THE INSTITUTE OF
Company Secretaries of India
भारतीय कम्पनी सचिव संस्थान
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament
(Under the jurisdiction of Ministry of Corporate Affairs)

ICSI (ANTI MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND KNOW YOUR CLIENT) GUIDELINES, 2026

In terms of the provisions of Prevention of Money- Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of records) Rules, 2005 (as amended from time to time), Reporting Entity are required to undertake certain actions.

In exercise of the powers conferred by the **AML & CFT Guidelines for Professionals with Certificates of Practice from ICAI, ICSI and ICMAI**, the Council of the Institute of Company Secretaries of India hereby issues the following guidelines:

CHAPTER I
PRELIMINARY

1. SHORT TITLE AND COMMENCEMENT

These Guidelines may be called as ICSI (Anti-Money Laundering, Counter-Terrorist Financing and Know Your Client) Guidelines, 2026 (ICSI AML, CFT and KYC Guidelines 2026). These Guidelines shall come into force with effect from March 27, 2026.

2. APPLICABILITY

The provisions of these Guidelines shall apply to every Reporting Entity who is registered as such with the Institute of Company Secretaries of India (ICSI).

3. OBJECTIVE

This document aims to provide the Reporting Entities registered with ICSI with a set of guidelines to conduct KYC and due diligence of the clients in accordance with **AML & CFT Guidelines for Professionals with Certificates of Practice from ICAI, ICSI and ICMAI** under the provisions of Prevention of Money Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 as amended from time to time.

4. DEFINITIONS

(1) In these Guidelines, unless the context otherwise requires, -

i. "Act" means the Prevention of Money Laundering Act, 2002

ii. "Beneficial Owner" means an individual who ultimately owns or controls a client of a reporting entity or the person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person.

iii. "Client" means a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who engaged in the transaction or activity, is acting

iv. "Client due diligence" means due diligence carried out on a client referred to in clause (ha) of sub-section (1) of Section 2 of the Act using reliable and independent sources of identification

v. "Designated Director" means a person designated by the Reporting Entity to ensure overall compliance with the obligations imposed under Chapter IV of the Act and the rules and includes:

   a) the managing partner if the Reporting Entity is a partnership firm,

   b) the proprietor if the Reporting Entity is a proprietorship concern,

vi. "Financial Intelligence Unit – India" refers to the national agency, set by the Government of India, which is inter-alia responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions.

vii. "Guidelines" means the AML & CFT Guidelines for Professionals with Certificates of Practice from ICAI, ICSI and ICMAI effective from June 19, 2023.

viii. "Know Your Client (KYC) records" means the records, including the electronic records, relied upon by a reporting entity in carrying out client due diligence as referred to in Rule 9 of PML Rules, 2005.

ix. "Money Laundering" shall have the meaning assigned to it under section 3 of the Act.

x. "Notification" for the purpose of these Guidelines shall mean the notification F.No.P-12011/12/2022-ES Cell-DOR, dated May 03, 2023 issued by the Ministry of Finance (Department of Revenue).

xi. "PML Rules or Rules" means the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

xii. "Principal Officer" means an officer designated by the Reporting Entity.

xiii. "Politically Exposed Persons" (PEPs) are individuals who have been entrusted with prominent public functions by a foreign country, including the heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

xiv. "Relevant Person" means a relevant person as defined under the notification as notified vide Central Government notification F.No. P-12011/12/2022-ES Cell-DOR dated May 03, 2023.

xv. "Reporting entity" means a banking company, financial institution, intermediary or a person carrying on a designated business or profession

xvi. "Suspicious transaction" means a transaction referred to in clause (h), including an attempted transaction, whether or not made in cash, which to a person acting in good faith—

   a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

   b) appears to be made in circumstances of unusual or unjustified complexity; or

   c) appears to have no economic rationale or bona fide purpose; or

d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

Explanation—Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organisation or those who finance or are attempting to finance terrorism.

(2) All other words and expressions used and not defined in these rules but defined in the PML Act, 2002 and PML Rules, 2005 shall have the meaning respectively assigned to them in the Act.

CHAPTER II
DUTIES OF REPORTING ENTITY AND DESIGNATED DIRECTOR/PRINCIPAL OFFICER

5. DUTIES OF A REPORTING ENTITY

Every Reporting Entity (RE) shall:

i. establish systems for identifying, monitoring and reporting suspected Money Laundering (ML) and Terrorist Financing (TF) transactions to the law enforcement authorities (if so required);

ii. implement policies, procedures, and internal controls that effectively serve to prevent and impede ML and TF incorporating key elements of these Guidelines.

iii. appoint a Designated Director and/or Principal Officer as defined under rule 2(1)(bb) and rule 2(1)(1) of PML Rules, 2005.

iv. adopt client acceptance and KYC policies and undertake client due diligence (CDD) measures in respect of notified transactions.

v. adopt internal policy for implementation of these guidelines.

vi. review its clients, their business and transactions against United Nations Security Council Sanctions lists and also against any other relevant sanctions list when complying with Client identification and verification.

vii. furnish the Suspicious Transaction Report (STR) regarding a suspicious transaction to FIU-IND through SRBs (ICSI), on being satisfied that the transaction is suspicious. Such information shall include any attempted transaction, whether or not made in cash.

viii. retain records defined in sec 12(1)(a) and 12(1) (e) of PML Act, 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 PML Act, 2002.

ix. along with their directors, officers and employees be prohibited from disclosing to the client, about any information regarding STR filing to FIU-IND.

x. provide AML/CFT training to all relevant employees, periodically

6. DUTIES OF A DESIGNATED DIRECTOR / PRINCIPAL OFFICER

The Designated Director shall ensure:

i. Furnishing of the information under Rule 8 (1) of the PML Rules;

ii. 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;

iii. Implementation of other internal policies 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;

iv. Periodic review of policies, procedures and internal controls to ensure their effective compliance.

CHAPTER III

DUE DILLIGENCE

7. CLIENT DUE DILIGENCE

Rule 9 of PML Rules, 2005 provides for 'Client Due Diligence'. 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'.

Reporting Entity, 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 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.

However, it should be kept in mind that as a business relationship develops, the associated ML/TF/PF risks may change.

7.1. Types of Client Due Diligence

7.1.1. Simplified Client Due Diligence

Where the risks of ML/TF are low, a Reporting Entity may conduct simplified CDD by:

a) Verifying the identity of Client and beneficial owner after the establishment of business relationship

b) Reduced frequency of Client identification data updates.

c) Reduced degree of on-going monitoring and scrutinizing transactions, based on reasonable monetary threshold.

d) inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures shall not be adopted where there is a suspicion of ML/TF.

7.1.2. Enhanced Due Diligence

i. Where the risks of ML/TF are high, a Reporting Entity shall conduct Enhanced due diligence measures.

ii. Enhanced due diligence is to be undertaken for higher-risk clients, such as Politically Exposed Persons (PEPs) and individuals closely associated with them.

iii. The Reporting Entity should:

i. consider 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.

ii. increase the degree and nature of monitoring of business relationship, in order to determine whether the transactions or activities appear unusual or suspicious.

iii. take additional steps to examine the ownership and financial position, including sources of funds of the client;

iv. take additional steps as may be prescribed to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties

iv. Where any specified transaction or series of specified transactions undertaken by a client is considered suspicious or likely to involve proceeds of crime, the Reporting Entity shall increase the future monitoring of the business relationship with the client, including greater scrutiny or transactions.

v. Enhanced due diligence may be carried out by:

i. Documenting income proofs

ii. Enhanced frequency of review of clients' profile/transactions

iii. Gathering information of the client from publicly available sources, such as:

a. Occupation, volume of assets, information available through public databases, internet, etc., and.

b. Ownership and financial position, including source of wealth and source of funds of the clients or, if applicable, of the Beneficial Owner.

c. Purpose behind conducting the specified transaction and the intended nature of the relationship.

iv. Conducting independent enquiries on the details collected on /provided by the Client where required

v. updating the identification data and client's beneficial owner more regularly

vi. Enhanced monitoring of business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

71.1.3. Ongoing Client Due Diligence

While undertaking ongoing Client due diligence, as required under aforesaid clauses, a Reporting Entity shall:

(i) Periodically review each Client to ensure that the risk rating assigned is commensurate with the ML/TF risks posed by the Client.

(ii) Request additional information and conduct a review of the Client's risk profile in order to determine if additional measures are necessary, where there are indications that the risks associated with an existing business relation with the Client may have increased.

(iii) Observe the conduct of Client's account and scrutinize transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with Reporting Entity's knowledge of the Client, its business and risk profile.

(iv) Pay particular attention to any complex, unusually large or unusual patterns of transactions undertaken throughout the course of business relations.

(v) Make further enquiries into the background and purpose of the transaction specified in above clause and document its findings so that this information is made available to the relevant authorities, if required.

(vi) Ensure that the Client Due Diligence data, documents and information obtained in respect of Clients, natural persons appointed to act on behalf of the Clients, related parties of the Clients and beneficial owners of the Clients, are relevant and kept up-to-date.

7.2. Client Identification and Verification

The Reporting Entity to conduct the CDD by obtaining following requisite documents:

Features	Documents to be Obtained
Individuals	
Natural Person	**Identity Proof (any of the following)** • Identity • Passport • PAN card • Voter's Identity Card • Driving licence • Identity card (subject to the satisfaction of reporting entity) • Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of reporting entity **Address Proof (any of the following)** • Telephone bill • Bank account statement • Letter from any recognized public authority • Electricity bill • Ration card • Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of reporting entity
Foreign Nationals	• National Identity Card and Voter Identification Card, issued by the Governments of foreign jurisdictions or agencies authorized by them capturing the photograph, name, date of birth and address

Features	Documents to be Obtained
Companies	
• Name of the company • Principal place of business • Mailing address of the company • Telephone Number	• Certificate of incorporation and Memorandum & Articles of Association • Resolution of Board of Directors and identification of those who have authority to deal with the reporting entity • Copy of PAN allotment letter • Copy of telephone bill
Partnership firms	
• Legal name • Address • Names of all partners and their addresses • Phone numbers of firm and partners	• Registration certificate, if registered • Partnership deed • Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf • Any officially valid document identifying the partners • Telephone bill in the name of firm/partners
Trusts & foundations	
• Names of trustees, settlers, beneficiaries and signatories • Names & addresses of founder, managers, directors & beneficiaries • Telephone numbers	• Certificate of registration, if registered • Power of Attorney granted to transact business on its behalf • Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses • Telephone bill

Further, in cases where the Client is a legal person or legal arrangement, a Reporting Entity shall, also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement.

7.3. Related Party and Beneficial Owner Identification

(i) A Reporting Entity additionally shall thrive to obtain information on related accounts wherein the Client holds or has held a prominent public position.

(ii) The Reporting Entity shall:

a) identify the Beneficial Owners and

b) take reasonable measures to verify their identities using the relevant information or data obtained from reliable, independent sources.

(iii) Identification of connected parties or related parties may be undertaken using publicly available sources or databases such as company registries, annual reports. Additionally, it could be based on substantiated information provided by the Clients.

(iv) For identification of the connected parties, a Reporting Entity shall obtain at the very least, the following information of each related or connected party:

a) Full name, including any aliases; and

b) Unique Identification Number (such as an Identity card number, passport number, etc.).

7.4. Timing of CDD

A Reporting Entity shall undertake Client Due Diligence:

7.4.1. At the time of establishing business relationship: The CDD process should commence during initial discussions but must be completed before the reporting entity agrees to provide services or accepts the client or new engagement; and,

7.4.2. A Reporting Entity shall also undertake Client Due Diligence if, at any time:

a) there are significant changes in the nature of the business relationship, ownership, or control structure.

b) in relation to an existing Client, it doubts the veracity or adequacy of documents, data or information obtained for the purposes of Client Due Diligence;

c) it suspects ML/TF; or,

d) there is a change in risk-rating of the Client, or it is otherwise warranted by a material change in circumstances of the Client.

CHAPTER IV
SUSPICIOUS TRANSACTIONS

8. IDENTIFICATION OF SUSPICIOUS TRANSACTIONS

8.1. A Reporting Entity shall establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious transactions with respect to potential ML/TF.

8.2. A Reporting Entity can identify suspicious transactions by following these four steps:

8.2.1. Detect suspicious indicator(s): Suspicious indicators act as “red flags” and alerts for the Reporting Entity to pay more attention to a particular Client or transaction(s). These indicators include:

a) complex, unusual or large transactions that have no apparent economic or lawful purpose

b) transaction (or attempted transaction) does not match the known background, nature and type of client, including source of funds;

c) unusual Client behaviour;

d) Clients whose identity verification seems difficult or clients that appear non-cooperative

e) Substantial increases in business without apparent cause

f) Attempted transfer of investment proceeds to apparently unrelated third parties

8.2.2. Ask the client questions: If one or more suspicious indicators are detected, the Reporting Entity and its employees may ask the Client relevant and appropriate questions to determine whether there is a reasonable explanation for that observed indicator.

8.2.3. ***Review client's records:*** To consider all information that is already known to it about the Client. This may include:

a) usual occupation, business or principal activity;

b) transaction history;

c) risk profile;

d) income level;

e) source of income as stated during initial engagement;

f) reasons for the suspicious transactions as provided by the Client;

g) relationship with the sender or beneficiary of funds;

h) frequency of transactions;

i) size and complexity of the transaction;

j) identity or location of any other person(s) involved in the transaction;

k) usual or typical financial, business or operational practices or behaviour of Clients in similar occupation or business category; and

l) availability of identification documents and other documentation

8.2.4. ***Evaluation of information:*** A Reporting Entity shall evaluate the:

a) Suspicious indicators,

b) information solicited from the Client through questions asked, and

c) known information about the Client to determine if there are reasonable grounds to suspect that the transaction(s) is related to the commission of a ML/ TF or any other serious offence.

9. REPORTING OF SUSPICIOUS TRANSACTIONS

9.1. Legal Obligation

9.1.1. The PML Act and PML Rules made thereunder cast obligations pertaining to filing of reports of certain reportable transactions on Reporting Entity to Financial Intelligence Unit-India (FIU-IND).

9.1.2. If the Reporting Entity have reasonable grounds to suspect that funds are the proceeds of crime or are related to ML, TF and PF, shall report their suspicions promptly to FIU-IND in the form of suspicious transaction reports, as well as other reportable transactions in pursuance of PML Act and PML Rules, 2005.

9.1.3. If a Reporting Entity is not able to obtain satisfactory evidence of a client's identity, the Reporting Entity should not proceed further with the transaction unless directed in writing to do so by the FIU-IND.

9.1.4. If the Reporting Entity considers the reasons for the client's failure or refusal to produce adequate identification documentations as unreasonable or suspicious, it shall report the attempted transaction to the FIU-IND as a suspicious transaction.

9.1.5. 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.

9.2. Mechanism for reporting

Reporting Entity is required to file prescribed reports with FIU-India through its Statutory body i.e., ICSI (SRB)

9.2.1. The SRBs shall verify that they hold a certificate of practice before forwarding the reports to FIU-INDIA.

9.2.2. 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 by SRB.

9.2.3. The mechanism for reporting to FIU-IND would be forwarded as a separate document.

9.2.4. Mechanism for monitoring suspicious transactions should be aligned to the category relevant persons as notified under 'the notification', and the services they provide.

9.3. Format for reporting

The reporting of transactions, including suspicious transactions shall be made in the Format as provided over the website of ICSI.

9.4. Time frame on reporting

In terms of Rules, the Reporting Entities shall inter-alia adhere to the following:

(i) 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.

(ii) suspicious transactions shall be reported not later than seven working days from the date of forming of suspicion on such transaction.

9.5. Nil Report

No Nil reporting needs to be made to FIU-IND in case there are no suspicious transaction.

9.6. 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.

10. MAINTAINING OF RECORDS

10.1. A Reporting Entity shall maintain the following records:

i. Copy of all documents and information obtained during initial and ongoing Client Due Diligence;

ii. Records of Client business relationships (both original and certified copies)

iii. Correspondence of information relating business of a client;

iv. Transactions to enable standalone transactions to be reconstructed; and

v. Internal findings and analysis relating to a business transaction or other transactions, where the transaction or business may be unusual or suspicious, whether or not it results in a Suspicious Transactions Report;

vi. Suspicious Transactions Reports and any relevant supporting documents and information, including internal findings and analysis;

vii. Any relevant communications, if made with the FIU-IND;

viii. Any other matter that the Reporting Entity may be expressly required to record and maintain, under these Guidelines.

10.2. The Reporting Entity shall preserve all necessary records, for at least five years, from the date on which business relationship has ended or transaction is completed.

10.3. The above records may be kept in electronic format, subject to the condition that such records are readily accessible and promptly made available to the ICSI or other law enforcement agency, on demand.

****

NOTE$