AML & CFT Guidelines

For

Professionals with Certificates of Practice from ICAI, ICSI and ICMAI

Table of Contents

Acronyms

Term	Definition
AML	Anti-Money Laundering
CFT	Countering the Financing of Terrorism
CDD	Customer Due Diligence
CPF	Combating Proliferation Financing
CKYCR	Central Know Your Customer Registry
CRS	Common Reporting Standards
DNFBP	Designated Non-Financial Business and Profession
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU-IND	Financial Intelligence Unit – India
KYC	Know Your Customer
ML/TF/PF	Money Laundering, Terrorism Financing and Proliferation Financing
NRA	National Risk Assessment
OVD	Officially Valid Document
PEPs	Politically Exposed Persons
PMLA	Prevention of Money Laundering Act 2002
PMLR	Prevention of Money-laundering (Maintenance of Records) Rules 2005
RBA	Risk-Based Approach
RE	Reporting Entities
STR	Suspicious Transaction Reporting
SRB	Statutory Body – ICAI, ICSI, ICMAI
UAPA	Unlawful Activities (Prevention) Act, 1967
UNSC	United Nations Security Council

Introduction

1. Background

1.1 The present document shall be referred to as the AML & CFT Guidelines (hereinafter called "The Guidelines") in respect of financial transactions carried out by relevant persons, such as, individuals who obtained certificate of practice under section 6 of the Chartered Accountants Act, 1949, under section 6 of the Company Secretaries Act, 1980 and under section 6 of the Cost and Works Accountants Act, 1959, as notified by the Central Government, vide notification F.No. P-12011/12/2022-ES Cell-DOR, dated May 03, 2023 (hereinafter referred to as ***'the notification'***). For the purpose of the present guidelines, money laundering has the same meaning as in Section 3 of Prevention of Money-Laundering Act, 2002 ('PMLA').

1.2 PMLA lays down record-keeping and reporting obligations for financial institutions and persons carrying on designated business or profession, with the latter defined in sub-clause (vi) of clause (sa) of sub-section (1) of section 2, which states that 'person carrying on designated business or profession', includes persons carrying on such other activities as the Central Government may, by notification, so designate from time-to-time. In exercise of said powers, the Central Government, vide notification F.No. P-12011/12/2022-ES Cell-DOR dated May 03, 2023, notified certain financial transactions carried out by relevant persons, such as, individuals who obtained certificate of practice under section 6 of the Chartered Accountants Act, 1949, under section 6 of the Company Secretaries Act, 1980 and under section 6 of the Cost and Works Accountants Act, 1959,.

1.3 The present document aims to provide a summary of legal provisions of anti-money laundering, counter-terrorism financing and proliferation financing legislations in India, viz. the Prevention of Money Laundering Act, 2002 (hereinafter referred to as the "PMLA"), the Unlawful Activities (Prevention) Act, 1967 (hereinafter referred to as the "UAPA"), the Weapons of Mass Destruction and Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (hereinafter referred to as the "WMDA") and rules/notifications thereunder and to lay down steps that a relevant person carrying out certain financial transactions, on behalf of their clients, as notified vide Central Government notification F.No. P-12011/12/2022-ES Cell-DOR dated May 03, 2023 **(*hereinafter referred to as 'Relevant Persons')***, shall implement to prevent, detect and report money laundering, terrorist financing or proliferation financing activities.

1.4 Relevant Persons

The Central Government vide notification F.No. P-12011/12/2022-ES Cell-DOR dated May 03, 2023, has notified the financial transactions carried out by a relevant person on behalf of his client, in the course of his or her profession, in relation to the activities listed below, as an activity for the purposes of sub-clause (vi) of clause (sa) of sub-section (1) of section 2 of the Prevention of Money-laundering Act, 2002 (15 of 2003),

(i) buying and selling of any immovable property;
(ii) managing of client money, securities or other assets;
(iii) management of bank, savings or securities accounts;
(iv) organisation of contributions for the creation, operation or management of companies;
(v) creation, operation or management of companies, limited liability partnerships or trusts, and buying and selling of business entities,

Explanation 1:-For the purposes of this notification 'relevant person' includes –

(i) An individual who obtained a certificate of practice under section 6 of the Chartered Accountants Act, 1949 (38 of 1949) and practicing individually or through a firm, in whatever manner it has been constituted;
(ii) An individual who obtained a certificate of practice under section 6 of the Company Secretaries Act, 1980 (56 of 1980) and practicing individually or through a firm, in whatever manner it has been constituted;
(iii) An individual who has obtained a certificate of practice under section 6 of the Cost and Works Accountants Act, 1959 (23 of 1959) and practicing individually or through a firm, in whatever manner it has been constituted.

Explanation 2:- For the purposes of this notification 'firm' shall have the same meaning assigned to it in sub-clause (i) of clause (23) of section 2 of the Income-tax Act, 1961 (43 of 1961).

2. Scope

The guidelines apply to financial transactions carried out by relevant persons as notified vide '***the notification'***.

3. Effective Date

These guidelines shall take effect immediately i.e. from June 19, 2023.

4. General Obligations of Relevant Persons.

4.1. Reporting of Reportable Transactions

The mechanism for reporting of reportable transactions in respect of money laundering, terrorist financing and proliferation financing has been designed to facilitate filing of reports by the respective relevant persons carrying out financial transactions, as defined vide '***the notification',*** through the respective Statutory Bodies (viz. ICAI, ICSI, and ICMAI) hereinafter referred to as **SRBs**.

4.2. Policies and Procedures to Combat Money Laundering, Counter Terrorist Financing and Combat Proliferation Financing: (AML/CFT/CPF Program)

Rule 7(3) of the PMLR casts an obligation on every reporting entity to evolve an internal mechanism to detect transactions as specified under Rule 3(1) and furnishing information about such transactions to FIU-IND.

In order to discharge said obligation, every relevant person carrying out financial transactions as notified under '***the notification'*** must have a robust AML/CFT/CPF policy in place, which shall include the following points.

4.3. Internal policies, procedures, and controls to be implemented by relevant persons

4.3.1 To comply with the obligations of relevant persons as specified under PMLA, PMLR, every relevant person/firm shall establish appropriate policies and procedures for the prevention of ML, TF, and PF, and ensure their effectiveness and compliance with all relevant legal and regulatory requirements. The reporting entities shall:

4.3.2 Adopt policies (board-approved in case of firms) including procedures for dealing with ML, TF and PF risks, reflecting the current statutory and regulatory requirements and guidance/guidelines issued by competent authorities and SRBs.

4.3.3 Periodically review the policies and procedures on the prevention of ML, TF, and PF to ensure their alignment with extant statutory provisions, rules and guidelines and guidance issued by competent authorities and SRBs.

4.3.4 Adopt client acceptance and KYC policies and undertake Client Due Diligence (CDD) measures in respect of the financial transactions notified vide '***the notification'***;

4.4. Registration of Reporting Entities, Appointment of Designated Director and Principal Officer

4.4.1 Registration of Reporting Entities – The SRBs shall identify members holding certificate of practice, who are undertaking activities notified vide ***'the notification'***. Consequent to identification of such members, the SRBs shall obtain information (name, designation and contact details such as mobile number and email) related to principal officers and/or designated directors from them, as applicable in accordance with clause 4.4.2 hereunder. The list of principal officers and/or designated directors shall be maintained by the SRBs and shall be communicated to FIU-INDIA periodically and in the event of changes.

4.4.2 Appointment of Designated Director and Principal Officer - In case where the relevant persons as defined under '***the notification'*** are firms, they shall appoint a Designated Director and Principal Officer, while in case of individual practicing professionals, the professional himself would be the Principal Officer in accordance with rule 2(1)(ba) and 2(1)(f) of PMLR.

4.4.3 **Roles and Responsibilities of Designated Director and the Principal Officer**

4.4.3.1 The Designated Director (where the relevant persons as defined under '***the notification'*** are firms) and the Principal Officer shall be responsible for the following obligations to combat money laundering/ countering the financing of terrorism/ combat proliferation financing:

4.4.3.2 Furnishing of the information under Rule 8 (1) of the PMLR, as prescribed under sub rule (1) of Rule 3 of the said rules every month, by 15th day of the succeeding month, in prescribed format to the Director, FIU-IND, as per the mechanism prescribed in clause 5.1.1. However, the information in respect of a suspicious transaction shall be furnished not later than seven working days on being satisfied that the transaction is suspicious as per Rule 8(2) of the PMLR. Such information shall include any attempted transactions, whether or not made in cash;

4.4.3.3 Evolving an internal mechanism with regard to any directions/ guidelines issued by competent authorities and for furnishing information as prescribed under sub rule (1) of Rule 3 of the PMLR;

4.4.3.4 Communication of firm wide policies, where applicable, relating to prevention of ML,TF and PF to all management and relevant staff that handle account information, money and client records, etc. within their organisation;

4.4.3.5 Implementation of other internal policies as drawn up under clause 7 of the present document and, including:

a. Maintenance of records;
b. Compliance with relevant statutory and regulatory requirements;
c. Cooperation with the relevant law enforcement authorities, including the timely disclosure of information;

4.4.3.6 Ensuring the robustness of periodic review of compliance function to ensure compliance with the policies, procedures and controls relating to the prevention of ML, TF and PF, including detection of suspected money laundering transactions.

4.5. Appointment of Nodal Officer and Permanent Technical Committee by SRBs

The SRBs shall undertake appointments as laid down below, with clear terms of reference and the objectives to be achieved via said appointment:

4.5.1 A "Nodal Officer" for the purpose of interaction and information sharing between their respective members and FIU-India, which may include notifications issued by competent authorities from time to time.

4.5.2 SRBs shall constitute a Permanent Technical Committee whose role is to verify that a relevant person filing prescribed report is holding certificate of practice, before forwarding the report to FIU-India.

4.5.3 The contact details of the Nodal Officer and head of the Permanent Technical Committee shall be communicated to FIU-IND within reasonable time in the event of changes.

4.6. Training

Appropriate training to be provided to employees (compliance and others)

4.6.1 Relevant persons carrying out financial transactions notified vide ***'the notification'***, should have adequate screening procedures when hiring employees.

4.6.2 Instruction manuals on the procedures for KYC, CDD, sanctions screening, record-keeping and transaction monitoring and review should be included in training material.

4.7. Periodic Review

Periodic review of policies, procedures and controls shall be undertaken to ascertain their alignment with extant statutory and regulatory requirements.

4.8. Know Your Customer (KYC) Norms

All relevant persons carrying out financial transactions on behalf of their clients, as notified under '***the notification'***, must have a robust mechanism in place for complying with KYC requirements prior to on boarding of clients as well as for carrying out re-KYC and continued due diligence (CDD) of existing customers in accordance with guidelines issued by SRBs in this regard.

4.9. Client due Diligence (CDD) Norms

4.9.1 Relevant persons as notified under '***the notification'***, should maintain accurate and up-to-date customer information.

4.9.2 Rule 9 of PML (Maintenance of Records) Rules, 2005 provides for 'Client Due Diligence' and in accordance with Rule 9 of these Rules each relevant person as notified under '***the notification'***, shall adopt written procedures to implement the anti-money laundering provisions as envisaged under the PMLA, related to the 'Client Due Diligence Process'.

4.9.3 Relevant persons as notified in '***the notification'***, would be expected to make use of relevant measures:

i. Perform robust due diligence on clients/ counterparties;
ii. Identify risk-related details about the client through sanctions screening
iii. Store customer KYC information for up to five years; and
iv. All identification documents secured through the CDD measures should be retained by for a period of at least five years as recommended under Chapter IV clause (3) of PMLA, 2002.
v. The extent of the ongoing CDD measures applied should be determined on a risk-sensitive basis.
vi. However, it should be kept in mind that as a business relationship develops, the associated ML/TF/PF risks may change.

4.10. Enhanced Due Diligence (EDD) Norms

4.10.1 Relevant persons as notified under '***the notification'***, should examine, as far as reasonably possible, the background and purpose of all complex, unusually large transactions, and all unusual patterns of transactions carried out on behalf of their clients,, which have no apparent economic or lawful purpose. Where the risks of money laundering, terrorist financing or proliferation financing are higher, they must conduct enhanced due diligence, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

4.10.2 Conducting enhanced due diligence should not be limited to merely documenting income proofs. It includes measures and procedures which are more rigorous and robust than normal KYC. These measures should be commensurate with the risk. While not intended to be exhaustive, the following are some of the reasonable measures in carrying out enhanced due diligence:

a. More frequent review of the customers' profile/transactions
b. Application of additional measures like gathering information from publicly available sources or otherwise
c. Reasonable measures to know the customer's that the source of funds is commensurate with the assessed risk of customer and product profile which may include:
    i. Conducting independent enquiries on the details collected on /provided by the customer where required,
    ii. Consulting a credible database, public or otherwise, etc.,

4.11. EDD with respect to high-risk jurisdictions/ persons/ entities

Due to the potential for increased anonymity or obfuscation of financial flows and the challenges associated with conducting CDD, including customer identification and verification, the indicative list (inter alia) of activities regarded as posing high ML/TF/PF risks that may potentially require the application of monitoring and EDD measures, where appropriate, is as below,

a. Application of EDD measures to business relationships and transactions with natural and legal persons from higher risk jurisdictions specifically with countries designated as tax-havens and those on the FATF grey and black lists.

b. Implementation of EDD procedures when entering into business relationships with Politically Exposed Persons ("PEPs"). For the purposes of these guidelines 'PEP' shall have the same meaning assigned to it as per rule 2(1) (db) of PMLR.

c. In cases where relevant persons as notified under '***the notification'***, are not able to undertake the required EDD, they must file a suspicious transaction report (STR).

4.12. Sanctions screening for notified activities

4.12.1 For the purpose of enhanced monitoring, sanctions screening should be carried out both at the time of on boarding, as well as when any of the notified activities are carried out and at the time of additions to designated lists.

4.12.2 Relevant persons as notified under '***the notification'***, must ensure prompt application of the directives when issued by the competent authorities for implementing United Nations Security Council Resolutions, as well as national sanctions, relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, and other related directives, as well as compliance with all other applicable laws, regulatory requirements and guidelines in relation to economic sanctions. Prompt application of the directives when issued by the competent authorities relating to the individuals designated as 'terrorist' under Section 35(1)(a) of the UAPA, 1967 and directives when issued by the competent authorities under WMDA, shall be ensured

4.13. Counterparty Screening

4.13.1 Relevant persons as notified under '***the notification'***, when acting on behalf of their clients shall ascertain any emergent risk stemming from suspicious transaction history or other information such as adverse media, published information about regulatory or criminal penalties in respect of their client's counterparty/ies.

5. Reporting Obligations of relevant persons as notified under '*the notification'*.

The PMLA, PMLR cast obligations pertaining to filing of reports on certain reportable transactions to Financial Intelligence Unit-India (FIU-IND) set up by the Government of India to coordinate and strengthen collection and sharing of financial intelligence through effective national, regional, and global network to combat money laundering

and related crimes. FIU-IND is the central nodal agency responsible for receiving, processing, analysing, and disseminating information relating to reportable transactions.

All relevant persons as notified under '***the notification'***, are required to, where they have reasonable grounds to suspect that funds are the proceeds of crime or are related to ML, TF and PF, report their suspicions promptly to FIU-IND in the form of suspicious transaction reports, as well as other reportable transactions in pursuance of PMLA and PMLR, as per the mechanism prescribed in clause 5.1.1 hereunder.

5.1. Reporting to Financial Intelligence Unit-India

In order to combat the menace of money-laundering, terror financing and other related serious crimes, Rule 7(3) of the PMLR casts an obligation on every reporting entity to evolve an internal mechanism to detect transactions as specified under Rule 3(1) of the PMLR and furnishing information about such transactions to the Director, Financial Intelligence Unit-India (FIU-IND).

5.1.1. Mechanism for reporting to FIU-India:

Relevant persons are required to file prescribed reports with FIU-India through the respective SRBs. The SRBs shall verify that they hold a certificate of practice before forwarding the reports to FIU-INDIA. In case of a relevant person holding certificates of practice from multiple SRBs, the relevant SRB shall be determined by such relevant person based on the nature of services provided to the client. The mechanism for reporting to FIU would be forwarded as a separate document.

5.1.2. Format for reporting Transactions

The format for reporting transactions, including suspicious transactions made or attempted, as required under Rule 7(2) of PMLR, would be as prescribed by FIU-IND.

5.1.3. Suspicious Transactions Report (STR):

Rule 8(2) read with Rule 3(1)(D) of the PMLR provides for timely reporting of a suspicious transaction, which also includes reporting of attempted suspicious transactions, to the Financial Intelligence Unit (FIU-IND), if a reporting entity suspects or has reasonable grounds to suspect that funds used by a client are the proceeds of a

criminal activity, or are related to terrorist financing or proliferation financing. As detailed in Rule 3(1) of PMLR, suspicious transactions shall be reported not later than seven working days from the date of forming of suspicion on such transaction.

Mechanism for monitoring suspicious transactions should be aligned to the category relevant persons as notified under '***the notification'***, and the services they provide. Special attention should be paid to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Background of such transactions, including all documents/office records/memorandums pertaining to such transactions, as far as possible, should be examined by the Principal Officer for recording their findings.

6. Prohibition on Tipping-off

Reporting entities and their directors, officers, and employees (permanent and temporary) are prohibited from disclosing ("tipping off") that an STR or any information is furnished to FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/ or any information but even before, during and after the submission of an STR or any such information to FIU-IND. Thus, it shall be ensured that there is no tipping off to the client at any level as provided for under Section 12(2) of PMLA.

7. Maintenance of Records

Relevant persons as notified under '***the notification'***, are required to retain records as defined in Sections 12(1)(a) and 12(1)(e)of PMLA and for a period of five years after the business relationship between a client and the reporting entity has ended or the engagement has been closed, whichever is later, as mentioned in Section 12(3) and 12(4) of PMLA , in order to ensure that such documents are not destroyed.

8. Risk Assessment

Risk assessments must be carried out to understand risk exposure. Further, a risk based approach (RBA) must be adopted to facilitate priority allocation of resources for appropriate control and oversight of AML/CFT/CPF safeguards. Relevant persons as notified under '***the notification'***, shall carry out risk assessment to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk, severally and together, for customers, countries or geographic areas, and services, transactions or delivery channels that is consistent with the national risk assessment duly notified by the Central Government.

A key element of their RBAs will entail that they should:

8.1 Take appropriate steps to ensure that any identified risks are managed and mitigated through the establishment of appropriate and effective policies, procedures, and controls.

8.2 The risk assessment shall be documented and be kept up-to-date. The Relevant persons as notified under ***'the notification'***, shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied to their clients. It shall be made available to competent authorities and SRBs, as and when required.

8.3 Risk Assessments should be subject to regular review and updation to ensure an effective system for remedying any identified deficiencies.

9. Role of Statutory Body (SRB) in supervision and monitoring

The ICAI, ICSI and ICMAI are Statutory Bodies (SRBs) in respect of the relevant persons as notified under '***the notification'***, and have a role in regulating the relevant persons that are qualified to enter and practise in the said professions. They also perform supervisory, advisory and/ or monitoring functions (e.g. to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession) to ensure that the objectives laid down in the PMLA and the rules framed thereunder are achieved in letters and spirit.

The following obligations are cast on the SRBs in respect of legal provisions pertaining to AML/CFT/CPF,

9.1. Understanding, Mitigating and Managing ML/TF/PF Risk

SRBs shall take necessary steps for spreading awareness about and encourage the compliance pertaining to legal provisions on AML/CFT/CPF, by their members. SRBs shall ensure that the norms and system are in place to take action against the member who is relevant person as per ***'the notification'***, but has failed to comply with the expectations related to AML/CFT/CPF compliance.

9.2. Monitoring and Supervision

9.2.1 SRBs should take measures to effectively monitor relevant persons through on-site and off-site supervision, in accordance with their guidelines/ notifications/ ethical standards.

9.2.2 The frequency and nature of ongoing AML/CFT supervision: SRBs should proactively adjust the frequency of AML/CFT supervision in line with the risks identified and combine periodic reviews and ad hoc AML/CFT supervision.

9.3. Guidance for SRBs

SRBs should communicate their regulatory expectations to the regulated members including,

9.3.1 Guidance on filing of Suspicious Transaction Reports with FIU-India should be issued to the relevant persons as notified under ***'the notification'***.

9.3.2 Guidance on the procedures for KYC, CDD, sanctions screening, record-keeping and transaction monitoring and review should be issued.

9.4. Information Exchange

Information sharing and intelligence sharing arrangements between SRBs and public authorities (such as FIU-India and law enforcement) is important to combat ML/TF/PF and should be robust, secure and subject to compliance with national legal requirements. The type of information that could be shared includes:

a. ML/TF risk assessments;

b. Typologies (i.e. case studies) of how money launderers or terrorist financers have misused relevant persons as notified under '***the notification'***;

c. Feedback on STRs and other relevant reports;

d. Targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards such as confidentiality agreements, it may also be appropriate for authorities to share targeted confidential information with the relevant persons as notified under '***the notification'***.

e. Countries, persons or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions.

***