SRI LANKA RELATED SERVICES PRACTICE STATEMENT 4755

ENGAGEMENTS TO REPORT ON THE COMPLIANCE WITH ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM GUIDANCE ISSUED BY THE CENTRAL BANK OF SRI LANKA

(Effective for Engagements commencing on or after 27th November, 2019)

CONTENTS

	Paragraph
Overview	**1**
What is the purpose of this guidance?	1.1
Who is this guidance for?	1.2
Definitions	1.3
What is ML?	1.3.1
What is TF?	1.3.2
What is FIU?	1.3.3
Legal framework for AML/CFT in Sri Lanka	**2**
What is the AML/CFT legal and regulatory framework?	2.1
Acts	2.1.1
Regulations	2.1.2
Rules	2.1.3
What are the Guidelines relevant to AML/CFT measures	2.2
Interpretations	2.3
"Institutions"	2.3.1
"Accountants"	2.3.2
"TCSPs"	2.3.3
AML/CFT Compliance Obligations for members of CA Sri Lanka	**3**
What are the AML/CFT Compliance Obligations of Accountants and TCSPs?	3.1

SLRSPS

Appointing an AML/CFT Compliance Officer ……..…… 3.1.1

ML/TF Risk Assessment and Management …… 3.1.2

Formation of AML/CFT Policies, Procedures and Controls ……..… 3.1.3

Conducting CDD …… 3.1.4

Record Keeping and Retention Requirements …… 3.1.5

Reporting Requirements to the FIU ……...… 3.1.6

Compliance with United Nations Security Council Resolutions ...…..… 3.1.7

Other Internal Controls on AML/CFT …… 3.1.8

AML/CFT training for Employees …… 3.1.8.1

Screening of Employees at Hiring ……..… 3.1.8.2

Conducting of Independent Auditing …… 3.1.8.3

What are the AML/CFT Obligations of Senior Management in a Financial Institution? …… 3.2

What are the AML/CFT Obligations of Senior Management in a Designated Non-Finance Business? …… 3.3

What are the AML/CFT Obligations of the Auditors of an Institution? ….. 3.4

Annexure: Guidance Checklist for Agreed Upon Procedures

(Effective for Engagements commencing on or after 15th December, 2024)

LIST OF ABBREVIATIONS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
CA SRI LANKA	Institute of Chartered Accountants of Sri Lanka
CDD	Customer Due Diligence
CO	Compliance Officer
CSTFA	Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005, as amended
DNFBs	Designated Non-Finance Businesses
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FTRA	Financial Transactions Reporting Act, No. 6 of 2006
ML	Money Laundering
ML/TF	Money Laundering/Terrorist Financing
NGO	Non-Governmental Organization
NPO	Not-for-Profit Organization
PEP	Politically Exposed Persons
PMLA	Prevention of Money Laundering Act, No. 5 of 2006, as amended
RBA	Risk-Based Approach
TCSPs	Trusts and Company Service Providers
TF	Terrorist Financing

Introduction

The Institute of Chartered Accountants of Sri Lanka (CA Sri Lanka) is committed to the goal of developing a set of Sri Lanka Standards and other pronouncements which are generally accepted worldwide. CA Sri Lanka members act in the common interest of the public at large and the worldwide accountancy profession. This could result in their taking a position on a matter that is not in accordance with current practice in their country or firm or not in accordance with the position taken by those who put them forward for membership of the CA Sri Lanka.

The purpose of this Sri Lanka Related Services Practice Statement 4755 (SLRSPS 4755) is to establish Standards and provide guidance on Circular No 5 issued by the FIU of the Central Bank of Sri Lanka (CBSL), on requiring the external auditor to ensure compliance by the Financial Institution with the reporting requirements specified in Section 6, 7 ,8 and 22 of the FTRA. These Institutions are expected to ensure that their ML/TF risk management framework and practices are subject to external audit review. These Guidelines provide an aid for members of CA Sri Lanka to comply with AML/CFT legal obligations in Sri Lanka. This guidance refers to the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA) and Rules and Regulations issued thereunder for finance businesses and non-finance businesses.

The Institute of Chartered Accountants of Sri Lanka (CA Sri Lanka) agreed in discussions with the CBSL to develop a guidance to practitioners to comply with the above direction. CA Sri Lanka considered international practice and technical guidance in audit practices to formulate this practice statement.

CA Sri Lanka believes this practice statement will provide a useful guidance to practitioners. This guidance also illustrates the responsibilities of auditors and directors in fulfilling the requirements enunciated by the above direction issued by the CBSL. In addition, illustrations of an engagement letter, report and an annexure to the report on factual findings are provided to assist the practitioners in reporting

These Guidelines are not intended to be exhaustive and do not impose legally binding practices on members of CA Sri Lanka, and do not constitute legal advice from CA Sri Lanka. Nothing in these Guidelines should be interpreted as releasing members of CA Sri Lanka from any of their obligations under the Customer Due Diligence Rules for Designated Non-Finance Businesses or the FTRA.

1. OVERVIEW

- What is the purpose of this guidance?
- Who is the guidance for?
- Definitions

1.1 What is the purpose of this guidance?

This guidance has been prepared to assist members of CA Sri Lanka to ensure compliance with the relevant legislations on Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) in Sri Lanka.

1.1.1 The term ‘‘shall’ is used throughout to indicate a mandatory legal or regulatory requirement. Members may seek an alternative interpretation of the Sri Lankan AML/CFT regime, but they shall be able to **justify** their decision to their AML/CFT supervisory authority.

1.1.2 Where the law or regulations require no specific course of action, ‘‘should” is used to indicate good practice sufficient to satisfy statutory and regulatory requirements. Members should consider their own particular circumstances when determining whether any such ‘good practice’ suggestions are indeed appropriate to them.

Alternative practices can be used, but members shall be able to explain their reasons to their AML/CFT supervisory authority, including why they consider them compliant with laws and regulations.

1.2 Who is this guidance for?

The AML/CFT regime applies to “Institutions” which are defined in Section 33 of the FTRA. This guidance is addressed to members of CA Sri Lanka who are:

- Accountants and TCSPs as defined in Section 33 of the FTRA;
- Senior Managers who work in “Institutions”;
- Auditors of “Institutions”;

(Refer section 2.3.1 for interpretations)

1.3 Definitions

1.3.1 What is Money Laundering (ML)?

- The processing of the criminal proceeds to disguise their illegal origin (Source: *Financial Action Task Force*).
- ML is considered as an offence in Sri Lanka under Section 3 of the Prevention of Money Laundering Act, No. 5 of 2006, as amended (PMLA). If a person;
  - engages directly or indirectly in any transaction in relation to

any property which is derived or realized, directly or indirectly, from any unlawful activity or from the proceeds of any unlawful activity or;

- receives, possesses, conceals, disposes of, or brings in to Sri Lanka, transfers out of Sri Lanka, or invests in Sri Lanka, any property which is derived or realized, directly or indirectly from any unlawful activity or from the proceeds of any unlawful activity; it is considered as an offence of ML in Sri Lanka.

- Members of CA Sri Lanka need to be alert to the ML risks posed by;
  - Clients, countries or geographical areas, products, services, transactions or delivery channels;
  - Suppliers;
  - Employees; and
  - Their associates.
- Three stages of ML are as follows;

Placement

Placement is the initial stage of money laundering where the launderer introduces his illegal profits into the financial system. This might be done by;

- breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account,
- by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.

Layering

After the funds have entered the financial system, the second or layering stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channeled through;

- the purchase and sales of investment instruments,
- wiring through a series of accounts at various banks across the globe.

Integration

Having successfully processed the launderer's criminal profits through the first two phases the launderer then moves them to the third stage, Integration, in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into;

- real estate,
- luxury assets, and
- business ventures.

(Source: FATF)

1.3.2 What is Terrorist Financing (TF)?

- TF is financing of terrorist acts, and of terrorists and terrorist organizations (FATF). Funds used to support terrorism, terrorists and terrorist organizations may originate from legitimate sources, criminal activities or both.
- TF is an offence in Sri Lanka under Section 3 of the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005, as amended (CSTFA):

Financing of terrorists or terrorist organizations is an offence in Sri Lanka under Section 3 of the CSTFA.

1.3.3 What is Financial Intelligence Unit (FIU)?

- The FIU has been established in March 2006 under the provisions of the FTRA with the main objective of combating ML/TF and other related crimes in Sri Lanka in line with international recommendations and standards. It functions as an independent institution within the administrative structure of the Central Bank of Sri Lanka. FIU is mainly to receive or collect financial information from Institutions to analyse and disseminate with Law Enforcement Authorities in identifying, controlling and mitigating ML/TF risk of the country and to supervise institutional compliance with AML and CFT obligations.

2. LEGAL FRAMEWORK FOR AML/CFT IN SRI LANKA

2.1 What is the AML/CFT legal and regulatory framework?

The AML/CFT legal and regulatory framework of Sri Lanka consists of the following legislations;

2.1.1 Acts:

- **Financial Transactions Reporting Act, No. 6 of 2006**: FTRA provides for the collection of data relating to suspicious transactions to facilitate the prevention, detection, investigation and prosecution of the offences of ML and TF respectively; to require certain Institutions to undertake due diligence measures to combat money laundering and the financing of terrorism; to identify the authority which will be responsible for monitoring the activities of all Institutions to whom said Act applies; and to provide for matters connected therewith or incidental thereto.
- **Prevention of Money Laundering Act, No. 5 of 2006, as amended**: PMLA was enacted; to prohibit money laundering in Sri Lanka ; to provide the necessary measures to combat and prevent money laundering ; and to provide for matters connected therewith or incidental thereto.
- **Convention on the Suppression of Terrorist Financing Act, No 25 of 2005, as amended**: CSTFA was enacted to give effect to the convention on the suppression of terrorist financing; and to provide for matters connected therewith or incidental thereto.

2.1.2 Regulations:

- **Suspicious Transactions (Format) Regulations of 2017 (STR Format Regulation):** STR Format Regulation shall apply to every Institution within the meaning of Section 33 of the FTRA which prescribes the formats to report suspicious transactions to the FIU.

2.1.3 Rules:

- **Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016** – Extraordinary Gazette No. 1951/13, January 27 of 2016 (CDD Rules for FIs): CDD Rules for FIs shall apply to every Institution which engages in Finance Business to which the provisions of the FTRA apply. Every Financial Institution shall take the measures as specified in these rules for the purpose of identifying, assessing and managing ML and TF risks posed by its customers, by conducting ongoing CDD based on the "Risk-Based Approach (RBA)".

- **The Designated Non-Finance Business (Customer Due Diligence) Rules, No. 1 of 2018**. - Extraordinary Gazette No 2053/20, January 10 of 2018 (CDD Rules for DNFBPs): Every DNFBP shall take the measures as specified in these rules for the purpose of identifying, assessing and managing ML and TF risks posed by its customers, by conducting ongoing CDD based on the "RBA".

2.2 What are the Guidelines Relevant to AML/CFT Measures:

Further to above, following Guidelines have been issued by the FIU under the provisions of the FTRA;

- Guidelines on AML/CFT Compliance Obligations for Money or Value Transfer Service Providers, No. 01 of 2017
- Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism Compliance Obligations for Dealers in Real Estate and Precious Metals, Precious and Semi-Precious Stones, No 03 of 2018
- Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism Compliance Obligations for Casinos and Gambling Houses, No. 2 of 2018
- Guidelines for Financial Institutions on Identification of Beneficial Ownership, No. 04 of 2018
- Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 01 of 2018
- Guidelines for Financial Institutions on Suspicious Transactions Reporting, No. 6 of 2018
- Guidelines, No. 5 of 2018 on Implementing United Nations (Sanctions in relation to Democratic People's Republic of Korea) Regulations of 2017
- Guidelines, No. 7 of 2018 on Implementing United Nations (Sanctions in relation to Iran) Regulations, No. 1 of 2018
- Guidelines for Designated Non-Finance Businesses on Suspicious Transactions Reporting, No. 01 of 2019
- Guidelines for Designated Non-Finance Businesses on Identification of Beneficial Ownership, No. 02 of 2019
- Guidelines on Identification of Politically Exposed Persons, No. 03 of 2019

You may refer the FIU website via www.fiusrilanka.gov.lk to refer the above documents.

2.3 Interpretations

2.3.1 "Institutions"

As per Section 33 of the FTRA;

"Institution" means any person or body of persons engaged in or carrying out any finance business or designated non-finance business within the meaning of the Act. Accordingly, the finance businesses and designated non-finance businesses include the following;

Finance Business including

- Licensed Banks
- Licensed Finance Companies
- Insurance Companies
- Stock Brokering Firms
- Restricted Dealers (formerly Authorized Money Changers)
- Money or Value Transfer Service Providers

Designated Non-Finance Business including

- Casinos & Gambling Houses
- Real Estate Agents
- Dealers in Precious Metals & Stones
- Lawyers & Notaries, Other Independent Legal Professionals and **Accountants**
- Trusts and Company Service Providers (**TCSPs)**

2.3.2 "Accountants"

"Accountants", when they prepare for or carry out transactions for their clients in relation to any of the following activities: -

(i) buying and selling of real estate;

(ii) managing of client money, securities or other assets;

(iii) management of bank, savings or securities accounts;

(iv) organization of contributions for the creation, operation or management of companies; and

(v) creation, operation or management of legal person or arrangements and the buying and selling of business entities;

are interpreted as DNFBs under Section 33 of the FTRA and required to comply with the AML/CFT obligations under the FTRA.

2.3.3 Trusts and Company Service Providers (TCSPs)

"TCSPs", when they provide one or more of the following services to third parties: -

(i) formation or management of legal persons;

(ii) 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;

(iii) 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;

(iv) acting as or arranging for another person to act as, a trustee of an express trust

(v) acting as or arranging for another person to act as, a nominee shareholder for another person

are interpreted as DNFBs under Section 33 of the FTRA and are required to comply with the AML/CFT obligations under the FTRA.

3. AML/CFT COMPLIANCE OBLIGATIONS FOR MEMBERS OF CA SRI LANKA

- What are the AML/CFT compliance obligations of Accountants and TCSPs?
- What are the AML/CFT obligations of Senior Management in Financial Institutions?
- What are the AML/CFT obligations of Senior Management in Designated Non-Finance Businesses?
- What are the AML/CFT obligations of the Auditors of an Institution?

3.1 What are the AML/CFT Compliance Obligations of Accountants and TCSPs?

Accountants and TCSPs are required to comply with the below mentioned key legal requirements on AML/CFT, which are specified under the FTRA and CDD Rules for DNFBs.

3.1.1 Appointing an AML/CFT Compliance Officer (CO)

- Under Section 14 (1) (a) of the FTRA, Accountants and TCSPs are required to appoint a CO. The CDD Rules for DNFBs specifies that the CO must be a Senior Management level officer. The Accountants and TCSPs should ensure that there are sufficient resources to undertake the work associated with the

CO's role.

- For consistency and ongoing attention to the AML/CFT requirements, the CO may choose to delegate certain duties to other employees.

For example, the CO may delegate an employee in a branch to ensure that AML/CFT compliance policies, procedures and controls are properly implemented at that branch. However, where such a delegation is made, the CO remains responsible for the implementation of the AML/CFT compliance policies, procedures and controls.

3.1.2 ML/TF Risk Assessment and Management

- Accountants and TCSPs shall have appropriate policies, procedures and controls for assessing and managing ML/TF risks.
- As specified in CDD Rules for DNFBs, a RBA should be adopted by Accountants and TCSPs in implementing a ML/TF risk management function which focuses resources on the areas of greatest risk. It is the ultimate responsibility of Accountants and TCSPs to identify the ML/TF risks arising from the client base, products or services, countries or geographical locations and transactions or delivery channels and then develop risk-based policies, procedures and controls to mitigate the identified risks.
- The ML/TF risk assessment should be reviewed and updated periodically with new and changing risks considered as and when they are identified.

3.1.3 Formation of AML/CFT Policies, Procedures and Controls

- Section 14 (1) (b) of the FTRA and CDD Rules for DNFBs specifies that Accountants and TCSPs are required to formulate internal policies, procedures and controls on AML/CFT to manage and mitigate ML/TF risks that have been identified, subject to any written law in force for the time being on AML/CFT.
- AML/CFT policies, procedures and controls are required to be approved by its Senior Management or Board of Directors and, required to address areas including;
  - ML/TF Risk Assessment and Management
  - Developing and updating AML/CFT Compliance policies, procedures and controls

- Identification and verification of clients and Beneficial Owners and, conducting CDD measures including;
  - Legal persons and legal arrangements
  - Non-face-to-face clients
  - Non-For-Profit Organizations(NPOs) and Non-Governmental Organizations(NGOs)
  - Politically Exposed Persons (PEP)s
  - Clients from High Risk Countries
- Record keeping and retention requirements
- Compliance with United Nations Security Council Resolutions (UNSCR)
- Procedures for reporting STRs, CTRs & EFTs etc.
- Training of employees
- Other AML/CFT controls such as screening at hiring employees and conducting independent audit for AML/CFT measures of the Institutions

3.1.4 Conducting Customer Due Diligence (CDD)

- As per Section 2 (1) of the FTRA, Accountants and TCSPs shall not open, operate or maintain an account, where the holder of such account cannot be identified, including any anonymous account or any account identified by number only, or any account which to the knowledge of the Accountant or TCSP is being operated in a fictitious or false name.
- CDD Rules for DNFBs specifies that, Accountants and TCSPs shall –

  (a) identify the client and verify that client's identity using reliable, independent source documents, data or information;

  (b) verify whether any person purporting to act on behalf of the client is so authorized, and identify and verify the identity of such person;

  (c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source, to the satisfaction of the Accountant or TCSP;

(d) understand and, where relevant, obtain information on, the purpose and intended nature of the business relationship.

- Accountants and TCSPs are shall at the minimum obtain the following information from its clients for the purpose of conducting CDD;

  (a) the full name;

  (b) permanent residential or mailing address;

  (c) occupation, name of employer, business or principal activity;

  (d) official personal identification number or any other identification document that bears a photograph of the client or beneficial owner such as the National Identity Card, passport or driving license;

  (e) date of birth;

  (f) nationality;

  (g) source of funds;

  (h) purpose of transaction;

  (i) telephone numbers (residence, office or mobile).

- According to the Rule 17 of CDD Rules for DNFBs, in the case of a client that is a legal person or legal arrangement, Accountants and TCSPs shall understand the nature of the client's business, its ownership and control structure; and identify and verify its identity of the client through obtaining information specified in Rule 17 (b).
- Rule 6 (c) of the CDD Rules specifies to conduct risk profiling on its clients considering their ML/TF risk level.

- According to the Rule 16 of CDD Rules for DNFB, Every Accountant and TCSPs shall conduct the enhanced CDD measures, in addition to the measures specified in Rule 11, where the assessed ML/TF risk for a client has been rated as a "High Risk". Also, the CDD Rules specifies that Enhanced CDD must be performed to;

  - Clients conducting non-face-to-face transactions
  - Transactions with NGOs and NPOs
  - PEPs
  - Clients from High-Risk Countries

3.1.5 Record Keeping and Retention Requirements

- Under Section 4 of the FTRA, Accountants and TCSPs shall maintain
  - records of transactions and of correspondence relating to transactions and records of all reports furnished to FIU for a period of six years from the date of the transaction, correspondence or the furnishing of the report, as the case may be, and
  - records of identity obtained in terms of Section 2 for a period of six years from the date of closure of the account or cessation of the business relationship, as the case may be.

Unless Directions have been issued by the FIU that such records or correspondence should be retained for a longer period, in which case the records or correspondence should be retained for such longer period.

3.1.6 Reporting Requirements to the FIU

- Section 6 of the FTRA specifies that Accountants and TCSPs shall report to the FIU;
  a) any transaction of an amount in cash exceeding such sum as shall be prescribed by the Minister by Order published in the Gazette, or its equivalent in any foreign currency (unless the recipient and the sender is a bank licensed by the Central Bank), and
  b) any electronic funds transfer at the request of a client exceeding such sum as shall be prescribed by regulation.

- According to Section 7 of FTRA, there is a duty on Accountants and TCSPs to report suspicious transactions when they;
  a) have reasonable grounds to suspect that any transaction or attempted transaction may be related to the commission of any unlawful activity or any other criminal offence; or
  b) have information that it suspects may be relevant—
    (i) to an act preparatory to an offence under the provisions of the CSTFA;
    (ii) to an investigation or prosecution of a person or

persons for an act constituting an unlawful activity, or may otherwise be of assistance in the enforcement of the PMLA and the CSTFA,

- Accountants and TCSPs shall, as soon as practicable, after forming that suspicion or, receiving the information, but no later than two working days therefrom, report the transaction or attempted transaction or the information to FIU.

3.1.7 Compliance with United Nations Security Council Resolutions (UNSCR)

- The CDD Rules specifies that Accountants and TCSPs shall verify whether any client or beneficiary appears on any designated list issued in compliance with the United Nations Act, No. 45 of 1968, with respect to Targeted Financial Sanctions relating to terrorism and terrorist financing and proliferation of weapons of mass destruction and its financing.

3.1.8 Other AML/CFT Controls

3.1.8.1 Conducting of AML/CFT Training for Employees

- Accountants and TCSPs are required that all relevant officers, employees, agents to be made aware of the law relating to ML/TF and given regular training in how to recognize and deal with suspicious activities which may be related to ML/ TF.
- A formal training plan can help make sure that relevant employees receive the right training to enable them to comply with their AML/CFT obligations. Training should be tailored to suit the particular role of the individual.

3.1.8.2 Screening of Employees at Hiring

- Accountants and TCSPs are required to develop and implement comprehensive employee due diligence and screening procedures at the time of appointing or hiring employees on permanent basis or any other basis.

3.1.8.3 Conducting of Independent Auditing on AML/CFT measures

- Accountants and TCSPs are required to maintain an independent audit function to test its AML/CFT policies, procedures and controls maintained by them subject to any written laws.

3.2 What are the AML/CFT Obligations of Senior Management in a Financial Institution?

- Every Financial Institution shall appoint a Senior Management level officer as the CO, who shall be responsible for ensuring the Financial Institution's compliance with the requirements of the FTRA and Rules issued thereunder.
- Senior Management of Financial Institutions should demonstrate a firm understanding of all aspects of the Institution's business model and is responsible for developing the components of the ML/TF risk management framework.
- Senior Management of Financial Institutions is also responsible for;
  - implementing the corporate vision, strategy and business model approved by the Board of Directors.
  - ensuring that the Institution has all the resources necessary to effectively manage ML/TF risks.
  - ensuring that effective communication and reporting arrangements are in place to support good ML/TF risk management practices.

    This includes ensuring that all staff members are aware of the requirements of the ML/TF risk management framework and their specific roles and responsibilities.
  - ensuring that internal reporting mechanisms, including reports to be sent to the Board of Directors, are developed to provide accurate and timely information relevant to the effective management of ML/TF risks.
  - Ensuring the effective functioning of the corporate governance framework on a day-to day basis for AML/CFT.
- Senior Management is required to develop policies, procedures and controls to effectively manage the ML/TF risks that arise from its operations. AML/CFT policies and procedures developed by Senior Management should be approved by the Board of Directors.
- When the assessed ML/TF risk of any client is "High" during the ML/TF Risk Profiling on its clients, Senior Management is required to grant the approval to commence or continue the business relationship, as a method of conducting Enhanced CDD measures for high risk clients/transactions.
- Senior Management needs to ensure the approved AML/CFT policies, procedures and controls are periodically reviewed or updated.

3.3 What are the AML/CFT Obligations of Senior Management in a Designated Non-Finance Business?

- Every non-finance business when appointing a CO, shall appoint a Senior Management level officer who shall be responsible for ensuring the business's compliance with the requirements of the FTRA and Rules issued thereunder.
- CDD Rules for DNFBs requires that the approval of the Senior Management should be obtained in following circumstances,
  - "Formulate internal policies, approved by its **Senior Management or Board of Directors**, subject to any written law in force for the time being on AML and CFT".
  - After conducting CDD, the ML/TF risk of the client needs to be assessed through a ML/TF Risk Profiling. When the assessed ML/TF risk for a client has been rated as "High-Risk", every non-finance business shall obtain approval from the **Senior Management**, if any, before establishing or in the case of an existing client for continuing such business relationship with the client (this provision applies to High-Risk clients).

In addition to above, the Senior Management is responsible to oversee the continuous implementation of the key AML/CFT legal obligations within the business and to ensure that relevant employees are made aware of all the AML/CFT policies, procedures and controls of the business.

3.4 What are the responsibilities of the Auditors of an Institution?

- According to the Section 22 of FTRA, where an auditor of an Institution has reasonable grounds to suspect that information that it has concerning any transaction or attempted transaction may, be –

  a) relevant to an investigation or prosecution of a person or persons for any unlawful activity;

  b) of assistance in the enforcement of the provisions of PMLA and the CSTFA;

  c) related to the commission of any offence constituting an unlawful act; or

  d) preparatory to the offence of the financing of terrorism,

the auditor of the Institution shall report the transaction or attempted transaction to the FIU.

Illustration of an engagement letter for agreed-upon procedures engagement to report on factual findings relating to the Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 01 of 2018

To the Board of Directors or other appropriate representatives of the client who engaged the auditor.

This letter is to confirm our understanding of the terms and objectives of our engagement and the nature and limitations of the services that we will provide. Our engagement will be conducted in accordance with the principles set out in Sri Lanka Standards on Related Service 4400 (SLSRS 4400) applicable to agreed-upon procedures engagements and we will indicate so in our report.

We have agreed to perform the procedures listed under the annexure 'A' and report to you the factual findings resulting from our work (Describe where relevant the timing and extent of the procedures to be performed in annexure 'A' including specific reference, where applicable, to the identity of documents and records to be reviewed, individuals to be contacted and parties from whom confirmations will be obtained.)

The procedures that we will perform are solely to assist you, to meet the compliance requirement under Circular No 5 issued by the FIU of the Central Bank of Sri Lanka (CBSL), to ensure compliance with the reporting requirements specified in Section 6, 7 ,8 and 22 of the FTRA. Our report is not to be used for any other purpose and is solely for your information.

The procedures that we will perform will not constitute an audit or a review made in accordance with Sri Lanka Auditing Standards and consequently, no assurance will be expressed.

We look forward to full cooperation with your staff and we trust that they will make available to us whatever records, documentation and other information requested in connection with our engagement.

Our fees, which will be billed as work progresses, are based on the time required by the individuals assigned to the engagement plus out-of-pocket expenses. Individual hourly rates vary according to the degree of responsibility involved and the experience and skill required.

(Additional terms and conditions may be added by the auditors)

Please sign and return the attached copy of this letter to indicate that it is in accordance with your understanding of the terms of the engagement including the specific procedures which we have agreed will be performed.

XYZ & CO.

Acknowledged on behalf of ABC Company PLC by

(signed)

Name and Title

Date

Annexure

Required Procedures
Inquire whether the Institution has a Code of Ethics developed and communicated amongst the employees.
Peruse evidence supporting the availability of Code of ethics and evidence of communication
Inquire the senior management person responsible in risk management for their roles and understanding of risk management.
Peruse the documentation relating to Senior Management's responsibility over risk management.
Inquire on the internal reporting requirements by Senior Management in relation to risk management.
Peruse evidence for periodic reporting by senior management over risks.
Inquire on the scope of the Risk Management function in relation to ML/TF risk management.
Obtain an understanding of the size and composition of the risk management division of the Institution.
Inquire on the availability of policies and procedures in relation to ML/TF risks and BOD approval of the same.
Obtain and scan the evidence of the above and communication of ML/TF policies and procedures to staff.
Inquire on the periodic review of ML/TF policies & procedures and also evidence supporting the same.
Inquire whether the ML/TF policies and procedures cover reporting lines for all persons and business units involved and peruse evidence supporting the same.
Inquire whether the ML/TF policies and procedures cover the limits in the context of ML/TF risk appetite and also reporting mechanism to report incidents and peruse evidence supporting the same.
Comment whether the internal audit function is an independent function with a direct reporting line to the Board and to the Audit Committee.
Inquire how the internal audit function periodically assesses the effectiveness of the institution’s ML/FT risk management framework and practices, paying specific attention to the institution’s adherence to established policies procedures and limits and applicable laws, regulations and guidelines.

Required Procedures
Obtain an understanding of the availability of a compliance officer and his experience and qualifications.
Inquire on the scope of work of the compliance function in relation to ML/TF risks.
Inquire on the MIS controls that mitigate ML/TF risks as well as provide data on the quantity and nature of the risks.
Inquire and observe how the MIS measures ML/TF risks, reports on adherence to policies and procedures designed to mitigate risks.
Peruse the reports generated from the system relating to ML/TF.
Inquire how frequently the reports relating to ML/TF are prepared and submitted to BOD.
Inquire on the training programmes relating to ML/TF conducted for staff and the extent of staff coverage achieved including for new staff
Inquire on the procedures followed by the Institution when assessing ML/TF Risk covering the following aspects as described in the guideline.
-Identification of vulnerabilities
-Identified risk factors for ML/TF
-Risk assessment
-Risk management and mitigation
Inquire upon and review the policies for enhanced CDD measures for higher risk of ML/TF customer transactions and report on evidence of such CDDs.
Inquire and review the policies for simplified CDD measures and report on evidence of such CDDs.
Inquire on the availability of the ML/TF risk management policies covering the requirements,
a) for reporting transactions in cash exceeding such sum prescribed by the Minister
b) for reporting suspicious transactions
c) For disclosing relevant details to the FIU of any person conducting suspicious transactions
Inquire on the employee due diligence and screening procedure carried out at recruitment.
Inquire about CDD over Foreign Branches and Subsidiaries as stipulated in the Act.

Required Procedures
Peruse documented policies covering group wide programmes for branches and subsidiaries for CDD on, - sharing information required for conducting CDD - providing information for implementing the suppression of money laundering and terrorist financing measures - Confidentiality and the use of information exchanged among branches and subsidiaries. - application of anti money laundering and terrorist financing measures in foreign branches
Inquire and peruse documented policies covering use of new technology in relation to new products and new delivery mechanisms
Peruse documented policies and procedures covering CDD procedures, for - not having numbered accounts - maintenance of accounts in order to be able to extract assets and liabilities of a customer - CDD measures on customers conducting transactions such as currency exchanging business for transactions involving amounts exceeding Rs. 200,000, occasional transactions involving Rs. 200,000 or its equivalent in foreign currency. - identifying and initial risk profiling of customers obtain minimal details such as purpose of the account and sources of earning etc. and conduct enhanced CDD measures for high risk customers. - taking reasonable measures to understand the ownership and control structure of the customer - obtaining information to identify beneficial owner if there is any - cases where delayed verification is allowed - taking actions where the financial institution is unable to conduct CDD measures - monitoring of business relationships with a customer - reporting of transactions inconsistent with the rules - periodical review of adequacy of customer information - conducting CDD measures on existing customers - CDD measures to follow for occasional, one off, walk-in and third party customers - CDD measures to follow for legal persons and legal arrangements - CDD measures to follow for Non-Government and Not-for-Profit organizations or charities - CDD measures to follow for beneficiaries of insurance policies - conducting enhanced CDD measures on customers and financial institutions from high risk countries - CDD measures to follow for politically exposed persons - CDD measures to follow for financial institutions which relies on a third party
Inquire, peruse and comment on documented policies and procedures covering correspondent banking as stipulated in the Act.

Required Procedures
Inquire on policies and procedures and Peruse documented policies and procedures covering cross border wire transfers over Rs. 100,000/- or its equivalent in any foreign currency
Inquire regarding policies and procedures over record keeping as stipulated in the Act and Peruse documented policies and procedures covering the, - sufficiency of records to permit reconstruction of individual transactions - maintenance of up to date records - retention of records (up to 6 years) - immediate availability of transaction records to relevant domestic authorities - verification of prospective customers or beneficiaries ***Note to Practitioners:*** Add any other procedures that may be required due to the nature of systems of the specific institution, other regulatory requirements or any limitations in performing the above procedures..

Illustration of a report of factual findings in connection with Circular No 5 issued by the FIU of the Central Bank of Sri Lanka (CBSL), on requiring the external auditor to ensure compliance with the reporting requirements specified in Section 6, 7 ,8 and 22 of the FTRA.

REPORT OF FACTUAL FINDINGS

To (those who engaged the auditor)

We have performed the procedures agreed with you and enumerated in an annexure to this report, with respect to Circular No 5 issued by the FIU of the Central Bank of Sri Lanka (CBSL), on requiring the external auditor to ensure compliance with the reporting requirements specified in Section 6, 7 ,8 and 22 of the FTRA. Our engagement was undertaken in accordance with the principles set out in Sri Lanka Standards on Related Service 4400 (SLSRS 4400) applicable to agreed-upon procedures engagements. The procedures were performed solely to assist you to meet the compliance requirement of the guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions.

We report our findings below: (List the results of the procedures performed as described in the annexure)

Because the above procedures do not constitute an audit or review made in accordance with Sri Lanka Auditing Standards, we do not express any assurance on the compliance with the guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions.

Had we performed additional procedures or had we performed an audit or review of the financial statements in accordance with Sri Lanka Auditing Standards, other matters might have come to our attention that would have been reported to you.

Our report is solely for the purpose set forth in the first paragraph of this report and for your information and is not to be used for any other purpose or to be distributed to any other parties. This report relates only to the items specified above and does not extend to any financial statements of ABC Company PLC, taken as a whole.

AUDITOR

Date

Address

Annexure

(Effective for Engagements commencing on or after 15th December, 2024.)

Agreed upon procedures to be followed by the practicing auditor.

Guidance Checklist for Agreed Upon Procedures

Financial Transactions Reporting Act, No. 6 of 2006 (FTRA) and rules, regulations, guidelines, directives, and circulars issued thereunder predominantly provide Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) compliance regime with regard to managing the risk of Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF).

Financial Institutions (FIs) are required to implement a transaction monitoring mechanism in terms of Section 14 (b) of the FTRA. This legal requirement has been further elaborated by the Rule 37-39 of the Financial Institutions (Customer Due Diligence) Rule, No. 1 of 2016 (CDD Rules), as amended. Accordingly, transactions monitoring and reporting suspicious transactions are statutory obligations cast upon FIs through FTRA. Such transaction monitoring mechanisms may be implemented through automated systems or manual processes.

In line with Targeted Financial Sanctions (TFS), FIs are required to prohibit conducting transactions with persons and entities designated under any regulation made in terms of the United Nations Act, No. 45 of 1968, with respect to any designated list on TFS related to TF and PF. Hence, transaction monitoring mechanisms should have the capability of detecting such designated person or entity through its system parameters.

Further, in terms of the FTRA and CDD Rules, FIs need to establish an audit function to test its procedures and systems.

#	**Required Procedures**	**Reference / guidance**	**Findings**
1	Inquire whether the Institution has a Code of Ethics developed and communicated amongst the employees.		
2	Peruse evidence supporting the availability of Code of ethics and evidence of communication	It is also appropriate to examine the coverage, adequacy and implementation of the code.	
3	Inquire the senior management person responsible in risk management for their roles and understanding of risk management.	Rule 5 of the CDD Rules is applicable to Every FI and it should not be limited to senior management person. It is required to ensure that this includes ML/TF risk of FIs	

#	Required Procedures	Reference / guidance	Findings
		considering NRA, regional risks, emerging risks etc. Further, ML/TF risk should be integrated with enterprise-wide risk assessment, and it should be adequate and up to date.	
4	Peruse the documentation relating to Senior Management's responsibility over risk management.	It is required to ensure that this includes the ML/TF risk aspect. (Pls refer to 3 above)	
5	Inquire on the internal reporting requirements by Senior Management in relation to risk management.	CDD Rules 12 - 13 are applicable to this requirement and it is required to ensure that this includes the ML/TF risk aspect. (Pls refer to 3 above)	
6	**1.** Obtain a listing of reports that needs to be submitted to the regulators including suspicious transaction reports. **2.** Peruse evidence whether the transaction monitoring system has the capabilities to generate the information needed for the reports required by the regulator including suspicious transaction reports.	1. Suspicious Transaction Report (STR) is not a routine report. STRs should be reported to the FIU independently through the compliance officer who should be at the senior management level when a suspicion arises. (Please refer to section to 7 of the FTRA.) 2. Transaction Monitoring System should have sophisticated and adequate rules to generate alerts for unusual transactions or transaction patterns. There should be filtering and prioritization process. 3. FIs shall not disclose STR information to any other person in terms of Section 9 of the FTRA. Accordingly, auditors may check the STR generation process in order to ascertain the adequacy of the system generated reports.	
7	Inquire on the scope of the Risk Management function in relation to ML/TF risk management.	Please refer to Rules 4 - 11 of the CDD Rules. (Pls refer to 3 above)	

#	**Required Procedures**	**Reference / guidance**	**Findings**
8	Obtain an understanding of the size and composition of the risk management division of the Institution.	The FIU considers the adequacy of resources in the compliance and ML/TF risk management functions, as well as the eligibility level and responsibilities of the compliance officer and compliance team. The compliance officer should be at the senior management level.	
9	1. Obtain BOD approved AML/CFT policies and procedures relating to definition of suspicious transactions, red flags, and reporting requirements. 2. Compare the definition of suspicious transactions, red flags, and reporting requirements provided by the management with the regulations and guidance issued by FIU.	Please refer to Rules 14 - 17 of the CDD Rules.	
10	Obtain and scan the evidence of the above and communication of ML/TF policies and procedures to staff.	Please refer to Rules 14 - 17 of the CDD Rules and special focus should be on ML/TF risk assessment.	
11	1. Obtain a listing of configuration settings included in the transaction monitoring systems and compare them with the AML/CFT policies. 2. Obtain the policy covering the continuous monitoring of compliance with the same during the reporting period on a sample basis.	Please refer to Rules 14 - 17 of the CDD Rules and special focus should be on ML/TF risk assessment	
12	1. Obtain listing of customer transaction processing systems used and compare the list with the information systems that have been linked to the transaction monitoring systems. 2. Inquire from the management how they ensure transaction data is complete, accurate, and timely and peruse evidence whether the procedures have been implemented on a sample basis.	Please refer to Section 5 of the FTRA and Rules 36 - 40 the CDD Rules.	

#	**Required Procedures**	**Reference / guidance**	**Findings**
13	Obtain a listing of red flag criteria defined in the transaction monitoring systems and compare the list with the AML/CFT policies and regulatory requirements.	Please refer to Guidelines for Financial Institutions on Suspicious Transactions Reporting, No. 06 of 2018 issued by the FIU.	
14	Comment whether the internal audit function is an independent function with a direct reporting line to the Board and to the Audit Committee.	Please refer to Rules 17 - 18 of the CDD Rules. As per the said CDD Rules, audit function should be independent.	
15	Inquire how the internal audit function periodically assesses the effectiveness of the institution's ML/FT risk management framework and practices, paying specific attention to the institution's adherence to established policies procedures and limits and applicable laws, regulations and guidelines.	Please refer to Rules 17 - 18 of the CDD Rules. As per the said CDD Rules, audit function should be independent.	
16	1. Obtain the organizational structure of the Division responsible for TMS and STR reporting process. 2. Inquire whether the human and other resources allocated are adequate to carry out the assigned responsibilities.	Please refer to Section 14 of the FTRA and Rule 17 of the CDD Rules. As per the above requirements, the compliance officer should be at the senior management level.	
17	Inquire on the scope of work of the compliance function in relation to ML/TF risks.	Please refer to Section 14 of the FTRA and Rule17 of the CDD Rules.	
18	Inquire on the MIS controls that mitigate ML/TF risks as well as provide data on the quantity and nature of the risks.	Please refer to Rules 11 - 17 of the CDD Rules.	
19	Inquire and observe how the MIS measures ML/TF risks, reports on adherence to policies and procedures designed to mitigate risks.	Please refer to Rules 11 - 17 of the CDD Rules.	
20	Peruse the reports generated from the system relating to: • Alerts Generation - review the alert generation procedure and process adopted by the institution in treating such alerts. - review the effectiveness of the alert generating process	Please refer to Section 5 of the FTRA and Rules 36 - 40 the CDD Rules. The alert closure procedure should also be examined.	

#	**Required Procedures**	**Reference / guidance**	**Findings**
	conducting series of test cases using a sample of historical data to verify whether the system generates alerts for known suspicious transactions. - Test the system's ability to detect transactions based on identified samples that should raise suspicion according to the established criteria and parameters. • Alerts Escalation - review the alerts escalation procedure in treating such alerts.		
21	Inquire how frequently the reports relating to ML/TF are prepared and submitted to BOD.	Please refer to Rules 12-13 of the CDD Rules. FIs should understand and apply AML/CFT obligations and mitigating measures including internal controls and procedures and audit requirements to ensure compliance with AML/CFT requirements.	
22	Inquire on the training programmes relating to ML/TF conducted for staff including: • the extent of staff coverage achieved for existing and new staff. assess the procedures in place to ensure whether employees understand how to use the system effectively and report.	Please refer to Section 14 of the FTRA and Rule 17 of the CDD Rules. Further, FIs should implement AML/CFT programmes, including internal policies, procedures and controls for employee screening during the hiring process.	
23	Inquire on the procedures followed by the Institution when assessing ML/TF Risk covering the following aspects as described in the guideline. – Identification of vulnerabilities – Identified risk factors for ML/TF – Risk assessment – Risk management and mitigation – Scenario testing – based on experience and knowledge of ML/TF typologies. Test the	1. Please refer to Rules 4-10, 36-40 of the CDD Rules. 2. The FIU has issued the Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 01 of 2018 for ML/TF risk assessment purpose. 3. These procedures are more relevant to the scope and detail procedures of transaction monitoring.	

#	Required Procedures	Reference / guidance	Findings
	system's ability to detect these scenarios and generate alerts. – Threshold testing – evaluate the effectiveness of transaction value and frequency thresholds. – Back-testing and benchmarking – analyze historical cases where ML/TF activities were identified and assess whether the transaction monitoring system would have captured these cases. This can be done using past incidents and benchmarks. – False positive rate analysis – examine the rate of false positive (legitimate transactions incorrectly identified as suspicious) and comment. – Documentation and reporting – Ensure that the reports prepared by the bank clearly indicate any deficiencies or areas where the system needs improvements. – Feedback loop – inquire if the bank has established a feedback loop with the bank's compliance team to discuss the results of testing, also to collaborate on improving the system based on identified weaknesses.	Institution's ML/TF risk assessment is more broader concept than transaction monitoring.	
24	Inquire upon and review the policies for enhanced CDD measures for higher risk of ML/TF customer transactions and report on evidence of such CDDs.	Please refer to Rules 27 (2), 45, 51-54, 57-58, and 59 of the CDD Rules.	
25	Inquire and review the policies for simplified CDD measures and report on evidence of such CDDs.	. FIs need to conduct minimum CDD as per Rule 27 of CDD Rules.	
26	Inquire on the availability of the ML/TF risk management policies covering the requirements,	Please refer to Rules 14 -15 of the CDD Rules.	
	a) for reporting transactions in cash exceeding such sum prescribed by the Minister	Please refer to Section 6 of the FTRA and Order and Regulation issued under Section 6 of the FTRA. This should include both cash transactions and electronic fund transfers.	

#	**Required Procedures**	**Reference / guidance**	**Findings**
	b) for reporting suspicious transactions	Pls refer to Section 7 of the FTRA, and Guidelines for Financial Institutions on Suspicious Transactions Reporting, No. 06 of 2018. As per the Section 9 of the FTRA, FIs shall not disclose STR information to any other person.	
	c) For disclosing relevant details to the FIU of any person conducting suspicious transactions	Please refer to Sections 7 - 10 of the FTRA.	
27	Inquire on the employee due diligence and screening procedure carried out at recruitment.	Please refer to Section 14 of the FTRA and Rule 17 of the CDD Rules.	
28	Inquire about CDD over Foreign Branches and Subsidiaries as stipulated in the Act.	Please refer to Rules 19 - 21 of the CDD Rules.	
29	Peruse documented policies covering group wide programmes for branches and subsidiaries for CDD on, - sharing information required for conducting CDD - providing information for implementing the suppression of money laundering and terrorist financing measures - confidentiality and the use of information exchanged among branches and subsidiaries. - application of anti money laundering and terrorist financing measures in foreign branches	Please refer to Rules 19 - 21 of the CDD Rules. Further, it is required to monitor the procedures relating to agents, if applicable.	
30	Inquire and peruse documented policies covering use of new technology in relation to new products and new delivery mechanisms	Please refer to Rules 22 and 23 of the CDD Rules.	
31	Peruse documented policies and procedures covering CDD procedures, for – not having numbered accounts	Please refer to Section 2-3 of the FTRA , Rules 26-27,47, 51-54,57-58,59-63 of the CDD Rules.	

#	Required Procedures	Reference / guidance	Findings
	– maintenance of accounts in order to be able to extract assets and liabilities of a customer – CDD measures on customers conducting transactions such as currency exchanging business for transactions involving amounts exceeding Rs. 200,000, occasional transactions involving Rs. 200,000 or its equivalent in foreign currency – identifying and initial risk profiling of customers obtain minimal details such as purpose of the account and sources of earning etc. and conduct enhanced CDD measures for high risk customers. – taking reasonable measures to understand the ownership and control structure of the customer – obtaining information to identify beneficial owner if there is any cases where delayed verification is allowed – taking actions where the financial institution is unable to conduct CDD measures – monitoring of business relationships with a customer – reporting of transactions inconsistent with the rules – periodical review of adequacy of customer information – conducting CDD measures on existing customers – CDD measures to follow for occasional, one off, walk-in and third party customers – CDD measures to follow for legal persons and legal arrangements – CDD measures to follow for Non-Government and Not-for-Profit organizations or charities – CDD measures to follow for beneficiaries of insurance policies – conducting enhanced CDD measures on customers and		

#	**Required Procedures**	**Reference / guidance**	**Findings**
	financial institutions from high risk countries – CDD measures to follow for politically exposed persons - CDD measures to follow for financial institutions which relies on a third party		
32	Inquire, peruse and comment on documented policies and procedures covering correspondent banking as stipulated in the Act.	Please refer to Rules 64 - 67 of the CDD Rules.	
33	Inquire on policies and procedures and Peruse documented policies and procedures covering cross border wire transfers over Rs. 100,000/- or its equivalent in any foreign currency	Please refer to Rules 68 - 83 of the CDD Rules.	
34	- Inquire regarding policies and procedures over record keeping as stipulated in the Act and Peruse documented policies and procedures covering the, - sufficiency of records to permit reconstruction of individual transactions - maintenance of up to date records retention of records (up to 6 years) - immediate availability of transaction records to relevant domestic authorities - verification of prospective customers or beneficiaries - process to customize the requirements to the specific risk profile and the regulatory environment.	Please refer to Section 4 of the FTRA and Rules 89 - 94 of the CDD Rules.	