 Secondly, analysis stage is the core of the ML/TF risk assessment process. This stage considers the nature, sources, likelihood and consequences of the identified risks or risk factors. This stage aims to gain a holistic understanding of each of the risks – as a combination of threat, vulnerability and consequence in order to work toward assigning some sort of relative priority to them. The consequence can be financial loss from the crime, fines from the authorities or enhanced mitigation measures. It can also consist of reputational damages to the entity or to the entire sector.

5.8 Finally, evaluation in the context of the ML/TF risk assessment process involves taking the risks analyzed during the previous stage to determine priorities for addressing them, taking into account the purpose established at the beginning of the assessment process. These priorities can contribute to development of a strategy for risk mitigation.

5.9 The risk identification and analysis should cover all the existing as well as the newly introduced products and services offered by financial institutions. This would be instrumental in implementation of the effective risk management of the ML/TF risk. The risk identification and assessment is crucial as the risk of different products and services varies. For example, the transaction with one geographical region may not be equally vulnerable as compared to another. Thus, after effective risk identification and assessment, financial institutions can focus on customers, countries, products, services, transactions and delivery channels that constitute the greatest potential risk.

5.10 Financial institutions should take a holistic approach in determining the level of ML/TF risk associated with a business relationship or transaction. Financial institutions can use the approach of likelihood and consequence to ultimately determine the level of risk. The likelihood of a risk to occur can be cross referenced with the consequence of that risk to determine the ultimate level of risk.

5.11 Risk assessment basically involves the calculation of the magnitude of potential consequences (levels of impacts) and the likelihood (levels of probability) of such

consequences to occur. Likelihood is the probability of occurrence of an impact, which is the combination of threat and vulnerability; and consequence is the impact if an event occurs. Thus, the risk level can be mitigated if the threat, vulnerabilities or their impact can be reduced.

5.12 Risk likelihood can also be assessed in terms of threat and vulnerability. For example, financial institutions may consider domestic tax evasion criminals as the threat, and accounts dealing with cash payments as the vulnerability. Depending on the risk assessment method used, this could result in likelihood scale rating of *very likely*. Financial institutions may then assess the impact of this event on their business and the wider environment.

5.13 Likelihood ratings and consequence ratings can provide a more comprehensive understanding of risk and a robust framework to help arrive at a final risk rating. For instance, if the risk is *very likely* to happen, and the expert professional of financial institutions based on a structured questionnaire conclude it to have a *moderate* impact, the cross reference of the likelihood and its impact will give the ultimate risk to financial institutions. Thus, financial institutions can address the ultimate risk with various control measures.

5.14 The illustrative risk matrix, to be assessed for each of the risks identified (for categories of products and services, types of customers, delivery channels, and geographical locations) is provided below:

	Consequence scale					
Likelihood scale		Minimal (1)	Minor (2)	Moderate (3)	Significant (4)	Severe (5)
	Very unlikely (1)	1	3	6	10	15
	Unlikely (2)	2	5	9	14	19
	Likely (3)	4	8	13	18	22
	Very likely (4)	7	12	17	21	24
	Most likely (5)	11	16	20	23	25

(Numbers shown in the cross-referenced cell indicates level of risk- smaller number shows lower risk and higher number shows higher risk)

	Inherent risk				
Risk rating	Low 1-3	Medium- Low 4-7	Medium 8-13	Medium-High 14-21	High 22-25

5.15 Financial institutions can compute institutional risk by combining all the inherent risks assessed for each category of risk. Financial institutions can give more risk weight to certain risk categories/sub-categories to provide a more nuanced understanding of ML/TF risk. An example of the summary table is shown below:

SN	**Category of risk**	**Sub-categories of risk (can be one or more)**	**Level of risk assessed**	**Risk weight/ priority**	**Institutional risk**
1	Product and services				
2	Customer types				
3	Delivery channels				
4	Geographical locations				
5	Other				

5.16 Appropriate program should be prepared to address higher risks with appropriate control measures. This should be done for each of the identified risks.

6. Control Measures

6.1 The understanding of the inherent ML/TF risk of financial institutions relating to the products and services, customer type, delivery channel and the geographical location within which or its customers transacts are crucial.

6.2 Controls are strategy, policies, programs or activities put in place by financial institutions to protect against the materialization of a ML/TF risk, or to ensure that

potential risks are promptly identified and subsequently mitigated. Controls are also used to maintain compliance of rules and regulations governing an organization's activities.

6.3 Policies and procedures for customer acceptance, due diligence and ongoing monitoring should be designed and implemented to adequately control identified inherent risks.

6.4 The residual risk (after applying control measures) should be managed based on the risk profile obtained through risk assessment process.

6.5 Following are major control categories applied across AML/CFT framework:

- Policies and procedures with timely update;
- Management oversight and accountability;
- Management information/reporting;
- AML/ CFT corporate governance;
- KYC, CDD, ECDD;
- Sanction screening systems;
- Previous other risk assessments (local and enterprise-wide);
- Record keeping and retention;
- Detection and STR/SAR filing;
- Monitoring and controls;
- Designated AML/CFT compliance officer/unit;
- Training and Capacity building;
- Sufficient budgeting for the budgeting of AML/CFT provisions; and
- Independent testing and oversight (including recent internal/ external audit or other material findings)

7. Applying a risk assessment

7.1 Bank should identify ML/TF risks and then assess the level of such risks. Assessed risks should then help financial institutions formulate necessary strategies, policies or programs.

7.2 Risk assessment should help financial institutions rank and prioritize risks and provide a framework of how those risks will be managed. Risk assessment must

enable financial institutions to prepare a comprehensive program. It should enable financial institutions to meet relevant obligations under the Act and regulations, including obligations to conduct CDD, monitor accounts and activities and report suspicious activity.

7.3 Risk assessment should help in determining suspicion and consequently assist in the decision to submit an STR/SAR to the FIU. Financial institutions must submit an STR/SAR to the FIU if they think activities or transactions are suspicious. For instance, financial institutions may consider unexpected international activity of a domestic-based customer unusual, especially if it involves a high-risk jurisdiction, and submit an STR/SAR.

7.4 As financial institutions must conduct ongoing CDD, risk assessment should help financial institutions target and prioritize the resources needed for ongoing CDD. For instance, financial institutions may undertake ongoing CDD on high-risk customers on a more regular basis than on lower-risk customers.

7.5 As financial institutions must undertake account monitoring, risk assessment should help financial institutions design the triggers, red flags and scenarios that can form part of account monitoring. For instance, financial institutions may check the activity of a high-risk customer in a high-risk jurisdiction (as identified in risk assessment) to be subject to more frequent and in-depth scrutiny.

7.6 Further, review and audit of risk assessment is highly recommended.

Additional reference materials:

FATF- Guidance for a risk based approach- Banking Sector- https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

Basel Committee on Banking Supervision- Sound management of risks related to money laundering and financing of terrorism- https://www.bis.org/bcbs/publ/d505.pdf