# Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 01 of 2018

## Introduction

1. The Financial Intelligence Unit of Sri Lanka (FIU), acting within the powers vested with it under the Financial Transactions Reporting Act, No. 06 of 2006 (FTRA), issued the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016 by Gazette Extraordinary No. 1951/13, dated January 27, 2016; effective from the date of issue, applicable to institutions which engage in "finance business" as defined under Section 33 of the FTRA.

2. As applicable under Rule 3 of the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016, the rules introduce, inter alia, provisions requiring financial institutions identified under the rules to take measures specified therein for the purpose of identifying, assessing, and managing Money Laundering (ML) and Terrorist Financing (TF) risks posed by its customers and business activities.

## Risk Management

3. Every Financial Institution should identify and analyze ML/TF risks present within the financial institution and design and effective implementation of policies and procedures that are commensurate with and that mitigate the identified risks to ensure sound ML/TF risk management.

4. In conducting a comprehensive risk assessment to evaluate ML/TF risks, every financial institution should consider all the relevant risk factors present in its customer base, products, delivery channels and services offered (including products under development or to be launched) and the jurisdictions within which it or its customers do business.

5. Risk assessments should be based on specific operational and transactional data and other internal information collected by the financial institution as well as external sources of

information such as national risk assessments conducted by Sri Lanka and by governmental agencies of foreign jurisdictions where the financial institution has business relationships, either through customers or branch/subsidiary networks, country reports from reliable international and regional organizations, such as reports and reviews prepared by the Financial Action Task Force (FATF), FATF-style regional bodies such as the Asia/Pacific Group on Money Laundering (APG), International Monetary Fund (IMF) and World Bank publications, and information from reliable commercial intelligence providers.

6. Financial Institutions are required to have a risk management framework to address ML/TF risks. Such a framework includes policies, controls and procedures that enable them to identify, measure, monitor, control and mitigate effectively the ML/TF risks that have been identified.

## Risk Management Framework

### Corporate Governance

7. The FIU expects financial institutions to establish a robust and effective corporate governance framework that ensures transparency, accountability and high ethical conduct in all aspects of their operations. Institutions should adopt a Code of Ethics that promotes consistently high standards of ethical conduct by all employees. A sound corporate governance framework includes the use of effective policies and procedures, monitoring and reporting mechanisms and internal controls. Measures that ensure appropriate separation of functions and the avoidance of conflicts of interests are essential hallmarks of an effective corporate governance regime. The Board of Directors (BoD) is ultimately responsible for establishing a corporate vision, strategy and business model and for overseeing an institution's corporate governance culture and is expected to develop mechanisms including board committees to achieve this objective. Senior management is responsible for ensuring the effective functioning of the corporate governance framework on a day-to day basis.

## I. Board of Directors (BoD)

8. Members of the BoD should have a good understanding of the institution's business model and operations and the general business climate in which it operates. They should have the qualifications and experience necessary to understand the institution's business model and operations and how these relate to Sri Lanka's general economic and social environment. The BoD should ideally be comprised of both executive and non-executive directors to ensure a desirable level of independence from the institution's management function.

9. The BoD should establish the institution's overall risk appetite and should ensure that mechanisms are in place to effectively mitigate risk. The BoD must ensure that appropriate policies, procedures and controls are in place to manage such risks and should also ensure that arrangements are in place for the effective reporting on all issues related to the functioning of the risk management framework. The BoD is ultimately responsible for the institution's operations, its management of the risk to which it is exposed and its compliance with all laws, regulations and guidelines to which it is subject.

## II. Senior Management

10. An institution's senior management is responsible for implementing the corporate vision, strategy and business model approved by the BoD. Senior management should demonstrate a firm understanding of all aspects of the institution's business model and is responsible for developing the components of the risk management framework. Senior management is responsible for ensuring that the institution has all the resources necessary to effectively manage risk. They are also responsible for ensuring that effective communication and reporting arrangements are in place to support good risk management practices. This includes ensuring that all staff members are aware of the requirements of the risk management framework and their specific roles and responsibilities. Senior management is responsible for ensuring that internal reporting mechanisms, including reports to be sent to the BoD, are developed to provide accurate and timely information relevant to the effective management of risks.

**The Risk Management Function**

11. The FIU expects institutions to develop an effective risk management function. The risk management function responsible for ensuring that the institution effectively identifies, measures, monitors, and controls and mitigates risks. From a day-to-day operational perspective risk management supports senior management and the BoD to achieve the ML/TF risk management objectives discussed in this guidance note. The risk management function should be commensurate with the, size, nature and complexity of the institution's business model and operations.

**Policies and Procedures**

12. The FIU expects the senior management to develop policies and procedures to effectively manage the ML/TF risks that arise from an institution's operations. Policies and procedures developed by senior management should be approved by the BoD. Policies and procedures should set out the day-to-day measures that should be employed to ensure that the institution effectively identifies, measures, monitors and controls ML/TF risks. They should therefore be developed to reflect the risks implicit in an institution's customers, products and services, delivery channels and geographic regions. Policies and procedures should be comprehensively documented and communicated to all staff. They should also be subject to periodic review to ensure they are appropriate in light of changes to the institution's ML/TF risk profile.

13. Policies and procedures should clearly set out lines of responsibility and accountability for the execution of the risk management function and should also establish effective reporting lines for all persons and business units involved in the management of ML/TF risks.

14. An effective risk management framework should establish limits in the context of the institution's stated appetite for ML/TF risk and the overall effective implementation of the risk management system. Policies and procedures should limit, for example, an

institution's exposure to the ML/TF risks arising from exposure to specific types of customers, products and services, delivery channels and geographic regions. An effective ML/TF risk management framework should include a mechanism to report incidents where established limits have been breached and the frequency of such events.

**Internal Controls**

15. An on-going system of internal controls is an essential component of a risk management framework. Institutions are expected to employ measures on an on-going basis to ensure adherence to establish policies and procedures as well as relevant laws, regulations and guidelines.

16. Arrangements should be in place to reinforce the "four eyes" principle and avoid conflicts of interest. Measures should be employed, for example, to ensure adequate separation between operational and control functions such as front office and back office activities.

17. Institutions are expected to develop effective internal audit arrangements. The internal audit function should be an independent function with a direct reporting line to the Board Audit Committee. The internal audit function should periodically assess the effectiveness of the institution's ML/FT risk management framework and practices paying specific attention to the institution's adherence to established policies procedures and limits and applicable laws, regulations and guidelines.

18. Institutions are also expected to ensure that their ML/TF risk management framework and practices are subject to external audit review.

**The Compliance Function**

19. The FIU expects institutions to develop an effective compliance function as a component of its ML/TF risk management framework. The compliance function should be commensurate with the, size, nature and complexity of the institution's business model and

operations. The compliance function is separate from the internal audit function as it is a component of an institutions day-to-day operational activity. The compliance function should on an-ongoing basis assess the extent to which the institution is complying with established policies, procedures and limits and obligations arising from applicable laws, regulations and guidelines. The effectiveness of the compliance function rests heavily on the effectiveness with which the Mangement Information System (MIS) generates accurate and timely reports related to the management of ML/TF risks. Compliance officer should possess sufficient seniority and knowledge and be up to date with recent laws and regulations

**Risk Monitoring and Reporting**

20. To effectively control and mitigate risk, institutions may need to develop MIS systems that provide reliable data on the quantity and nature of ML/TF risks and the effectiveness with which risks are being mitigated. The MIS system used by an institution should be commensurate with the size, nature and complexity of its business model and operations. Such systems should constantly measure ML/TF risks, changes to the nature of such risks and should also report on adherence to the policies and procedures designed to mitigate risks. The system should, for example, not only identify instances in which policies and procedures have been breached but should maintain a record of all such incidents. The system should provide timely reports to all business units and senior management to allow them to make judgments on the measures necessary to manage risks. Reports should also be prepared and submitted to senior management and the BoD indicating how well the institution is managing risk and highlighting instances of breaches of risk management policies, procedures and limits and obligations arising from applicable laws, regulations and guidelines.

**Training**

21. The FIU expects institutions to have effective arrangements in place to train their staff on all issues related to their AML/CFT regime. It is important that staff understand the institution's inherent ML/TF risks and the nature of the measures that have been developed

to mitigate these risks. Training must be provided for all staff upon joining the institution and should be an-ongoing activity. Apart from general training provided to all staff, targeted training programs should be developed for specific categories of staff in light of the nature of their work in the context of ML/FT risks. AML/CFT awareness raising programs should be conducted for members of the BoD.

**Assessing ML/TF Risk – Some Guidance**

22. The following guidance sets out a methodology for the conduct of an assessment of ML/TF risks by a financial institution. It is not mandatory to follow this methodology, however, the FIU requires that each financial institution should undertake a comprehensive assessment of its ML/TF risks and develop appropriate risk management processes.

## I. Identification of Vulnerabilities:

23. Financial Institutions are required to take appropriate steps to identify aspects of their business activities, including types of customers and transactions, which may be vulnerable to ML/TF and should in doing so, take into account the findings of the National Money Laundering and Terrorist Financing Risk Assessment of Sri Lanka[1]. Financial institutions should consider the following areas when identifying risk factors of their business that make them susceptible to ML/TF.

i. The nature, size and complexity of the business

The size and complexity of a financial institution plays an important role in how attractive or vulnerable it is for ML/TF. For example, a large financial institution is less likely to know its customers personally and this could offer a greater degree of anonymity to customers than a smaller financial institution.

[1] A copy of this report can be found at the FIU's website, http://www.fiusrilanka.gov.lk/docs/Other/Sri_Lanka_NRA_on_ML_2014_-_Sanitized_Report.pdf

Similarly, a financial institution that conducts complex transactions across international jurisdictions could offer greater opportunities for ML/TF than a purely domestic business.

ii. The products and services the business offers

Some products and services are more attractive for ML/TF. When considering whether the products and services the business offers could be susceptible or attractive for ML/TF, the following is a list of indicators (not exhaustive) that identifies ML/TF risk arising from products and services that are commonly offered by financial institutions.

- private banking services such as prioritized or privileged banking
- credit/ debit and other top-up cards
- non- face-to-face business relationship or transaction
- payment received from unknown or unrelated third parties
- any new product & service developed
- services to walk-in customers
- mobile banking
- single premium insurance policy

iii. The types of customers the financial institution deals with

Listed below are some indicators (not an exhaustive list) to identify ML/TF risk arising from customers.

Categories of customers pose a higher risk of ML/TF can include:

- new customers that wish to carry out a large transaction(s)
- non face-to-face customer on-boarding
- customers involved in occasional or one-off transactions above the threshold (either specified in the FTRA, the Customer Due Diligence (CDD) Rules or the financial institution's internal limits)
- customers who use complex business structures that offer no apparent financial benefits

- customer or a group of customers making numerous transactions to the same individual or group
- customers who are Politically Exposed Persons (PEPs)
- customer who has a business which involves large amounts of cash
- customer whose identification is difficult to check
- customer who bring in large amounts of used notes and/or small denomination notes.
- customers conducting their business relationship or transactions in unusual circumstances for example: significant and unexplained geographic distance between the financial institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations
- non- resident customers
- corporate customers whose ownership structure is unusual and excessively complex
- customers whose origin of wealth and/or source of funds cannot be easily verified or where the audit trail appears to be broken and/or unnecessarily layered
- customers that are non-profit organizations
- customers who conduct business through or are introduced by "gatekeepers" such as accountants, lawyers, or other professionals
- customers of a type that have been identified in National or Sector Risk Assessments as higher risk

iv. the countries that the financial institution deals with

Financial institutions should give consideration to the following factors as indicators of higher risk for ML/TF:

- any country subject to United Nations sanctions embargoes or similar measures
- any country identified by credible sources such as the FATF as lacking adequate AML and CFT system
- any country which is identified by credible sources as having significant level of corruption, tax evasion, and other criminal activity
- any country identified by credible sources as supporting TF

- any country that are identified by credible sources as tax havens

v. the business delivery methods or channels

The way the financial institution delivers its products and services affects its vulnerability to ML/TF.

The following are some indicators (not an exhaustive list) that may help to identify ML/TF risk involved with business delivery methods or channels

- non-face-to-face customers (via post, telephone, internet,) that pose challenges for verifying the identity of the account holder/customer.
- indirect relationships with customers (via intermediaries, gatekeepers, pooled accounts)

## II. Risk Assessment

24. Having identified the threats involved, financial institutions need to assess and measure ML/TF risk in terms of the likelihood (chance of the risk event occurring) and the impact (the amount of loss or damage if the risk event occurs). The risk associated with an event is a combination of the likelihood that the event will occur and the seriousness of the damage it may do.

### Likelihood scale

25. A likelihood scale refers to the potential of an ML/TF risk occurring in the business for the particular risk being assessed. Three levels of likelihood of ML/TF risk are shown below, but financial institutions can have as many scales as are necessary for their circumstances.
    i. Very likely - Almost certain;
    ii. Likely- High probability;
    iii. Unlikely- Low probability, but not impossible.

**Impact scale**

26. An impact refers to the seriousness of the damage that is likely to be caused if the ML or TF occurs. In assessing the possible impact or consequences, the assessment should be made from a range of viewpoints relevant to the business. Those set out below are not exhaustive. The impact of ML/TF occurring could, depending on the individual financial institution and its business circumstances, be rated or looked at from the point of view of:
    i. how it may affect the business in terms of financial loss relating to market perceptions (for example loss of investor confidence) and reputation or through fines or other sanctions (such as loss or suspension of business licenses) imposed by a regulator
    ii. the risk that a particular transaction may be seen to contribute to the activities of a terrorist or terrorist organizations.
    iii. the risk that a particular transaction may result in funds being used for any unlawful activity as defined in Section 33 of the FTRA
    iv. how it may affect the reputation of the financial institution if it is found to have aided, investigated, prosecuted or otherwise implicated in an illegal act, which may lead to loss of important commercial relationships (such as correspondent accounts) or being shunned by the community of customers or shareholders/investors

27. Three levels of impact of an ML/TF risk to financial institutions are shown below as an example. However, the FIU encourages financial institutions to develop their own ML/TF risk processes and assessments for dealing with certain customers/undertaking transactions in the way that best suits their business model/activities.
    i. Major- significant consequences, that inflict substantial damage, possibly resulting in the closure of the financial institution, cessation of business activities, regulatory sanctions being imposed or financial/reputational damage being experienced by the financial institution which will have a significant impact on business activities.
    ii. Moderate- moderate impact, involving substantial damage to the business and its reputation.
    iii. Minor- minor or negligible consequences or effects upon the financial institution.

28. Based on the likelihood and impact scale, it is suggested that financial institutions should assess an overall risk score. The risk rating may be used to aid decision making and help in deciding what action to take in view of the overall risk. A suggested risk rating derivation can be seen in the risk matrix *(Annex 1)*. However, institutions are encouraged to adopt their own approach to assessing, identifying and quantifying ML/TF risk. Irrespective of the methodology adopted, the FIU requires institutions to develop a framework and implement practices to effectively identify, measure, monitor, control and mitigate ML/TF risks as required by the FTRA and CDD Rules.

i. Extreme - risk almost certain to happen and/or to have very serious consequences on the financial institution, including its financial standing and reputation.
   Response: Do not allow transaction to occur/or customer relationship to be established or reduce the risk to acceptable level through risk mitigation, such as enhanced due diligence.
ii. High - risk likely to happen and/or to have serious consequences.
   Response: Do not allow transaction/establishment of customer relationship until risk reduced through risk mitigation, such as enhanced due diligence.
iii. Medium - possible this could happen and/or have moderate consequences.
   Response: Mitigate risk; normal CDD and other requirements apply.
iv. Low - unlikely to happen and/or have minor or negligible consequences.
   Response: Mitigate risk: simplified CDD and other requirements apply.

## III. Risk Mitigation

29. Once the financial institution assesses the ML/TF risk of individual customer, product/service, delivery channel and risks related to geographic region, it should develop strategies policies and procedures to manage and mitigate the risk.

Examples of a risk reduction or mitigation are:

i. Setting transaction limits for high-risk products or delivery channels

ii. Having a management approval process for higher risk customers, products, services, or deliver channels

iii. Risk rating customers and applying different requirements for high or low risk customers including applying different identification and verification methods and enhanced customer due diligence requirements

iv. Not accepting customers who wish to transact with a high-risk country or customers that are considered to be higher risk based on the institution's board-approved customer acceptance policy.

**Risk Management Strategies**

30. Financial institutions shall adopt the following components, among others, as part of their risk management strategy:

i. Develop and implement ML/TF risk management objectives at the board and senior management level of the financial institution and monitoring progress of implementation of objectives.

ii. Implement clearly defined management responsibilities and accountabilities regarding ML/TF risk management.

iii. Provide adequate staff resources to undertake functions associated with ML/TF risk management.

iv. Introduce staff reporting lines from the ML/TF risk management system level to the board or senior management level, with direct access to the board members or senior managers responsible for overseeing the system.

v. Implement procedural controls relevant to particular services and products, customers, and delivery channels that have been identified as being vulnerable to ML/TF.

vi. Documenting all ML/TF risk management policies and ensuring that these are kept up to date and reviewed regularly reflecting both the scope and nature of the institution's activities and the findings of risk assessments conducted by authorities. Such policies should also identify processes relating to non-compliance, including reporting of suspicious transactions to the FIU.

vii. Provide appropriate training programs for staff to develop expertise in the identification of ML/TF risks across the financial institution, including reporting of suspicious transactions.

viii. Develop an effective information management system which produce detailed and accurate financial, operational and compliance data relevant to ML/TF risk management.

**Enhanced and Simplified Due Diligence Measures**

31. There are circumstances where the risk of ML/TF is higher and enhanced CDD measures must be taken and, where the risks of ML/TF are lower, simplified CDD measures may be taken. These enhanced and simplified measures are outlined below:

**Enhanced due diligence measures for high risk customers/transactions**

32. Every financial institution should examine and document, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of ML/TF are higher, financial institutions should be required to conduct enhanced due diligence (EDD) measures for higher-risk business relationships which may include:

i. Obtaining and verifying additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet search, etc.)
ii. Updating more regularly the identification data of customer and beneficial owner
iii. Obtaining and verifying additional information on the intended nature of the business relationship
iv. Obtaining and verifying information on the source of funds or source of wealth of the customer
v. Obtaining and verifying information on the reasons for intended or performed transactions
vi. Obtaining and verifying the approval of senior management to commence or continue the business relationship
vii. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
viii. Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

**Simplified CDD measures for low risk customers/transactions**

33. Where the risks of ML/TF are lower, the financial institutions are, subject to the regulations, allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring).

Examples of possible measures are:

i. Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (delayed verification)
ii. Reducing the frequency of customer identification updates
iii. Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold
iv. Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established

34. Simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF, or where specific higher-risk scenarios apply.

**Annex 1**

**Overall AML/CFT Risk**