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

මූල්‍ය බුද්ධි ඒකකය
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-02/2020

Ref: 037/08/001/0027/018

June 10, 2020

To: Chief Executive Officer/ General Manager/ Proprietor

Dear Sir/Madam,

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

The above mentioned 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,

E H Mohotty
Director/ Financial Intelligence

Cc: Compliance Officers

☎ 011-2477125
011-2477509
011-2477692
011-2477708
flu@cbsl.lk
dflu@cbsl.lk
www.flusrilanka.gov.lk

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

PART I
Introduction

1. These Guidelines are issued pursuant to Section 15 (1) (j) of the Financial Transactions Reporting Act, No. 6 of 2006 (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.

2. These Guidelines are provided as an aid to interpret the CDD Rules and shall act as a guidance for the following categories of designated non-finance businesses as defined under the Section 33 of the FTRA (hereinafter referred to as "Service Provider(s)").

    i. 'Accountants who provide accountancy services when such Accountants as part of their professional services, prepare for or carry out transactions for their clients in relation to any of the following 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.'[1]

[1] As defined in Subsection (j) of Designated Non-Finance Business in Section 33 of the FTRA.

ii. 'Trusts or Company Service Providers (TCSPs) not otherwise covered by this definition, which as a business provides one or more of the following services to third parties:[2]

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;
e) Acting as or arranging for another person to act as, a nominee shareholder for another person.

Activities mentioned in 2(i) and 2(ii) above are hereinafter referred to as "Captured Activities".

3. These Guidelines are issued for the purpose of assisting the Service Providers in identifying, assessing and managing Money Laundering (ML) and Terrorist Financing (TF) risks, when carrying out Captured Activities.

4. These Guidelines are not intended to be exhaustive and can be considered only as indicative guidance when developing policies, procedures and controls to achieve compliance with FTRA and other rules and regulations issued thereunder. Nothing in these Guidelines are to be considered as legal advice from the Financial Intelligence Unit.

5. For the purpose of these Guidelines, unless the context otherwise requires:

- **AML/CFT** means Anti-Money Laundering and/or the Countering the Financing of Terrorism as recommended by the Financial Action Task Force (FATF);

[2] As defined in Subsection (k) of Designated Non-Finance Business in Section 33 of the FTRA.

- **Beneficial Owner** means a natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a person or a legal arrangement.
- **CDD** means Customer Due Diligence;
- **Client** means "Customer" as defined in Section 33 of the FTRA;
- **FATF** means the Financial Action Task force**,** the intergovernmental body that sets international standards that aim to prevent Money Laundering and Financing of Terrorism and the harm these cause to the society.
- **FIU** means the Financial Intelligence Unit of the Central Bank of Sri Lanka which is designated under the Financial Transactions Reporting Act, No. 6 of 2006, and charged with the implementation and administration of the provisions of the FTRA;
- **ML** means the offence of money laundering, as defined in and punishable under Section 3 of the Prevention of Money Laundering Act, No. 5 of 2006;
- **TF** means the offence of terrorist financing, in terms of Section 3 of the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005;
- **ML/TF** means Money Laundering/Terrorist Financing;
- **NGOs/NPOs** means Non-Governmental Organizations / Not-for-Profit Organizations;
- **PEP** means Politically Exposed Person, an individual who is 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.

Vulnerabilities of Accounting Services

6. Some of the services provided by the accountants are more susceptible to money laundering and terrorist financing risks. Therefore, they can be exploited by potential

money launderers and terrorist financiers. Accountants are used as gatekeepers in utilizing their expertise to conceal the proceeds of crime. Some such services include:

a) Buying or selling of property – criminals may use property transfers to serve either as a cover for transfers of illegal funds or as a final investment of illicit proceeds, while the transaction may be wholly or part of the laundering process.

b) Performing financial transactions – criminals or would be offenders may use accountants to carry out or facilitate various financial operations on their behalf (e.g. cash deposits or withdrawals on accounts, retail foreign exchange operations, issuing and cashing cheques, purchase and sale of stock, sending and receiving international funds transfers, etc.).

c) Gaining introductions to financial institutions- criminals may use accountants as introducers or intermediaries. This can occur both ways as criminals may use financial institutions to gain introductions to accountants as well.

d) Company and Trust formation – criminals may attempt to confuse or disguise the links between the proceeds of a crime and the perpetrator through the formation of corporate vehicles or other complex legal arrangements.

7. The professional knowledge, skills and abilities of Accountants are vulnerable to be misused by criminals when conducting ML/TF activities. If, Service Providers are involved knowingly or unknowingly in the case of their clients engaged in ML/TF activities they will have to suffer various disadvantages including loss of reputation and possible legal actions.
8. Criminals or would be offenders may abuse the services provided by accountants to attribute a sense of legitimacy to falsified accounts in order to conceal the source of funds. For example, accountants may review and sign off such accounts for businesses engaged in criminality, thereby facilitating the laundering of the proceeds. Insolvency practice, which may be conducted by certain accountancy professionals also pose a risk of criminals concealing the audit trail of money laundered through a company and transferring the proceeds of crimes.

Vulnerabilities of Trusts or Company Service Providers

9. Trusts or Company Service Providers (TCSPs) provide services relating to the formation and management of companies and trusts which are considered as vulnerable for ML/TF activities.

10. Criminals and would be offenders often use companies, trusts and other similar legal arrangements to hide the origin and ownership of the criminally earned assets/finance terrorist activities.
11. Further, money launderers and terrorist financiers form shell companies which do not have independent operations, significant assets, ongoing business activities, or employees to conceal beneficial ownership, conduct transactions, or bring about a perception of legitimacy.
12. Criminals and would be offenders use address of TCSPs instead of using their physical location which allow them to keep anonymity and distance from the transactions and activities they are undertaking. Further it adds perception of legitimacy to their activities.
13. Criminals and would be offenders obtain the services of TCSPs for the management positions of the companies or trusts in order to provide greater respectability and legitimacy to the company or trust and its activities, to launder money and to finance terrorist activities.
14. Criminals and would be offenders use TCSPs as nominee shareholders or nominee directors or trustees of the companies or trusts or other legal arrangements to obscure their ownership of assets. This may provide a false impression of legitimacy for the activities undertaken by the company or legal arrangement enabling the criminals to use their companies or other legal arrangements for laundering money, financing of terrorism or other crimes without being detected.

Part II

Risk-Based Approach

15. Every Service Provider is required under the CDD Rules to identify and assess their exposure to ML/TF risk and develop suitable policies, procedures and controls to effectively manage and mitigate such risk. It is also expected to monitor the ongoing effectiveness of those policies, procedures and controls. The Risk Based Approach enables the service providers to allocate more resources to areas where the risks are higher.
16. Each Service Provider is expected to use their own judgment, knowledge and expertise to develop an appropriate risk-based approach for their particular organizational structure and business activities based on the nature and size of the

Service Provider. Risk assessment is the key starting point of the risk based approach and it is required to commensurate with the nature, size and complexity of the business. Some of the factors that can be considered when developing a risk-based approach are as follows.

- Risks related to the size, geographical location and organizational complexity of the Service Provider.
- Risks related to the specific services offered by the Service Provider
- Risk related to the specific types of the clients
- Risk related to the delivery channels

These factors can be considered either independent of one another or in combination in order to determine ML/TF risk. For example, a Service Provider that incorporates one or more Captured Activities as formation of companies, managing clients' money, having clients with complex beneficial ownership structures or known political exposure or in high risk and other monitored jurisdictions[3] and/or functioning in a high risk business sector could be more vulnerable to ML/TF than a firm that is exposed to only one of these risk categories.

17. 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;
    D. Monitor and improve the effective operations of the Risk-Based controls.

(A) Identify the ML/TF Risk

18. As the first step of the Risk-Based Approach, the Service Provider should identify their direct and indirect ML/TF risk factors associated with clients, geographical locations, services and delivery channels.
19. When identifying the risks associated with above mentioned aspects, the Service Provider should consider and document the risk related to:

[3] 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).

- Clients including their beneficial owners
    - Business or professional activities of clients/ beneficial owners.
    - Reputation of clients/ beneficial owners.
    - Nature and the behavior of clients/ beneficial owners.
- Geographical locations
    - The geographical origin and location of the client/beneficial owner.
    - Places of business of the customer/beneficial owner.
    - The geographical locations where the customer/beneficial owner have relevant personal links.
- Services
    - Types of services offered by the Service Providers.
    - Complexity of transaction.
    - Value or size of the transaction.
- Delivery channels
    - The extent to which the business relationship is conducted on non-face to face basis.
    - Any introducers or intermediaries used in the transaction process and nature of their relationship.

20. Examples for ML/TF risks associated with the Captured Activities and sample checklist for ML/TF risk identification and assessment is given respectively in **Annexure I and II** as a guidance. Service Provider is encouraged to develop a checklist of their own based on their own ML/TF risk identification and assessment, and to this end the **Annexure II** would provide some guidance.

(B) Assess the ML/TF Risks

21. The ML/TF Risk Assessment is required to be carried out once the Service Provider's ML/TF risk factors are identified.

    The ML/TF Risk Assessment is an analysis of potential threats and vulnerabilities of ML/TF to which the Service Provider is exposed. The complexity of the ML/TF Risk Assessment depends on, among the other factors, the nature, size and ML/TF risks faced by the Service Provider.

22. ML/TF Risk Assessment is carried out irrespective of any existing Policies, procedures and controls on customer identification, record keeping and reporting requirements.

(C) Design and Implement Controls to Manage and Mitigate the ML/TF Risks

23. Risk mitigation is about implementing controls to address risk drivers or the sources of the risk (i.e. threats, vulnerabilities) in a timely manner, which is tolerable to the Service Provider. Controls should be in the form of written policies and procedures.
24. The Service Provider is required to ensure the continuation of the AML/CFT Compliance Policy, procedures and controls without any disruptions due to changes in management, employees or the structure of the business.

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

25. The effective management of ML/TF risk is a continuous and dynamic process. The Service Provider should 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, caused by changes in the scale or nature of operations, new types of services, new customer types, etc.
26. The checklist developed for the purpose of assessing the risk of the Service Provider can be maintained as an ongoing tool to duly update the new and emerging risks as and when necessary.

Part III

Compliance

Compliance Officer

27. Every Service Provider is required to appoint a Compliance Officer, who works at the senior management level, to ensure compliance of the Service Provider with the provisions of the FTRA and other Rules and Regulations issued thereunder. The Compliance Officer is responsible for the establishment and maintenance of the procedures and systems to comply with the AML/CFT requirements. The Compliance Officer requires the authority and the resources necessary to discharge his or her responsibilities effectively. The Compliance Officer requires to monitor

AML/CFT measures of the Service Provider in order to ensure that they are effectively implemented and up to date.

28. According to the management structure of the Service Provider, the Compliance Officer should be in a position to have direct access to higher management or the Board of Directors. Therefore, the Compliance Officer position should be of the senior management level.
29. The Service Provider has a duty to declare the initial appointment of the Compliance Officer and any subsequent change as well, to the Director of the FIU through the 'Compliance Officer Declaration Form' (**Annexure III**), via email to fiudnfbp@cbsl.lk followed with the hard copy by post to the address: Director, Financial Intelligence Unit, Central Bank of Sri Lanka, No. 30, Janadhipathi Mawatha, Colombo 01.
30. The appointment should be formally made and responsibility should be incorporated to the Compliance Officer's Job Description.

Part IV

AML/CFT Compliance Policy, Procedures and Controls

31. Each Service Provider is required to establish a written AML/CFT Compliance Policy according to the ML/TF Risk assessment. The AML/CFT Compliance Policy is expected to be fully and effectively implemented by the Service Provider using procedures and controls that are communicated timely, understood and followed by the staff of the Service Provider.
32. The extent and the level of detail of each Service Provider's AML/CFT Compliance Policy, procedures and controls would depend on the specific circumstances of the Service Provider, as well as the results of the risk assessment.
33. The Service Provider 's AML/CFT Compliance Policy, procedures and controls are required to be approved by the senior management or senior partners. The AML/CFT Compliance Policy, procedures and controls are required to include, at a minimum;
    - client identification and verification,
    - conducting other aspects of CDD (including identifying and verifying beneficial owners and/or any person acting on behalf of the client),
    - record keeping,

- submission of mandatory reports to the FIU,
- ensuring independent audits on the conduct of Service Provider's AML/CFT compliance measures,
- screening clients against the UNSCR designated lists on Terrorism, Terrorism Financing and Proliferation of Weapons of Mass Destruction,
- screening employees before hiring and employee training on ML/TF.

34. Senior partners/senior management are required to understand statutory duties related to AML/CFT compliance vested upon the board of directors, the staff and the entity itself. Senior partners/senior management 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 entity.
35. The AML/CFT Compliance Policy, procedures and controls described are required to be reviewed and updated as an ongoing process to ensure that they commensurate with evolving and emerging risks.
36. When the Service Provider maintains any local or overseas branches/offices/subsidiaries, it is required to establish a 'Group AML/CFT Compliance Policy' to ensure that all branches /offices/subsidiaries implement the same AML/CFT measures, consistent with local laws and regulations.
37. If the overseas laws and/or regulations applicable for an overseas branch/office/subsidiary contradict or otherwise limit the application of Sri Lankan laws and/or rules, the Service Provider is required to act as specified in the CDD Rules.

PART V

Customer Due Diligence

Identification and Verification of Client, Beneficial Owners and Persons Acting on behalf of a Client

38. Service Providers, when carrying out the Captured Activities, are required to conduct CDD on their clients including occasional and one-off clients as specified in the CDD Rules.
39. The Service Provider is required to determine whether the client is acting on behalf of a third party, where the client is an agent of the third party who is the beneficial owner of the client and/or who is providing the funds for the transaction.

Accordingly, the Service Provider is required to conduct CDD on the beneficial owners also in relation to a Captured Activity.

40. The Service Provider is required to obtain minimum information on the identity of the client, beneficial owner and the person acting on behalf of the client as specified in the CDD Rules and verify such identity through independent, reliable source document.
41. Service Providers are required to conduct CDD before or at the time of starting a business relationship with a client. Generally, business relationship with a client begins after initial inquiries have been made by the prospective client but before any work is commenced.
42. The Service Provider is required to obtain information on the identity of any third party and their relationship with the client or ultimate beneficial owner for CDD purposes. The Service Provider shall also obtain documentary evidence to the effect that the respective third party has authorization to act on behalf of the client.
43. If a client does not submit satisfactory evidence of his/her identity to the Service Provider as required by the FTRA and the CDD Rules, the Service Provider is not in a position to proceed any further with the transaction unless directed to do so by the FIU, and shall report the attempted transaction to the FIU as a suspicious transaction. Further, if the client is reluctant to divulge CDD information, then also the Service Provider is required to submit an STR to the FIU.
44. If the Service Provider reasonably believes conducting of CDD measures would tip off the customer, the Service Provider may proceed with the transaction without conducting the CDD measures. However, the Service Provider is required to file an STR immediately.
45. Based on unique factors and attributes that are inherent to each business relationship, characteristics of the client, nature of the captured activity and the transactions to be conducted and potential exposures to ML/TF risks, the Service Provider has to determine whether Enhanced CDD is to be conducted.
46. Clients, beneficial owners and persons acting on behalf of clients that are identified as high risk are required to be subject to Enhanced CDD measures. Accordingly, at the situations where a client/beneficial owner/ third party acting on behalf of the client is identified as of high risk with respect to ML/TF, the Service Provider should apply Enhanced CDD measures as specified in the CDD Rules.

47. Moreover, Service Providers are required to conduct ongoing CDD on existing clients by regularly reviewing information and analyzing any new transactions.

Client Risk Profiling

48. After conducting CDD, Service Provider is required to profile and categorize all clients/beneficial owners/third parties acting on behalf according to their correspondent level of ML/TF risk.
49. Where the Service Provider's dealings with a client is limited to a single transaction (one-off transaction), it is not considered to be an ongoing business relationship. However, the Service Provider is required to complete a risk assessment of such client. If the Service Provider suspects that the transaction is related to an offence, then such transactions have to be reported to the FIU as an STR. Please refer Part VI for further information.

Enhanced CDD Measures

50. There are clients/ types of transactions / services which may pose higher ML/TF risk to Service Providers. In such a situation, the Service Provider is required to take additional CDD measures.

    Examples for instances where Enhanced CDD measures are required to be conducted for a client/beneficial owner/third party;

    a) Who has links with countries which do not or which insufficiently comply with the recommendations of the FATF {for High Risk and Non-Cooperative Jurisdictions please refer the FATF website (http://fatf-gafi.org),Web site of Asia Pacific Group on Money Laundering (http://apgml.org), FIU website (http://fiusrilanka.gov.lk)};
    b) Linked 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) Linked with any country that has been identified by a reputable organization as having high levels of public corruption;
    d) Who conducts a complex or unusual transaction, (whether completed or not), unusual patterns of transactions for the client profile, transactions that match patterns associated with unlawful activity, and transactions which have no apparent lawful purpose;

e) Who is domestic or foreign PEP including their family members and close associates.

Further, Enhanced CDD measures are also required to be conducted in the following instances;

a) Any client or transaction that the Service Provider has identified as posing a higher risk to the Service Provider, when it conducts the Client Risk Profiling;
b) Transactions where the natural person is not physically present in conducting the Captured Activity;
c) Transactions conducted with NGOs/NPOs.

Compliance with United Nations Security Council Resolutions

51. The Service Provider is required to cross-check whether any client/beneficial owner/third party acts upon the client appears on any designated list issued in compliance with the United Nations Act, No. 45 of 1968, with respect to following regulations issued on targeted financial sanctions related to terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing.
    a) **The United Nations Regulations No. 01 of 2012 :** issued by the Minister of Foreign Affairs promulgating the United Nations Security Council Resolution 1373 (2001) designating individuals and entities related to terrorism and terrorist financing in national level.
    b) **The United Nations Regulations No. 02 of 2012:** issued by the Minister of Foreign Affairs promulgating the United Nations Security Council Resolution 1267(1999) and the modifications and strengthening of the Resolution's sanctions regime by subsequent resolutions, and any other subsequent resolution on Taliban (Islamic Emirate of Afghanistan), Islamic State of Iraq and Levant (ISIL, also known as Da'esh) and Al-Qaida, imposing upon member States of the United Nations a series of obligations to apply sanction measures to any natural or legal person, group or entity associated with Taliban, ISIL (Da'esh) or Al-Qaida.
    c) **United Nations (Sanctions in relation to Democratic People's Republic of Korea) Regulations of 2017:** issued by the Minister of

Foreign Affairs promulgating the United Nations Security Council Resolution 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016) and successive Resolutions imposing certain measures on DPRK.

d) **United Nations (Sanctions in relation to Iran) Regulations No. 1 of 2018:** issued by the Minister of Foreign Affairs giving effect to the United Nations Security Council Resolutions 1737 (2006) and 2231 (2015) and any subsequent resolutions related to Iran and all resolutions that repeal, replace or amend earlier resolutions related to Iran.

52. The designated lists issued by the Ministry of Defense of Sri Lanka under the above regulations can be referred via http://fiusrilanka.gov.lk/unscr.html.

53. The Service Provider is 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.

54. The contact details of Competent Authority is as follows,
    Office of the Competent Authority,
    Ministry of Defence
    No.15/5, Baladaksha Mawatha
    Colombo, Sri Lanka.
    Tel. +94 112320585
    Fax +94 112390288
    email: camod@defence.lk

PART VI
Reporting

Duty of Submitting Suspicious Transactions Reports

55. In making the decision to submit an STR, the Service Provider may take into account, the client profile and any information of the client's business/employment activities. The list of red flag indicators as mentioned in **Annexure IV** will provide some additional guidance as to what constitute a suspicious activity. Industry-specific indicators would also help the Service Provider to better identify

suspicious transactions whether completed or attempted. Some examples of ML using Service Providers are given in **Annexure V.**

56. Each Service Provider is required to pay attention to attempted suspicious transactions. If a client attempts to conduct a transaction, but for whatever reason that transaction is not completed, and if the Service Provider determines that the attempted transaction is suspicious, the Service Provider is required to report it to the FIU.
57. The Service Provider is required to submit STRs using the format as prescribed in Suspicious Transactions (Format) Regulations of 2017, Gazette (Extraordinary) No: 2015/56 dated April 21, 2017 (**Schedule V-Annexure VI**).
58. The Compliance Officer is required to maintain a register of STRs including dates, serial numbers, name of the employee who reported STR, etc.

PART VII

Record Keeping

59. The Service Provider is required to take appropriate steps to put in place and maintain a system for record keeping as stipulated in the FTRA, which allows data to be retrieved immediately whenever required, or when requested by the FIU. Records maintained should carry CDD information, copies of identification documents, transaction records, correspondence relating to transactions and any other report furnished to the FIU.

PART VIII

Other AML/CFT Requirements

60. Service Providers is required to have a screening policy when hiring employees to ensure high standards and to ensure that the employees are not involved in any ML/TF activity.
61. Service Providers are required to provide training on AML/CFT compliance to senior partners/senior management, employees, agents or any other individuals authorized to act on behalf of the Service Provider.
62. Such training is required to raise awareness of the AML/CFT Compliance Policy on the entity, internal procedures and controls for preventing ML/TF. Training programs are required to provide a clear understanding of the related individual's

responsibilities so that they can foster a sub culture where all the employees of the Service Provider work towards adopting and implementing AML/CFT measures.

63. Service Provider is required to ensure that policies, procedures and controls are in accordance with the prevailing AML/CFT laws of the country.
64. Service Providers is required to be aware that an auditor has an obligation under the FTRA to submit an STR if the auditor suspects any transaction or series of transactions is related with ML/TF, during the course of performing the audit.

PART IX

Penalties for Non-Compliance

65. Failure to comply with the FTRA and any rules or regulations issued thereunder shall lead to penalties. In addition, there may be other actions including regulatory and disciplinary measures moved against the Service Provider via the respective Professional Bodies.

Issued on June 10, 2020

Annexure I

Examples for ML/TF risks associated with the Captured Activities

	Captured Activity	**Examples for such Activities**	**Examples for ML/TF Risks associated with such Activities**
1	Buying and selling of real estate	Involving or arranging buying and selling of immovable properties on behalf of the client.	Criminals may use Accountants as front persons to purchase properties on behalf of them exploiting Accountants' reputation.
2	Managing of client money, securities or other assets	Making direct payments on behalf of a client, directly from bank accounts of the client.	As the holding of funds are transferred to the service provider, it adds an appearance of legitimacy and may conceal the source of funds.
3	Management of bank, savings or securities accounts	Making investments in securities using funds of the client's account.	
4	Organization of contributions for the creation, operation or management of companies		
5	Creation, operation or management of legal persons or arrangements and the buying and selling of business entities	Registering a company with the company's office on behalf of a client.	- The actual ownership of the company may be concealed/obscured - Complex legal structures are used
		Forming an incorporated society on behalf of a client	- The implied purpose of a charitable trust seems to be broad with no clearly targeted groups.

Annexure II

An Example of a Checklist for Service Provider's ML and TF Risk Assessments

The following checklist is intended to provide an example of how to assess risk for your customers, products, services, delivery channels and geographic locations. This is only a starting point and the service provider 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.

Sample Institutional ML/TF Risk Assessment for Accountants and Trusts or Company Service Providers					
Name of the Institution		XXX			
S/N	**Risk Factor**	**Institutional Risk**	**Risk Indicator**		**Risk Mitigating Measure**
			High	**Low**	
1) Assessing Nature, size and complexity of the Institution					
1.1	Size of the business	Eg. Large/Small (considering the organizational structure, number of employees, availability of branches, number of clients, etc.)			
1.2	Ownership structure	Eg. Individual ownership (local, foreign, dual citizens)/ Ownership under another entity (local, foreign) or (sole proprietorship, partnership, company)			
1.3	Complexity of the service provider	Eg. Sole Proprietor with a simple structure/ Partnership with a simple structure/ Pvt Ltd Company/ Public Ltd Company/ company with branches in foreign countries.			

1.4	Nature of the services provided and activities recognised as being associated with ML/TF vulnerability	Eg. Services which are involved in sectors identified as highly vulnerable to ML/TF or highly cash intensive businesses (Real Estate businesses, casino, gem and jewelery dealers, auto mobile industry).			
2) Client Risk					
2.1	Ownership structure	Eg. Individual ownership (local, foreign, dual citizens)/ Ownership under another entity (local, foreign) or (sole proprietorship, partnership, company)			
2.2	Clients in high-risk occupations	Eg. Clients who are engaged in businesses or occupations that are highly vulnerable to ML/TF (Casinos, Real Estate Businesses, Accountants, Lawyers)			
2.3	Clients residing outside Sri Lanka	Eg. Foreign clients / Local clients			
2.4	Clients reside in high-risk jurisdiction	Eg. Clients from Iran/ Pakistan or any Other Jurisdictions Monitored by the FATF			
2.5	Politically Exposed Persons (PEPs)	Eg. Client who is a Politician/ Senior government officer/ Head of a State or a Government, etc.			
2.6	Clients are located in a known high crime rate area	Eg. Clients from Mexico which is well-known for Drug trafficking			
2.7	Client's physical location	Eg. Well known clients/ Well established business persons/ Clients not known to the service provider/ Clients using their company secretary's address as the business address			
2.8	Clients have a criminal records or links to organized crime	Eg. Known criminals			

3) Services risk					
3.1	Services support physical cash deposits and/or withdrawals	Eg. Accepting money from the client			
3.2	Services that facilitates international fund transfers	Eg. Fund transfers from foreigners			
3.3	Services support payments to /from third parties or non-clients	Eg. Allows non-face-to-face transactions/ Refund on advances are paid to a party other than the client or to a different account which the funds were initially generated.			
3.4	Services support transactions that can be conducted remotely or without interaction with the service provider	Eg. Maintain client's bank accounts			
3.5	Provide services linked with establishing, operating or managing of a shell company, company in nominal ownership.	Eg. Engages in creation, operation or management of legal persons or arrangements.			
3.6	Conducts transactions without clear commercial rationale	Eg. Continuously transfer funds to dormant account			
4) Delivery Channels/Business Relationships Risk					
4.1	Method of delivery remove or minimise face-to-face contact with the client	Eg. Transaction through internet/ wire transfers			
4.2	Third party can be used as delivery channel	Eg. Use of agents/ Service providers/ Lawyers/ Accountants			
4.3	Delivery channels involving cross-border payments	Eg. Wire transfers, Online transactions			

4.4	Delivery channels involving cash payments	Eg. Using cash for service charges			
5) Geographical Risk					
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 Securities Council Resolution (UNSCR)	Eg. Countries which are monitored jurisdictions like Ghana, Botswana, etc./ High risk jurisdictions-Iran and North Korea			
5.2	Dealings with countries where illegal activities are taken place.	Eg. countries with 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	Eg. Somalia, South Sudan, Syria (Source: Corruption Perceptions Index 2018)			
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	Eg. Syria, Afghanistan, Iraq			
5.5	Any country identified as a financial secrecy haven or jurisdiction	Eg. Switzerland, USA, Cayman Islands (Source: The Financial Secrecy Index 2018)			
5.6	Branches and subsidiaries of the service provider are located in other countries	Eg. Country which has weak or ineffective AML/CFT measures/ High-Risk Jurisdiction/ Countries that have a high degree of organised crime or drug related crime or high degree of people trafficking or smuggling/ Countries having strict AML/CFT laws and regulations			

Notes to the Risk Assessment

S/N	Risk Factor	Description on the Risk Factor
1) Assessing Nature, size and complexity of the Institution		
1.1	Size of the business	Larger the business, possibility of occurring suspicious activities and transactions during the course of business is higher.
		Large organisations may have difficulty in monitoring the implementation of AML/CFT measures to meet AML/CFT requirements.
1.2	Ownership structure	The ML/TF risk is higher when the ownership is under foreign/dual citizens or another entity compared to local/ individual ownership.
1.3	Complexity of the services	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	Nature of the services provided and activities recognised as being associated with ML/TF vulnerability	Services or activities which have been identified as high or medium level vulnerable to ML/TF during the National Risk Assessment or high cash intensive businesses.
2) Client Risk		
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, jewellers, high-value goods dealers, real estate agents, travel agents, import/export companies, remitters and money service businesses)
2.3	Clients residing outside Sri Lanka	Clients who are foreigners or Sri Lankan expatriates residing in other countries.
2.4	Clients reside in high-risk jurisdiction	Client reside in a high-risk jurisdiction pose a higher level of ML/TF vulnerability to the service provider.
2.5	Politically Exposed Persons (PEPs)	Due to their position and influence, PEPs are in positions that potentially can be abused for the purpose of committing ML offences and related predicate offences, including corruption and bribery, as well as conducting activity related to 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 service provider.
2.7	Client's physical location	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 in high ML/TF vulnerability to the service provider.
2.8	Clients with criminal records or links to organized crime	When the clients have prior criminal records or links to organised crimes. The ML/TF vulnerability posed by such customers become high.
3) Services risk		
3.1	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 a large amounts it will compound the ML/TF risk.
3.2	Services that facilitates international fund transfers	If the services facilitate inward or outward remittances, such remittances which are received or paid avoided the stipulated mechanisms (IIA, OIA).
3.3	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.
3.4	Services support transactions that can be conducted remotely or without interaction with the service provider	Less face-to-face interaction with a customer 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 service provider and client.
3.9	Provide services linked with establishing, operating or managing of a shell company, company in nominal ownership.	Shell companies (also called phantom firms or anonymous companies) are entities that are used to disguise the identity of their true owner) who ultimately control or profit from the company.
3.10	Conducts transactions without clear commercial rationale	Criminals do transactions without any specific reason to hide criminally earned money. This will create a high ML/TF vulnerability.
4) Delivery Channels/Business Relationships Risk		
4.1	Method of delivery remove or minimise face-to-face contact with the customer	Non- face-to-face interaction with a customer increases vulnerability to ML/TF activities.

4.2	Third party can be used as 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 involving cross-border payments	Cross border payments, foreign remittances, and transfers from foreign currency accounts involve high ML/TF risk.
4.4	Delivery channels involving 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.
5) Geographical Risk		
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 Securities Council Resolution (UNSCR)	Some countries have been identified by the Financial Action Task Force (FATF) as non-cooperative in the fight against money laundering or terrorist financing aa well as United Nations impose sanctions against some countries. Clients from such countries poses high ML/TF risk to the service provider.
5.2	Dealings with countries where illegal activities are taken place.	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. Non-profit organisations 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 occurs when there is a refusal to share financial information of a person/entity with legitimate authorities - for example, tax authorities and police authorities. Hence, when dealing with customers from such countries the barriers on obtaining their financial information shall be assessed in terms of high or low ML/TF risk.
5.6	Branches and subsidiaries of the Institution are located in other countries	When the service provider's branches or agents are located in other jurisdictions the ML/TF risk may be high or low depending on the factors such as AML/CFT deficiencies, measures and laws prevailing in those countries.

Annexure III- Compliance Officer Declaration Form

Financial Intelligence Unit මූල්‍ය බුද්ධි ඒකකය நிதியியல் உளவறிதல் பிரிவு	**Declaration of the Compliance Officer appointed under Section 14 (1) (a) of the Financial Transactions Reporting Act, No. 6 of 2006**	*for office use only*

This form should be filled by the owner/Managing Director/Chief Executive Officer of the institution

Type of declaration

A ☐ Initial Registration

B ☐ Alteration of existing information

Sector

A ☐ Real Estate

B ☐ Gem and Jewellery

C ☐ Casino

D ☐ Lawyer/Notary

E ☐ Accountant

F ☐ Trust/Company Service Provider

We wish to inform you that Mr/Mrs /Miss ……(*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.

The details of the Compliance Officer are as follows:

NIC/Passport Number: ……..

Official Address : ……..

Telephone number : Office …….. Mobile……..

Email Address : …….. Fax ……..

Specimen Signature : ……

Yours faithfully

…….. ……

Signature of the owner/MD/CEO with Official Stamp Date

Name of the owner/MD/CEO : Mr/Mrs/Ms/Dr ……..

NIC/Passport Number : ……

Official Address : ……

Telephone number : Office …….. Mobile ……..

Email Address : …… Fax ….....

Copy to :…… (*name of the compliance officer*)

Annexure IV

Anti-Money Laundering/Countering Financing of Terrorism Suspicious Indicators (Red Flags) for Accountants

Client and client behavior:

i. Client executes transaction/transactions which is/are not consistent with his usual profile.
ii. Client makes a transaction/s inconsistent with his usual financial status/profile.
iii. Client has cheques inconsistent with his/her sales (i.e. unusual payments from unlikely sources).
iv. Client has a history of changing book-keepers or Accountants very frequently.
v. Client is a company that has no employees, which is unusual for the type of business.
vi. Client is a company that is paying unusual consultant fees to offshore companies.
vii. Client conducts large or frequent transactions using foreign currency without any economic rationale.
viii. Client is suspected to be using forged, fraudulent or false identity documents for due diligence and record keeping.
ix. Client maintains and submits incomplete account records to the Accountants in order to finalize the accounts.
x. Client is unusually concerned and/or makes inquiries about the AML/CFT requirements and internal compliance policies, procedures or controls.
xi. Client attempts to maintain a high degree of secrecy with respect to transactions, for example by requesting not to keep normal business records.
xii. Client avoids answering questions related to the source of funds.
xiii. Client is known to have a criminal/terrorism background.
xiv. Client appears to be related to a country or entity that is associated with ML/TF activities.
xv. Client is a resident in a geographical area which is considered as high risk for ML/TF.
xvi. Client is a company that has nominee shareholders shares in bearer form.
xvii. Client is a company that involves in a cash intensive business.
xviii. The corporate structure of the client(company) is unusual or complex as that of the other similar corporates in the same industry.
xix. The legal structure of the client (company) is frequently altered including name changes, transfers of ownership, and location of headquarters.
xx. The Accountant does not have a face-to-face introduction to the client.
xxi. Beneficial ownership of the client is unclear.

xxii. The client is a PEP or a close relative of such a person.

Product, Service or Delivery Method Risk:

i. The product involves private banking.
ii. Payments are received from unknown or unassociated third parties.
iii. New products, new delivery channels and new business practices are involved.

Country/Geographic Risk

i. Client is dealing with a country which is not having effective systems to counter ML/TF.
ii. Client is remitting funds to countries which have been recognized as having significant level of corruption, drug/human trafficking or terrorism.
iii. Client is receiving funds from a country which is known for financing terrorism.

Annexure V

Case Studies as Examples of ML & TF through Accountants

Case Study 01

The Police of Country Z has revealed that Mr. D, a human trafficker in Country Z has received a large amount of funds as frequent cash deposits in small amounts. These funds have been used to purchase real estate in Country Y. It has also been revealed that an Accountant has been used by Mr. D to open bank accounts and purchase real estate. Accountant also has offered investment advices to Mr. D.

Case Study 02

"Company M" which is an Accounting Firm has provided his service to "Client H" to purchase number of properties. "Client H" owns a car sale business However, he has links to a drug trafficking business as well.

Funds to purchase these properties were provided in cash and the amount of cash given has been huge despite the earnings from his legitimate business activities.

After the reveal of the connection "Client H" had with the drug trafficking business, "Company M" was convicted for not making a Suspicious Transactions Report to the FIU.

Case Study 03

Client A of "Accounting Firm KA" has made frequent requests to wire money to and from various bank accounts without giving any reasonable explanation for it. Client A has also requested the firm to make cash deposits in different financial institutions. The Compliance Officer of "Accounting Firm CA" has identified this client as suspicious and had reported to the FIU of this suspicious nature of transactions. Later it has been revealed that the Client A has links with a terrorist group and had assisted terrorism financing activities using the Accounting Firm.

Annexure VI

Schedule V

CONFIDENTIAL

Province :
District :

SUSPICIOUS TRANSACTION REPORT		
a. This report is made pursuant to the requirement to report suspicious transactions under the Financial Transaction Reporting Act, No. 6 of 2006 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		
PART A - DETAILS OF REPORT		
1	Date of Sending Report	
2	Is this replacement to an earlier report?	Yes ☐ No ☐
PART B - INFORMATION ON SUSPICION		
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 ☐ Female ☐
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	
PART C - DESCRIPTION OF SUSPICION		
12	Details of Transaction / Activity	

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