



ශ්‍රී ලංකා මහ බැංකුව  
இலங்கை மத்திய வங்கி  
CENTRAL BANK OF SRI LANKA

இலாச இடீவீ ஸீகைச  
நிதியியல் உளவறிதற் பிரிவு  
FINANCIAL INTELLIGENCE UNIT

අංක 30, ජනාධිපති මාවත, කොළඹ 01, ශ්‍රී ලංකාව  
இல. 30, சனாதிபதி மாவத்தை, கொழும்பு - 01, இலங்கை  
No. 30, Janadhipathi Mawatha, Colombo 01, Sri Lanka

Guidelines - 02/2023

Ref: 037/08/007/0001/022

September 01, 2023

To: Attorneys-at-Law / Notaries Public

Dear Sir/Madam,

**Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism  
Compliance Obligations for Attorneys-at-Law and Notaries, No. 02 of 2023**

The above guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 6 of 2006 and the Designated Non-Finance Business (Customer Due Diligence) Rules, No. 1 of 2018.

Yours faithfully,

  
Mrs. E H Mohotty

Director

Financial Intelligence

Cc: Compliance Officers

**Guidelines on Anti-Money Laundering and Countering the Financing of  
Terrorism Compliance Obligations for Attorneys-at-Law and Notaries,  
No. 02 of 2023**

**PART I**

**Introduction**

1. These Guidelines are issued pursuant to Section 15 (1) (j) of the Financial Transactions Reporting Act, No. 6 of 2006 (hereinafter referred to as “FTRA”). These Guidelines should be read together with the Designated Non-Finance Business (Customer Due Diligence) Rules, No. 1 of 2018 (hereinafter referred to as “CDD Rules”) by Gazette Extraordinary No. 2053/20, dated January 10, 2018, and any other Rules, Regulations and Guidelines issued under the FTRA, where specifically mentioned therein.
2. These Guidelines are provided as an aid to understand the CDD Rules and shall act as a guidance for the Attorneys-at-Law and Notaries as defined under Section 33 of the FTRA (hereinafter referred to as “Legal Professional (s)”) when they prepare for or carry out transactions for their clients in relation to any of the following activities as defined under subsection (j) of Designated Non-Finance Business definition provided in Section 33 of the FTRA (activities hereinafter referred to as “Captured Activities”):
  - a) Buying and selling of real estate;
  - b) Managing of client money, securities or other assets;
  - c) Management of bank, savings or securities accounts;
  - d) Organization of contributions for the creation, operation or management of companies; and
  - e) Creation, operation or management of legal persons or arrangements and the buying and selling of business entities.
3. These Guidelines are issued with the primary objective of assisting Legal Professionals in identifying, assessing and managing Money Laundering (ML) and Terrorist Financing (TF) risks, when carrying out Captured Activities. These Guidelines are applied to all Legal Professionals when they carry out the said activities for their clients.
4. These Guidelines are non-exhaustive and in no means should be interpreted as advice for any Attorney-at-Law to act contrary to the professional obligations identified under the Supreme Court (Conduct and Etiquette for Attorneys-at-Law) Rules of 1988, as amended from time to time, issued by the Supreme Court of Sri Lanka published in Gazette Extraordinary No. 535/17 of December 07, 1988 (hereinafter referred to as the Supreme Court Rules).
5. These Guidelines should be viewed as complementary to the Supreme Court Rules, more specifically the Supreme Court Rules 9, 10, 11 and 12.

6. Legal Professionals when acting as Trust or Company Service Providers (TCSPs) and providing one or more of the following services to a third party, should refer the Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism Compliance Obligations for Accountants and Trusts or Company Service Providers, No. 02 of 2020.
  - a) Formation or management of legal persons;
  - b) Acting as or arranging for another person to act as a director or secretary of a company, a partner or a partnership or a similar position in relation to other legal persons;
  - c) Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or for any other legal person or arrangement;
  - d) Acting as or arranging for another person to act as, a trustee of an express trust; and
  - e) Acting as or arranging for another person to act as, a nominee shareholder for another person.<sup>1</sup>
7. These Guidelines act as an indicative guide for the Legal Professionals to develop policies, procedures and controls in compliance with the FTRA and any regulations, rules and directives issued thereunder. Nothing in these Guidelines should be considered as consisting of legal advice from the Financial Intelligence Unit (FIU). These Guidelines should not be construed as relieving Legal Professionals from any of their obligations under the FTRA and rules and regulations issued thereunder.

### **Glossary of Terms Used in the Guidelines**

8. For the purpose of these Guidelines, unless the context otherwise requires:
  - **Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT)** refers to laws, regulations, policies and procedures that give effect to the 40 Recommendations of the Financial Action Task Force (FATF) through assessing and understanding the risk of Money Laundering and Terrorist Financing and taking steps to prevent Money Laundering and Terrorist Financing from occurring, or, where it has occurred, to detect, deter and take action against such activities, and confiscate the criminal proceeds of such activities;
  - **Beneficial Owner**<sup>2</sup> means a natural person who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a legal person or an arrangement;
  - **CDD** means Customer Due Diligence;

---

<sup>1</sup> As defined in Subsection (k) of Designated Non-Finance Business in Section 33 of the FTRA.

<sup>2</sup> As defined in FATF 40 Recommendation

- **Client** shall be synonymous with “Customer” as defined under Section 33 of the FTRA;
- **FATF** means the Financial Action Task Force, an inter-governmental body that acts as the global money laundering and terrorist financing watchdog and sets, develops, and promotes international standards and policies to protect the global financial system against the threat of money laundering, terrorist financing and financing for proliferation of weapons of mass destruction;
- **FIU** means the Financial Intelligence Unit of the Central Bank of Sri Lanka, which is designated under the FTRA, and charged with the implementation and administration of the provisions of the FTRA;
- **ML** means the offence of money laundering in terms of section 3 of the Prevention of Money Laundering Act, No 5 of 2006, as amended;
- **TF** means an act constituting an offence under section 3 of the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005, as amended;
- **ML/TF** means Money Laundering/Terrorist Financing;
- **NGOs/NPOs** means Non-Governmental Organizations/Not-for-Profit Organizations;
- **PEP** means a Politically Exposed Person, who is an individual entrusted with prominent public functions either domestically or by a foreign country, or in an international organization and includes a Head of a State or a Government, a politician, a senior government officer, judicial officer or military officer, a senior executive of a state-owned corporation, government or autonomous body but does not include middle rank or junior rank individuals;
- **STRs** means Suspicious Transaction Reports filed in terms of Section 7 of the FTRA;
- **UNSCR** means the United Nations Security Council Resolution.

### **Legal Professional’s Duty Owed to a Client**

9. Legal Professionals owe a special duty of confidentiality to their clients. Also, when undertaking any Captured Activity on behalf of a client, the Legal Professionals often act on behalf of the client and by doing so interact with other institutions that may transact with the client’s assets. This professional engagement has the potential to be abused by criminal elements intending to carry out ML/TF, which would, in turn, undermine the effectiveness of the AML/CFT framework in Sri Lanka.
10. The Legal Professionals should, at all times, act to prevent misuse and abuse of their professional services by criminal elements. Therefore, Legal Professionals should exercise due care to prevent facilitating criminal activities, especially ML/TF activities carried out by their clients. Hence, Legal Professionals have a responsibility to ensure that, when engaging in Captured Activities, the Legal Professionals fully comply with

AML/CFT obligations as per the FTRA and rules and regulations issued thereunder. Failure to do so will expose Legal Professionals to reputational risk as well as substantial penalties.

11. In complying with these obligations, the size and breadth of the professional practice does not by itself reduce the compliance obligations of the Legal Professionals. It may, however, impact the assessment of ML/TF risks faced by the Legal Professionals along with other factors such as the area of legal practice, diversity in scale, and the functions engaged in. Therefore, the Legal Professionals may look to introduce adequate risk mitigation measures considering the varying circumstances surrounding individual professional practice. A “one-size-fits-all” approach will not function well to mitigate ML/TF risks faced.

## **PART II**

### **Knowing Your ML/TF Risk Using a Risk-Based Approach**

12. The AML/CFT processes engaged by the Legal Professionals when carrying out the Captured Activities shall be risk-based in terms of the measures specified in Rule 4 - 7 of the CDD Rules. A risk-based approach allows the Legal Professionals,
  - to identify and assess the risks of exposure to ML/TF;
  - to develop suitable policies, procedures and controls to effectively manage and mitigate such risks; and
  - to monitor the ongoing effectiveness of those policies, procedures and controls.
13. (1) The Legal Professionals are expected to use their own professional judgment, knowledge and expertise to develop an appropriate risk-based approach for their particular organizational structure and business/professional activities based on the nature, scale and complexity of the Legal Professionals practice and/ or Captured Activities. Some of the factors that could be considered when developing a risk-based approach are as follows:
  - Risks related to the overall size, geographic areas of practice, and organizational complexity of the Legal Professionals practice,
  - Risks related to the specific services offered or transactions engaged by the Legal Professionals,
  - Risk related to the specific types of the client,
  - Risks related to the delivery channels of the client(s).
- (2) These factors can be considered either independent of one another or in combination in order to determine ML/TF risk.

For example, a Legal Professional that incorporates one or more Captured Activities as components of the services offered to clients, and where it is observed that the client has a complex or unusual ultimate beneficial ownership, or a known political

exposure, and where the client is operating in a high risk or monitored jurisdictions,<sup>3</sup> and where the client is functioning in a business sector that has a high- ML/TF risk exposure, could be more vulnerable to ML/TF risks than a Legal Professional that is exposed to only one of these risk categories.

- (3) In the context of ML/TF, the risk-based approach encompasses the following steps:
- A. Identify the ML/TF risks;
  - B. Assess the ML/TF risks;
  - C. Design and implement controls to manage and mitigate the ML/TF risks proportionate to the assessment of those risks;
  - D. Regularly review and update the effective operations of the risk-based controls.

#### **(A) Identifying the ML/TF Risk**

14. As the first step of the risk-based approach, the Legal Professionals should be able to identify their direct and indirect ML/TF risk factors. A sample checklist for ML/TF risk identification and assessment is provided within **Annexure I** as a guidance. Legal Professionals are encouraged to develop a checklist of their own, based on their own experience and expertise, for ML/TF risk identification and assessment, and to this end **Annexure I** would provide some guidance.

#### **(B) Assessing the ML/TF Risks**

15. As per the Rule 6 (a) of the CDD Rules, a ML/TF risk assessment is required to be carried out once the Legal Professionals enter into a professional business relationship with a client considering all relevant risk factors of the client. The relationship can be a one-time transaction or a continuing relationship.
16. The ML/TF Risk Assessment is an analysis of potential threats and vulnerabilities of ML/TF, to which, the Legal Professionals are exposed. The complexity of the ML/TF Risk Assessment depends on, among others, the nature, size, and the type of ML/TF risks faced by the Legal Professionals.
17. When conducting an ML/TF Risk Assessment, the Legal Professionals are required to consider and document the following:

---

<sup>3</sup>The FATF identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in two FATF public documents. For more information and to obtain the latest updated list of high risk and other monitored jurisdictions please refer the FATF website: [http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc\(fatf\\_releasedate\)](http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)).

Figure 1

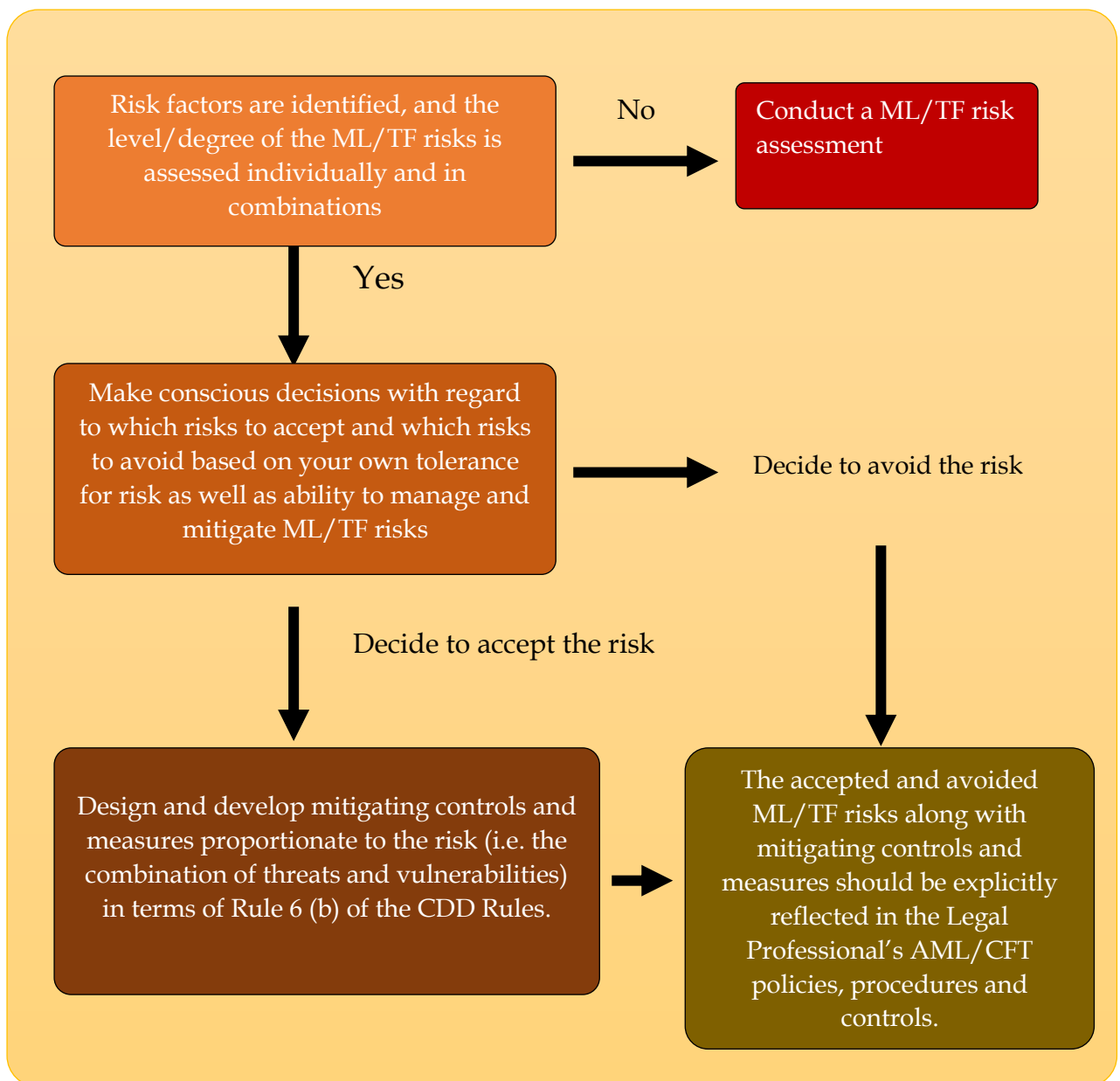
<b>Aspects to be Considered When Conducting the ML/TF Risk Assessment</b>
<ul style="list-style-type: none"><li>• Types of clients, their beneficial owners, and nature of business relationships.</li></ul>
<ul style="list-style-type: none"><li>• Types of services offered by the Legal Professionals.</li></ul>
<ul style="list-style-type: none"><li>• Delivery channel(s) of services offered by the Legal Professionals (e.g. face to face or non-face-to-face).</li></ul>
<ul style="list-style-type: none"><li>• The geographic origins and locations of the clients and their beneficial owners.</li></ul>
<ul style="list-style-type: none"><li>• Other relevant factors related to the activities conducted by the Legal Professionals.</li></ul>
<ul style="list-style-type: none"><li>• The client or beneficial owners' presence in list of designated individuals or entities issued under United Nations Security Council Resolutions.</li></ul>
<ul style="list-style-type: none"><li>• The political exposure of the client and client's ultimate beneficial owners.</li></ul>

18. The ML/TF Risk Assessment requires detailed knowledge of the business operations of the client and informed judgment exercised by the legal professional so that the level of risks for ML/TF can be determined according to each individual factor as well as a combination of factors. The ML/TF Risk Assessment will continuously change over time as the various risk factors evolve and change over the course of time.
19. Where the Legal Professional's dealing with a client is limited to a single transaction (one-off transaction), it is not considered to be an ongoing business relationship. If the Legal Professionals have reasonable ground to suspect that the transaction is linked to commission of or, an attempt to commit, or carried out in furtherance to an unlawful activity or to an ML/TF offence, then the transaction is required to be reported to the FIU as an STR. (Please refer to **Part VII** for further information).



**(C) Designing and Implementing Controls to Manage and Mitigate the ML/TF Risks**

Figure 2





20. The following are several approaches of ML/TF risk mitigations that the Legal Professionals are required to develop and implement through their AML/CFT policies, procedures and controls.
- a) Informing senior management/senior partners about compliance initiatives, identified compliance deficiencies and corrective actions taken, as well as specific high-risk situations (e.g. engagement with PEPs) that require their approval;
  - b) Subjecting new clients to in-depth interviews to identify beneficial ownership and source of funds and to provide a basis for risk-based verification of their claims.
  - c) Ensuring the continuation of the AML/CFT policies, procedures and controls without disruptions due to changes in management, employees or the structure of the Legal Professionals;
  - d) Incorporating AML/CFT compliance responsibilities into job descriptions of the employees and performance measurement practices of the Legal Professionals;
  - e) Increasing awareness of high-risk situations within the Legal Professionals through training, participating in industry focus groups, and other forms of awareness-raising;
  - f) Establishing criteria for risk-rating updates for ongoing client relationships. (Please refer **Part VI** for more details on Customer Risk profiling).

**(D) Monitor and Improve the Effective Operations of the Risk Based Controls**

21. The effective management of ML/TF risk is a continuous and dynamic process. The Legal Professionals are required to ensure that the management of ML/TF risks is subject to regular reviews of effectiveness and is updated as new or emerging risks are identified, whether caused by changes in the scale or nature of operations, new types of services, new customer types, etc. Changes to client acceptance policies or practices or a geographic expansion of the Legal Professionals are required to, for example, trigger an update of the risk assessment and risk-based controls.

**PART III  
Compliance**

**Compliance Officer**

22. In terms of Section 14 (1) (a) of the FTRA and Rule 41 of the CDD Rules, every Legal Professional is required to appoint a Compliance Officer, who works at a senior management/senior partner level, to ensure the compliance of the Legal Professional with the provisions of the FTRA and rules and regulations issued thereunder. According to the management structure of the Legal Professionals, Compliance Officer

is required to be in a position to have direct access to senior management or to the senior partner of the Legal Professionals. Therefore, the Compliance Officer position is required to be of the senior management level. Compliance Officer function entails responsibilities cast upon it in terms of the FTRA. Therefore, the Compliance Officer should possess sufficient expertise and capacity to discharge this function.

23. Legal professionals who work independently is required to appoint himself as the Compliance Officer.
24. The Compliance Officer is responsible for the establishment and maintenance of the procedures and systems for the Legal Professional to comply with AML/CFT requirements. Moreover, The Compliance Officer is required to monitor AML/CFT measures of the Legal Professional in order to ensure that those AML/CFT measures are effectively implemented and up to date and the Compliance Officer requires the authority and the resources necessary to discharge his or her responsibilities effectively.
25. The Legal Professionals are required to declare the initial appointment of the Compliance Officer and any subsequent change thereof to the Director of the FIU through the Compliance Officer Declaration Form (**Annexure II**) via email to [fiudnfbp@cbsl.lk](mailto:fiudnfbp@cbsl.lk) followed with a hard copy by post to the Director, Financial Intelligence Unit, Central Bank of Sri Lanka, No. 30, Janadhipathi Mawatha, Colombo 01. The appointment is required to be formally made and responsibility is required to be incorporated to the Compliance Officer's Job Description.

## **PART IV**

### **AML/CFT Compliance Policy, Procedures and Controls**

26. In terms of Rule 6 (f) of the CDD Rules, Legal Professionals are required to develop an AML/CFT Compliance Policy and maintain it as a document. The policy is expected to be fully and effectively implemented by the Legal Professionals using procedures and controls that are communicated timely, understood and followed by relevant staff of the Legal Professionals to prevent, detect and remedy instances of non-compliance.
27. When Legal Professionals maintain any local or overseas branches/offices, the Legal Professionals are required to establish a Group AML/CFT Compliance Policy to ensure that all branches /offices implement the same AML/CFT measures, consistent with local laws and regulations.
28. If the applicable laws and/or regulations of an overseas branch/office contradict or otherwise limit the application of Sri Lankan laws and/or rules, Legal Professionals are required to act as specified in the CDD Rules.
29. The AML/CFT Compliance Policy, procedures and controls are required to be established to manage and mitigate the risks related to ML/TF identified at the ML/TF Risk Assessment. This ML/TF Risk Assessment is carried out irrespective of any

existing policies, procedures and controls on customer identification, record keeping and reporting requirements.

30. The extent and the level of details of each Legal Professional's AML/CFT Compliance Policy, procedures and controls would depend on the specific circumstances of the Legal Professional, as well as the Legal Professional's assessed risk to ML/TF.
31. The Legal Professional's AML/CFT Compliance Policy, procedures and controls are required to be approved by the senior management/senior partners and/or proprietor. The AML/CFT Compliance Policy, procedures and controls are required to include, at a minimum, the areas specified under Rule 6 (g) of the CDD Rules.
32. The Legal Professional's senior management/senior partners and/or proprietor are required to understand statutory duties related to AML/CFT compliance vested upon the senior management/senior partners and/or proprietor, the staff and the Legal Professional himself. Senior management/senior partners and/or proprietors are ultimately responsible for making decisions related to AML/CFT Compliance Policy, procedures and controls that mitigate and manage the risks of ML/TF within the Legal Professionals.
33. The AML/CFT policies, procedures and controls described in the AML/CFT Policy documents of the Legal Professionals are required to be reviewed and updated as an ongoing process to ensure that they commensurate with emerging ML/TF threats and vulnerabilities.

## **PART V**

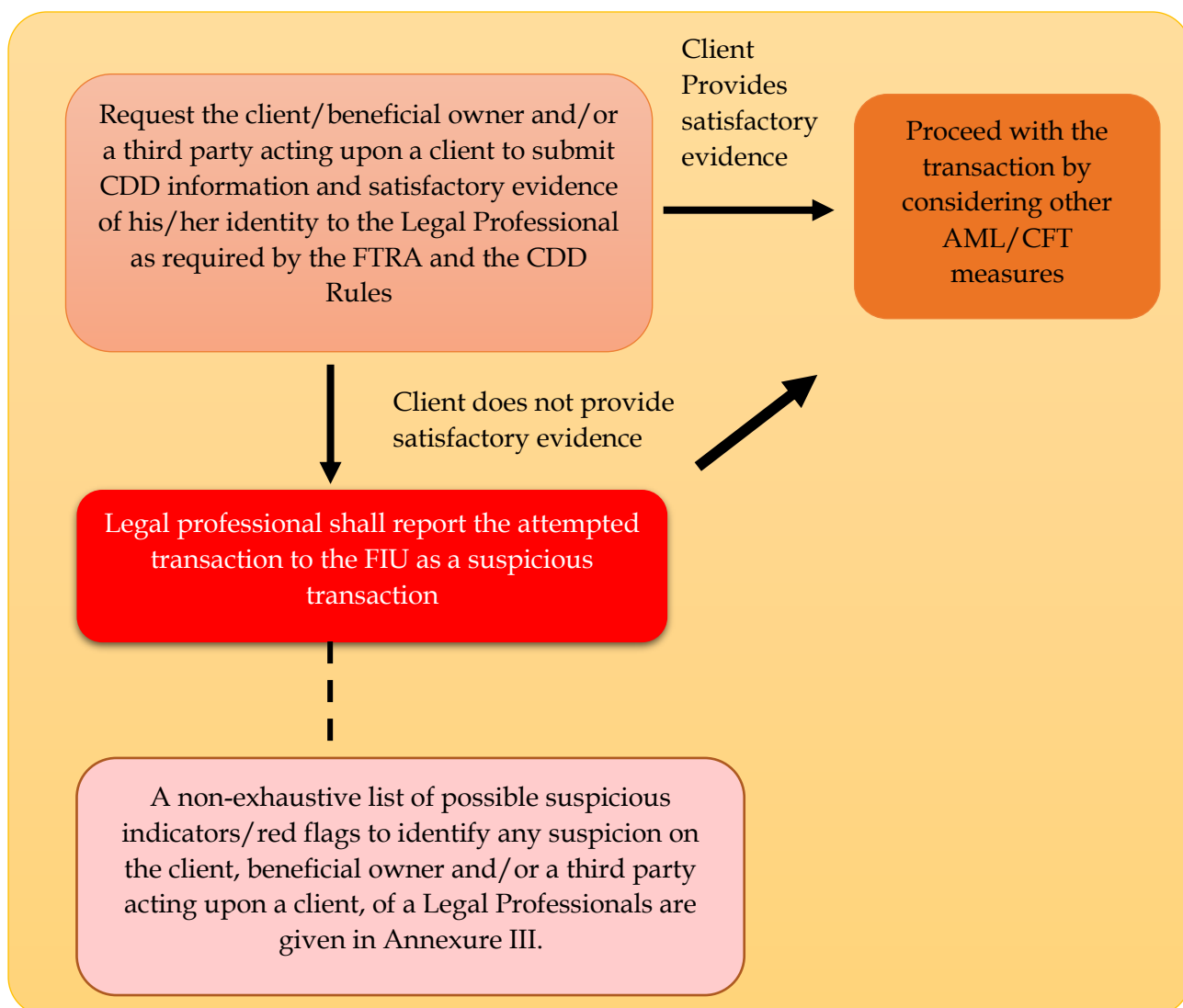
### **Customer Due Diligence**

#### **Identification and Verification of Client, Beneficial Owners and Third Party Acting upon the Client**

34. Legal Professionals, when carrying out the Captured Activities, are required to conduct CDD on their clients including occasional and one-off clients, beneficial owners and/or a third party acting in concert with a client as specified in Part II of the CDD Rules.
35. In cases where a third party is involved, the Legal Professionals are required to obtain information on the identity of the third party and their relationship with the ultimate beneficial owner and verify such information using reliable, independent source documents. The Legal Professionals are also required to review and establish the authenticity of enforceable documents demonstrating the authority of the third party to act on behalf of the ultimate beneficial owner. The Legal Professional is also required to obtain documentary evidence to the effect that the respective third party has authorization to act on behalf of the client.
36. If CDD information and the satisfactory evidence of the identity of the client/beneficial owner and/or a third party acting upon a client as required by the

FTRA and the CDD Rules, are not submitted, then the Legal Professional shall report the attempted transaction to the FIU as a suspicious transaction.

Figure 3



37. Clients, beneficial owners and third parties acting upon clients that are identified as high risk are required to be subject to Enhanced CDD measures as specified in Rule 16 of the CDD Rules.
38. Legal Professionals are required to conduct ongoing CDD on existing clients by regularly reviewing and updating CDD information and monitoring transactions to ensure consistency with the client profile.
39. CDD is required to be conducted prior to or at the time of establishing a client relationship. Legal Professionals may use their own professional judgment and discretion to determine the point at which a relationship has been established with a client. Generally, a client relationship begins after initial inquiries have been made by the prospective client but before any services have been rendered.

## **Client Risk profiling**

40. Legal Professionals are required to create individual risk profiles of their clients and based on the results of their CDD process as per Rule 6 (c) of the CDD Rules. The risk profiles should then be grouped into risk categories and subjected to documented risk controls for that category. It is never acceptable to alter a client risk profile for the purpose of avoiding controls that might damage a client or potential client relationship. (A sample of a client risk profiling format is Annexed at **Annexure IV**). Upon the initial acceptance of the client, the client's risk profile is required to be regularly reviewed and updated based on their level of ML/TF risks.

## **Enhanced CDD Measures**

41. Where a client is identified as high risk with respect to the client risk profiling, the Legal Professionals are required to apply Enhanced CDD measures as specified in the CDD Rules.

42. Specific measures to be taken in conducting Enhanced CDD are elaborated in Rule 16 of the CDD Rules.

43. Examples of situations where Enhanced CDD measures are required to be taken with respect to clients, beneficial owners or relevant third parties acting upon clients:

- a) Links with countries which do not or which insufficiently comply with the recommendations of the FATF<sup>4</sup>;
- b) Links with a country that has been identified by a national authority as a jurisdiction of concern for drug trafficking, human trafficking, money laundering, terrorism or illicit financing;
- c) Links with a country that has been identified by an organization as having high levels of public corruption;
- d) Unnecessarily complex transactions, unusual transactions, (whether completed or not), unusual patterns of transactions for the customer profile, transactions that match patterns associated with unlawful activity, and transactions which have no apparent lawful purpose;
- e) Clients who are domestic or foreign Politically Exposed Persons including their immediate family members and close associates;
- f) Clients whose risk profile identifies them as posing a higher risk to the Legal Professionals;
- g) Transactions where the natural person is not physically present in conducting the Captured Activity.

---

<sup>4</sup> Please refer the FATF website for more information and to obtain the latest updated list of High risk and monitored jurisdictions: [http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc\(fatf\\_releasedate\)](http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate))

- h) When entering into relationship with and conduct transactions with NGOs/NPOs.
- i) Where an existing client provides unsatisfactory information relating to CDD.

### **Compliance with United Nations Security Council Resolutions**

44. As per the Rule 42 of the CDD Rules, every Legal Professional is required to verify whether any client/beneficial owner/third party who acts upon the client appears on any designated list issued in compliance with the United Nations Act, No. 45 of 1968, with respect to any designated list on targeted financial sanctions related to terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing and any other subsequent Resolutions.
- a) The United Nations Regulations No. 01 of 2012  
([http://fiusrilanka.gov.lk/docs/UNSCR/Regulations/1758/1758\\_19\\_\(E\).pdf](http://fiusrilanka.gov.lk/docs/UNSCR/Regulations/1758/1758_19_(E).pdf))
  - b) The United Nations Regulations No. 02 of 2012  
([http://fiusrilanka.gov.lk/docs/UNSCR/Regulations/1760/1760\\_40\\_\(E\).pdf](http://fiusrilanka.gov.lk/docs/UNSCR/Regulations/1760/1760_40_(E).pdf))
  - c) United Nations (Sanctions in relation to Democratic People's Republic of Korea) Regulations of 2017  
([http://fiusrilanka.gov.lk/docs/UNSCR/Regulations/2039\\_32/2039\\_32\(E\).pdf](http://fiusrilanka.gov.lk/docs/UNSCR/Regulations/2039_32/2039_32(E).pdf))
  - d) United Nations (Sanctions in relation to Iran) Regulations No. 1 of 2018  
([http://fiusrilanka.gov.lk/docs/UNSCR/Regulations/2080\\_34/2080\\_34\(E\).pdf](http://fiusrilanka.gov.lk/docs/UNSCR/Regulations/2080_34/2080_34(E).pdf))
45. The designated lists issued by the Ministry of Defence of Sri Lanka under the above regulations can be referred via <http://fiusrilanka.gov.lk/unscr.html>
46. The Legal Professionals are required to ensure that no funds, financial assets or economic resources are made available to or for the benefit of such designated persons or entities, or their beneficiaries. In the event of an attempted transaction by or for a designated individual or entity, Legal Professional are required to, not later than 24 hours from the time of finding out such client, inform to the Competent Authority with a copy to the FIU.
47. The contact details of Competent Authority are as follows,
- Office of the Competent Authority,  
Ministry of Defence,  
Defence Headquarters Complex,  
Sri Jayawardenepura,  
Kotte.  
Tel. + 94 11 2430860 up to 69 and + 94 11 2430870 up to 78  
Fax +94 112390288  
email: [reachus@defence.lk](mailto:reachus@defence.lk)

## **PART VI**

### **Reporting**

#### **Duty of Submitting Suspicious Transactions Reports**

48. In terms of Section 7 of the FTRA and Rule 14 of the CDD Rules, Legal Professionals are required to submit Suspicious Transactions Reports (STRs) to the FIU.
49. Legal Professionals are required to review and follow Guidelines issued by the FIU on Suspicious Transaction Reporting. The Guidelines for Designated Non-Finance Businesses on Suspicious Transactions Reporting, No. 01 of 2019 can be viewed via the link <http://fiusrilanka.gov.lk/docs/Guidelines/2019/Guideline-01-2019.pdf>
50. Suspicious Transactions are required to be reported at the time of its formation regardless of whether the activity/ transaction that gave rise to such suspicion has actually been completed. For example, if the suspicion is formed when establishing the business relationship with a client, that suspicion is required to be reported regardless of whether the relationship is actually established. Similarly, if discussions and events surrounding a potential transaction cause formation of a suspicion then that suspicion is required to be reported at the time of formation regardless of the eventual completion or non-completion of any transaction.
51. STRs need to be submitted using the format as prescribed in Suspicious Transactions (Format) Regulations of 2017, Gazette (Extraordinary) No: 2015/56 dated April 21, 2017 (**Schedule V-Annexure V**).
52. The CO appointed under Section 14 of the FTRA is required to submit the STR on behalf of the Legal Professional and also is required to maintain a register of STRs including the records of the STRs submitted to the FIU.

## **PART VII**

### **Record Keeping**

53. The Legal Professionals are required to take appropriate steps to keep records for six years as described in Section 4 of the FTRA and Part III of the CDD Rules. Records maintained should carry CDD information, copies of identification documents, transaction records, correspondence relating to transactions and any other report furnished to the FIU.



Figure 4

Type of Record	Retention Period
CDD information	6 years from the date of closure of the account or cessation of the business relationship
Transaction Records	6 years from the date of transaction
Correspondence relating to the transactions	6 years from the date of correspondence
Reports furnished to the FIU	6 years from the date of furnishing the report

54. Any record which is subject to an on-going investigation or litigation or required to be produced in a court of law or before other appropriate authority such record shall be retained until such time the Legal Professional is informed by the relevant authority that such records are no longer required.

## PART VIII

### Other AML/CFT Requirements

55. Legal Professionals are required to have a screening policy when hiring employees as specified in Rule 6 (g) (iv) of the CDD Rules to ensure that the employees are not involved in any ML/TF activity.
56. Legal Professionals are required to provide training on AML/CFT compliance to the senior management/senior partners, employees, agents or any other individual authorized to act on behalf of the Legal Professional.
57. Such training is required to include raising awareness of the AML/CFT Compliance Policy, procedures and controls of the Legal Professional for preventing and managing risk of ML/TF. Training programmes are expected to provide a clear understanding of individual responsibilities with respect to AML/CFT and foster a culture where all the employees of the Legal Professional work towards effective implementation of all AML/CFT measures.
58. Legal Professionals are required to maintain an independent audit function, as specified in Rule 6 (g) (v) of the CDD Rules, to ensure that their AML/CFT functions are audited.
59. The Compliance Officer of the Legal Professional needs to take the leading role in conducting AML/CFT related training and awareness sessions.

## PART IX

### Role of FIU

60. The FIU is entrusted with the administrative powers of the FTRA to act as national agency for implementing AML/CFT obligations in Sri Lanka. Accordingly, FIU is the AML/CFT supervisor for Attorneys-at-Law and Notaries that are reporting entities under Section 33 of the FTRA. The FIU performs the following functions to ensure a sound AML/CFT regime in Sri Lanka.

Figure 5

Functions of the FIU
Review and amend relevant Acts, Regulations and Rules on AML/CFT in line with current market developments and international best practices and coordinate the issuance of the same.
Facilitate country's compliance with AML/CFT international standards and best practices.
Disseminate financial intelligence to appropriate Law Enforcement Agencies (LEAs) and Supervisory Authorities (SAs) after conducting strategic and operational analysis.
Implement Risk-Based AML/CFT Supervision in Financial Institutions (FIs) and DNFBPs to combat ML/TF in Sri Lanka.
Implement provisions of the Targeted Financial Sanctions in United Nations Security Council Resolutions (UNSCRs)
Strengthen the domestic coordination and international cooperation on AML/CFT related matters.
Conduct awareness programmes for stakeholders including FIs, DNFBPs, LEAs and SAs
Issue the FIU publications including the FIU Annual Report.

61. The contact details of the FIU are as follows,

Financial Intelligence Unit of Sri Lanka,  
Central Bank of Sri Lanka,  
No.30, Janadhipathi Mawatha,  
Colombo 01.  
Tel. +94112477509  
Fax +94112477692  
email: [fiudnfbp@cbsl.lk](mailto:fiudnfbp@cbsl.lk)  
Website : <http://fiusrilanka.gov.lk/index.html>.

## PART X

### Privileged Communication and Professional Secrecy

62. Privileged communication and professional secrecy are entrenched in the Attorney-client relationship. Hence, the actions and behaviors discussed in these Guidelines would apply without any contradiction to Rules 31-38 of the Supreme Court Rules of 1988, as amended, and to Section 126 of the Evidence Ordinance.
63. Further to the above, Section 13 of the FTRA states that -
- “Nothing contained in Sections 4, 5, 6, 7 or 8 of the FTRA shall be construed as requiring a lawyer to disclose any privileged communication only if,*
- a. it is a confidential communication, whether oral or in writing, passing between,*
    - i. a lawyer or a legal advisor in his or her professional capacity and another barrister, solicitor, lawyer, attorney or legal advisor in such capacity; or*
    - ii. a lawyer or a legal advisor in his or her professional capacity and his or her client, whether made directly or indirectly through an agent of either; and*
  - b. it is made or brought into existence for the purpose of obtaining or giving legal advice or assistance; and*
  - c. it is not made or brought into existence for the purpose of committing or furthering the commission of some illegal or unlawful act.”*
64. However, Legal Professionals are required to give their special attention to Section 13 (3) of the FTRA.
- “Where the information consists wholly or partly of, or relates wholly or partly to receipts, payments, income, expenditure, or financial transactions of a person (whether a lawyer his or her client, or any other person), it shall not be a privileged communication if it is contained in, or comprises the whole or part of any book, account, statement or other record prepared or kept by the lawyer in connection with a trust account of the lawyer”*
65. There may be instances where within a single matter, privilege may attach to some but not for all communications and advice. Hence, Legal Professionals are required to clearly understand the instances where privileged communication and professional secrecy apply.
66. By profession, many Legal Professionals identify their clients and provide legal advice to them. If a Legal Professional provides professional advice to a client that helps the client to breach AML/CFT obligation, that Legal Professional may, depending on the Legal Professional’s state of knowledge, liable to be treated as an accomplice to the violations/offending ensuring.
67. In situations where Legal Professionals are claiming Legal Professional privilege or professional secrecy, they must be satisfied that the information is protected by the privilege/professional secrecy and the relevant rules. Otherwise, it can be treated as a breach of AML/CFT obligations.

Issued on September 01, 2023

## Annexure I

### Sample Institutional ML/TF Risk Assessment for Legal Professionals.

The following checklist is intended to provide an example of how to assess risk for your client, products, services, delivery channels and geographic locations. This is only a starting point and the Legal Professional should customize the checklist according to your business. If you already use another risk assessment tool, you can continue to use it or enhance it as necessary.

When risk indicators are high or medium, you should consider risks for money laundering or terrorist financing and appropriate risk responses in the form of policies, procedures and controls to avoid or to control and mitigate the risks, as appropriate for your practice.

	Risk Factor	Institutional Risk	Risk Indicator			Risk Mitigating Measure
			High	Medium	Low	
<b>1) Assessing nature, size and complexity of the Legal Professional</b>						
1.1	Size of the professional chamber					
1.2	Value, volume and velocity of the transactions associated with the chamber					
1.3	Complexity of the professional/ business relation undertaking					
1.4	Possibility of using business data or annual report data to assess ML/TF risk of the Institution/ professional engagement					
1.5	Nature of the business transactions and activities recognised as being associated with ML/TF vulnerability					
<b>2) Client Risk</b>						
2.1	Ownership structure					
2.2	Clients in high-risk occupations					
2.3	International business transactions					
2.4	Clients reside in high-risk jurisdiction					

	Risk Factor	Institutional Risk	Risk Indicator			Risk Mitigating Measure
			High	Medium	Low	
2.5	Politically Exposed Persons (PEPs)					
2.6	Clients are located in a known high crime rate area					
2.7	Client do not have an address or who have several addresses without justified reason					
2.8	Clients have a criminal records or links to organized crime					
2.10	High net worth clients and whether they are connected to high-risk industries					

### 3) Risk Emanating from Services Offered

3.1	Services identified as presenting heightened risk by the AML/CFT supervisors					
3.2	Services support physical cash deposits and/or withdrawals					
3.3	Services which provide international funds transfer capability					
3.4	Services support payments to/from third parties or non-clients					
3.5	Services support transactions that can be conducted remotely or without interaction with a legal professional					
3.6	Services allow high-value, high-volume					

	Risk Factor	Institutional Risk	Risk Indicator			Risk Mitigating Measure
			High	Medium	Low	
	and high-velocity transactions					
3.7	Services operate using commission-based remuneration					
3.8	Services make difficult to identify clients such as support the pooling of funds and investments					
3.9	Services targeted to offshore clients					
3.10	Services assist in the establishment of a company					
3.11	Perform tasks of real estate transfer between clients in an unusually short time period without visible legal, economic or other justified reason					
3.12	Provide services linked with establishing, operating or managing of a shell company, company in nominal ownership.					
3.13	Conducts transactions without clear commercial rationale					
<b>4) Delivery Channels/Business Relationships Risk</b>						
4.1	Method of delivery remove or minimise face-to-face contact with the client					
4.2	Third party can use delivery channels					

	Risk Factor	Institutional Risk	Risk Indicator			Risk Mitigating Measure
			High	Medium	Low	
4.3	Delivery channels involve complicated financial transactions					
4.4	Delivery channels involve cross-border payments					
4.5	Delivery channels involve cash payments					
<b>5) Geographical Risk</b>						
5.1	Dealings with countries that have weak or ineffective AML/CFT measures or subject to sanctions, embargoes or similar measures issued by the United Nations Security Council Resolution (UNSCR)					
5.2	Dealings with countries that have a high degree of organised crime or drug related crime or high degree of people trafficking or smuggling					
5.3	Dealings with countries that have a high degree of corruption and bribery					
5.4	Dealings with countries that are in a conflict zone or have significant terrorism activity or as providing funding or support for terrorist activities					
5.5	Any country identified as a financial secrecy haven or jurisdiction					



## Notes to the Risk Assessment

	Risk Factor	Description on the Risk Factor
<b>1) Assessing Nature, size and complexity of the Institution</b>		
1.1	Size of the professional chamber	The larger the business, possibility of occurring suspicious activities and transactions during business is high. Large organizations may have difficulty in implementing AML/CFT measures to meet AML/CFT requirements.
1.2	Value, volume and velocity of the transactions associated with the chamber	Capacity for high-value, high-volume and high-velocity transactions have a potential ML/TF risk on the business. Individually, each variable presents possible avenues of ML/TF, and this risk is compounded in combination.
1.3	Complexity of the professional/ business relation undertaking	Greater complexity decreases the transparency of business transactions and activities, increases ML/TF vulnerability and may reduce the effectiveness of AML/CFT measures.
1.4	Possibility of using business data or annual report data to assess ML/TF risk of the Institution/ professional engagement	Availability of business data or annual report data to measure the level of ML/TF risk exposure (as an example business data can indicate how many of your clients have use of this service, how many of them are from high-risk jurisdictions)
1.5	Nature of the business transactions and activities recognized as being associated with ML/TF vulnerability	Business transactions or activities which have been identified as high or medium level vulnerable to ML/TF during the National Risk Assessment.
<b>2) Client Risk</b>		
2.1	Ownership structure	Complex and non-transparent structures may hide and disguise beneficial ownership/effective control and disguise ML/TF activities. Client may establish legal entities in a chain of multi-jurisdictional structures to hide the true ownership and control of assets held overseas.
2.2	Clients in high-risk occupations	Some occupations can have greater vulnerability to ML/TF. (For example, cash intensive businesses, gatekeeper occupations, jewelers, high-value goods dealers, real estate agents, travel agents, import/export companies, remitters and money service businesses)
2.3	International business transactions	Client operating in international level may exposed to high ML/TF risks and encounter regulation and law enforcement in different jurisdictions. Therefore, this may create unnecessary complexity and confusion with regard to ML/TF risk.


	<b>Risk Factor</b>	<b>Description on the Risk Factor</b>
2.4	Clients reside in high-risk jurisdiction	Client resides in a high-risk jurisdiction create a higher level of ML/TF vulnerability to the Institution.
2.5	Politically Exposed Persons (PEPs)	PEPs and their relatives and close associates can mean greater vulnerability to ML/TF
2.6	Clients are located in a known high crime rate area	Clients reside in a knowing area for high crime rate may create a higher level of ML/TF vulnerability to the Institution.
2.7	Client do not have an address or who have several addresses without justified reason	It is difficult to track down the true identity of a client who does not have an address or who have several addresses. This will result ML/TF vulnerability to the Institution.
2.8	Clients have a criminal records or links to organized crime or convicted by a Court.	When the clients have prior criminal records or links to organized crimes there is a high potential that these types of clients may present high ML/TF risk.
2.10	High net worth clients and whether they are connected to high-risk industries	High net worth clients (including heads of international organizations) can present a range of risks from illegal capital flight to high-level corruption and this risk is compounded by high-risk industries.
<b>3) Services risk</b>		
3.1	Level of engagement with the Services specified by the Section 33 of the FTRA.	Higher the level of engagement with the Services specified by the FTRA among other services provided by your Institution, higher the ML/TF risk.
3.2	Services support physical cash deposits and/or withdrawals	The ease of movement of cash without audit trail makes it highly vulnerable to ML/TF activity. If the offered services by your Institution provide platform to deposit or obtain cash (e.g. at ATMs, at point of sale, or through a cash advance transaction) then ML/TF risk of such occasions should be considered. When these cash transactions are in large amounts it will compound the ML/TF risk.
3.3	Services which provide international funds transfer capability	When services enable funds to be transferred to a jurisdiction outside of the country (e.g. using wire transfers or high-value commodities) this may be considered an ML/TF risk.
3.4	Services support payments to/from third parties or non-clients	This can disguise the beneficial ownership or effective control of funds. The presence of multiple intermediaries and agents can hide and disguise beneficial ownership.
3.5	Services support transactions that can be conducted remotely or without interaction with a reporting entity	Less face-to-face interaction with a client increases vulnerability to ML/TF activity. Especially online activity can facilitate high-frequency and high-value activity on an international level, often with little or no interaction between the Institution and client.

	<b>Risk Factor</b>	<b>Description on the Risk Factor</b>
3.6	Services allow high-value, high-volume and high-velocity transactions	The value, volume and velocity of transactions and activities are key indicators and warnings of ML/TF activity. You should consider these elements individually and in combination.
3.7	Services operate using commission-based remuneration	A conflict of interest between effective AML/CFT measures and commercial gain may lead to AML/CFT measures being ignored or reduced in order to gain/maintain business.
3.8	Services make difficult to identify clients such as support the pooling of funds and investments	This can disguise the beneficial ownership of funds. As an example, creation of trust account or client account. This can enable criminals to place money within the financial system with fewer questions being asked because of the perceived respectability and legitimacy of the source of funds.
3.9	Services targeted to offshore clients	Having clients offshore may expose your business to ML/TF risks that are beyond your control, especially in connection with jurisdictions with AML/CFT deficiencies, high levels of corruption and bribery and organized crime.
3.10	Perform tasks of real estate transfer between clients in an unusually short time period without visible legal, economic or other justified reason	Purchasing and re-selling of real estate is a ML/TF technique. This may add layers to the transaction and create difficulty to identify criminals. Therefore, it is better to be conscious on such transactions.
3.11	Provide services linked with establishing, operating or managing of a shell company, company in nominal ownership.	This can disguise the beneficial ownership of funds as both shell companies and company in nominal ownership may be easily used for illegal purposes such as ML.
3.12	Conducts transactions without clear commercial rationale	Criminals do several transactions to add layers and hide criminal earned money. This will create a high ML/TF vulnerability.
<b>4) Delivery Channels/Business Relationships Risk</b>		
4.1	Method of delivery remove or minimize face-to-face contact with the client	Less face-to-face interaction with a client increases vulnerability to ML/TF activity.
4.2	Third party can use delivery channels	This may result in your client's identity, beneficial owner or effective controller not being transparent, which increases ML/TF risk.
4.3	Delivery channels involve complicated financial transactions	Complicated financial transactions in delivery channels create high ML/TF vulnerability.

	<b>Risk Factor</b>	<b>Description on the Risk Factor</b>
4.4	Delivery channels involve cross-border payments	Payments involving cross-border transactions especially in connection with jurisdictions with AML/CFT deficiencies, high levels of corruption and bribery and organized crime.
4.5	Delivery channels involve cash payments	The ease of movement of cash without audit trail makes it highly vulnerable to ML/TF activity. If there are high volume cash payments involved, then ML/TF risk of such occasions should be considered.
<b>5) Geographical Risk</b>		
5.1	Dealings with countries that have weak or ineffective AML/CFT measures or subject to sanctions, embargoes or similar measures issued by the United Nations Security Council Resolution (UNSCR)	You should consider which jurisdiction your client is from, or is resident in, when assessing ML/TF risk. Some countries have been identified by the Financial Action Task Force (FATF) as non-cooperative in the fight against money laundering or terrorist financing. Therefore, it should be checked whether the FATF has assessed the specific jurisdiction as having AML/CFT deficiencies. Further, UNSCR sanction list also have to be checked.
5.2	Dealings with countries that have a high degree of organised crime or drug related crime or high degree of people trafficking or smuggling	The presence of a high level of organised crime is an important consideration in determining country risk.
5.3	Dealings with countries that have a high degree of corruption and bribery	The presence of a high level of bribery and corruption is an important consideration and a primary driver in determining country risk. Bribery and corruption fundamentally weaken any AML/CFT regime.
5.4	Dealings with countries that are in a conflict zone or have significant terrorism activity or as providing funding or support for terrorist activities	Conflict zones present an extremely high risk of TF and ML. Tracing the flow of funds into and through these regions is extremely difficult. NGO/NPOs operating in these zones may be vulnerable to abuse or used as cover.
5.5	Any country identified as a financial secrecy haven or jurisdiction	Financial secrecy is one of the main component of ML/TF. Therefore, it has to be more vigilant when dealing with such jurisdictions.

## Annexure II

### Compliance Officer Declaration Form

 <p>Financial Intelligence Unit මූල්‍ය මුද්ධි ඒකකය நிதியியல் உளவறிதல் பிரிவு</p>	<p><b>Declaration of the Compliance Officer appointed under Section 14 (1) (a) of the Financial Transactions Reporting Act, No. 6 of 2006</b></p>	<p><i>for office use only</i></p>
<p>This form should be filled by the owner/Managing Director/Chief Executive Officer of the institution</p>		
<p><b>Type of declaration</b></p> <p>A <input type="checkbox"/> Initial Registration</p> <p>B <input type="checkbox"/> Alteration of existing information</p>	<p><b>Sector</b></p> <p>A <input type="checkbox"/> Real Estate                      D <input type="checkbox"/> Lawyer/Notary</p> <p>B <input type="checkbox"/> Gem and Jewellery              E <input type="checkbox"/> Accountant</p> <p>C <input type="checkbox"/> Casino                                  F <input type="checkbox"/> Trust/Company Service Provider</p>	
<p>We wish to inform you that Mr./Mrs./Miss/Dr. .... .....(name).....(Designation) has been appointed as the Compliance Officer of ..... (Reporting Institution) under Section 14 (1) (a) of the Financial Transactions Reporting Act, No. 6 of 2006, to ensure the institution's compliance with the Act.</p>		
<p><b>The details of the Compliance Officer are as follows:</b></p>		
<p>NIC/Passport Number: .....</p>		
<p>Official Address : .....</p>		
<p>Telephone number : Office ..... Mobile.....</p>		
<p>Email Address : ..... Fax .....</p>		
<p>Specimen Signature : .....</p>		
<p>Yours faithfully</p>		
<p>.....</p>		
<p>Signature of the owner/MD/CEO with Official Stamp</p>		<p>Date</p>
<p>Name of the owner/MD/CEO:Mr/Mrs/Ms/Dr .....</p>		
<p>NIC/Passport Number : .....</p>		
<p>Official Address : .....</p>		
<p>Telephone number : Office ..... Mobile .....</p>		
<p>Email Address : ..... Fax .....</p>		
<p>Copy to :..... (name of the compliance officer)</p>		

## **Annexure III**

### **Non-Exhaustive Money Laundering/ Terrorist Financing Suspicious Indicators (Red Flags) for Legal Professionals**

#### **Client and client behavior:**

1. Is overly secretive.
2. Is using an agent or an intermediary or avoids personal contact without a good reason.
3. Is reluctant to provide or refuses to provide information or documents usually required to enable the transaction's execution.
4. Holds or has previously held a senior public position or has professional or family ties to such individuals.
5. Is known to have been the subject of investigation for an acquisitive crime (i.e., one where the offender derives material gain from the crime, such as theft or embezzlement).
6. Is known to have ties to criminals.
7. Shows unusual interest and asks repeated questions on the procedures for applying ordinary standards.
8. Is constantly at a significant distance from the transaction without a legitimate or economic reason.
9. Hires a lawyer who does not have experience in providing the particular services needed.
10. Suggests paying substantially higher than usual fees without a legitimate reason.
11. Frequently changes his lawyers, or the client has multiple legal advisors without logical reason.
12. Requests services previously refused by another professional.
13. Executes transactions that are unusual with regards to the type of operation and the transaction's typical size, frequency or execution.
14. Executes transactions that do not correspond to his normal business activities and shows that he does not have a suitable knowledge of the nature, object or the purpose of the professional performance requested.
15. Requests the creation of complicated ownership structures or structures with involvement of multiple countries when there is no legitimate or economic reason.
16. Does not have documentation to support historical company activities.
17. Exhibits inconsistencies and unexplained last-minute changes to instructions.
18. Has no sensible commercial/financial/tax reason for the transactions or increased complexity that unnecessarily results in higher taxes or fees.
19. Abandons transactions with total disregard for fee level or potential losses.
20. Provides a power of attorney for the administration or disposal of assets under unusual circumstances without logical reason.
21. Requests to settle a litigation too easily or quickly with little or no involvement of the lawyer.
22. Requests for payments to third parties without substantiating reason or corresponding transaction.
23. Is native to, or resident in, or is incorporated in a high-risk country.
24. Is connected to the opponent without an apparent business reason.

25. Is tied to the opponent in a way that generates doubts as to the real nature of the transaction.
26. Attempts to disguise his real ownership of the business.
27. Is not directing the transaction. Rather, the person directing the operation is not one of the formal parties to the transaction.
28. Does not appear to be a suitable representative for the transaction.
29. Provides funds using unusual payment arrangements.
30. Withdraws funds from a source located in a high-risk country.
31. Does not provide a logical explanation to a significant increase in capital for his recently incorporated company.
32. Owns businesses that have unusually high capital in comparison with similar businesses.
33. Derives funds from a security transferred with an excessively high or low price attached.
34. Generates business income from large financial transactions that cannot be justified by the corporate purpose.

Source: ACAMS

The American Bar Association Provides a very good treatment of Red Flags in Chapter IV of "A Lawyer's Guide to Detecting and Preventing Money Laundering", which is available at this address:

<https://www.anti-moneylaundering.org/Document/Default.aspx?DocumentUid=3DBCE981-598E-45E6-8723-CC89C89E8086>



## Annexure IV- Matrix for Client Risk Profiling

Matrix for Client Risk Profiling					
Index	Score 1 - Low Risk	Score 2 - Medium Risk	Score 3 - High Risk		
	Criteria	Category	Allocation of score	Given mark	Possible highest mark
1	Country of Residence/ Incorporation	Sri Lanka	1		3
		Iran	3		
		North Korea	3		
		Countries with strategic AML/CFT deficiencies	3		
		Countries with high crime rates/terrorist problems	3		
		Other Countries			
2	Nature of the client	Legal Person	2		3
		Company with nominee shareholders	3		
		Company with a complex organizational structure	2		
		Individual	1		
		Trusts or other vehicles of holding personal assets	2		
		NGO/NPO	3		
3	Nature of Business/occupation of the client	Salaried resident individuals of government sector and well-established private sector entities such as banks, blue chip companies.	1		2
		Self-employed in SME sector	1		
		Client is or involve in businesses such as; - businesses vulnerable to ML/TF money changers, night clubs, casinos, supply of fire arms and ammunitions etc..) - cash intensive businesses - businesses where activities and nature are ambiguous	3		
		Other businesses, individuals where apparent	1		

		issue related with ML/TF cannot be identified			
		Unemployed personnel or personnel with unexpressed earnings	2		
4	Beneficial Owners	Easy to identify	1		3
		Difficult to identify	3		
5	Is the client/beneficial owner/related party a PEP?	Yes	3		3
		No	1		
6	Delivery Mode	Face to face	1		3
		Non-face-to face	3		
		Cross Border	3		
7	Transaction Mode	Cash	3		3
		Bank Transfer	1		
		Cheque/bank draft	1		
		Card Payment	2		
		Through money transfer service providers	2		
		Through Hawala/Hundial or other illegal methods	3		
8	Nature of the transaction process	Involve complicated financial transactions (e.g. payment schemes)	3		3
		Involve payments to/from third parties	3		
		Involve high risk real estate transactions	3		
		Transaction process is simple and transparent (e.g. one bank-to-bank transfer)	1		
9	Country of origin of funds/destination country	Country with a strategic AML/CFT deficiencies or reputed for criminal/terrorist activities	3		3
		Other countries	1		
10	Client or related party appear in the sanctions list?	Yes	3		3
		No	1		
11	Source of income	Can be identified easily	1		3
		Cannot be easily identified	3		
12	General information about the client (through google search, generally available information,	Positive	1		3
		Moderately adverse/not known	2		
		Negative	3		

	previous criminal records etc.)				
13	Client Behavior	Genuine	1		3
		Evasive	3		
		Secretive	3		
14	Overall satisfaction of the client's identity and profile with regard ML/TF	Well-satisfied	1		3
		Moderately satisfied	2		
		Not-satisfied (suspicious)	3		
<b>Total Score</b>				<b>(a)</b>	<b>(b)</b>
<b>Risk Rating</b>				<i>(a) as a percentage of (b)</i>	
The ultimate risk exposure will be determined by the Risk Rate above, segmented as per the chart below.					
<b>Risk Rating</b>		<b>Correspondent Risk Level</b>			
Below 65		Low Risk			
65 and above		High Risk			

**Annexure V**

**Schedule V**

**CONFIDENTIAL**

Province :

District :

<b>SUSPICIOUS TRANSACTION REPORT</b>		
<p>a. This report is made pursuant to the requirement to report suspicious transactions under the Financial Transaction Reporting Act, No. 6 of 2006</p> <p>b. Under Section 12 of the Act, no civil, criminal or disciplinary proceedings shall be brought against a person who makes such report in good faith</p>		
<b>PART A - DETAILS OF REPORT</b>		
1	Date of Sending Report	
2	Is this replacement to an earlier report?	Yes <input type="checkbox"/> No <input type="checkbox"/>
<b>PART B - INFORMATION ON SUSPICION</b>		
3	Name in Full (if organization, provide registered business/organization name)	
4	Residential/ Registered Address	
5	NIC No. / Passport No./ Business Registration No.	
6	Gender	Male <input type="checkbox"/> Female <input type="checkbox"/>
7	Country of Residence and Nationality (if an individual)	
8	Business/ Employment Type	
9	Occupation (where appropriate, principal activity of the person conducting the transaction)	
10	Name of Employer (where applicable)	
11	Contact Details	
<b>PART C - DESCRIPTION OF SUSPICION</b>		

12	Details of Transaction / Activity	
13	Ground / Reasons for Suspicion	
<b>PART D - DETAILS OF REPORTING PERSON</b>		
14	Date of Reporting	
15	Signature	
16	Name of Reporting Person/Agency	
17	NIC Number	
18	Designation / Occupation	
19	Address	
20	Contact Details	