Anti-Money Laundering 18

This Module includes:

Anti-Money Laundering

SLOB Mapped against the Module

To understand international standards on combating money laundering and provide guidance to prevent and control money laundering transactions in the business operations. (CMLO 2c)

Module Learning Objectives:

To prevent criminal activity, nearly all countries in the world have committed themselves to extremely tough laws against money laundering and terrorist financing. Money laundering is defined as criminal proceeds finding their way into the formal economy via transactions that conceal their true origins. Terrorist financing can come from rogue regimes or terrorist organisations that feed their cells worldwide under trade payments, investments, remittances, and money for education. After studying this module, the students will be able to –

- Understand Money Laundering / Terrorism Financing methods and typologies that are relevant to the organisation
- Analyse the AML policies, procedures systems & controls adopted by the Organisations
- Acquire the skill to identify suspicious activities & unusual behaviour of customers and report them to the AML compliance officer
- Understand the responsibilities and role of individuals in the organisation towards countering money laundering and financing of terrorism.

Introduction

18

Money laundering is the practice of transferring funds gained through illegal activities like gambling, drug trafficking, corruption, or embezzlement into a legitimate source in order to conceal its true source. The objective of money laundering is to show that money from criminal activity has come from a legitimate (legal) source.

The money from the criminal activity is considered dirty and the process launders it to make it look clean.

Money laundering is a crime.

It is the process of conversion of such proceeds of crime, the dirty money to make it appear as legitimate money.

Anti-money laundering (AML) refers to the activities financial institutions perform to achieve compliance with legal requirements to actively monitor for and report suspicious activities.

The United States was one of the first nations to enact anti-money laundering legislation when it established the Bank Secrecy Act (BSA) in 1970. In an early effort to detect and prevent money laundering, the BSA has since been amended and strengthened by additional anti-money laundering laws. The Financial Crimes Enforcement Network is now the designated administrator of the BSA with a mission to "safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering, and other illicit activity."

In 1989, multiple countries and organisations formed the global Financial Action Task Force (FATF). Its mission is to devise and promote international standards to prevent money laundering. Shortly after the 9/11 attacks on the US, FATF expanded its mandate to include AML and combating terrorist financing. The International Monetary Fund (IMF) is another important organisation. With 189 member countries, its primary purpose is to ensure the stability of the international monetary system. The IMF is concerned about the consequences money laundering and related crimes can have on the integrity and stability of the financial sector and the broader economy.

Importance of understanding Anti-money laundering

The estimated amount of **money laundered globally in one year is 2% to 5% of global GDP, or US$800 billion to US$2 trillion** – and that's a low estimate. Money laundering often accompanies activities like smuggling, illegal arms sales, embezzlement, insider trading, bribery, and computer fraud schemes. It's also common with organized crime including human, arms or drug trafficking, and prostitution rings.

Anti-money laundering is closely related to counter-financing of terrorism (CFT), which financial institutions use to combat terrorist financing. AML regulations combine money laundering (source of funds) with terrorism financing (destination of funds).

Beyond the moral imperative to fight money laundering and terrorist financing, financial institutions also use AML tactics for:

- **Compliance with regulations** that require them to monitor customers and transactions and report suspicious activity.

- **Protection of their brand reputation** and shareholder value.
- **Avoidance of consent orders** as well as civil and criminal penalties that could be levied because of non-compliance or negligence.
- **Reduction of costs** related to fines, employee and IT costs, and capital reserved for risk exposure.

How Money Laundering Works

To identify and report potential money laundering and address compliance requirements, financial institutions must have a deep understanding of how the crime works. Money laundering involves three stages:

- Placement,
- Layering, and
- Integration.

These are a complex series of transactions that start with depositing funds, then gradually moving them into what appear to be legitimate assets.

Placement refers to how and where illegally obtained funds are placed. Money is often placed via Payments to cash-based businesses; payments for false invoices; "smurfing," which means putting small amounts of money (below the AML threshold) into bank accounts or credit cards; moving money into trusts and offshore companies that hide beneficial owners' identities; using foreign bank accounts, and aborting transactions shortly after funds are lodged with a lawyer or accountant.

Layering refers to separating criminal funds from their source. It involves converting the illicit proceeds into another form and creating complex layers of financial transactions to disguise the funds' origin and ownership. Criminals do this to obfuscate the trail of their illicit funds so it will be hard for AML investigators to trace the transactions.

Integration refers to the re-entry of the laundered funds into the economy in what appears to be normal, legitimate business or personal transactions. This is sometimes done by investing in real estate or luxury assets. It allows launderers and criminals to increase their wealth.

Cycle of Money Laundering

The cycle of money laundering can be broken into following 3 distinct stages :

1. Placement

   1st and initial stage where black money is injected into the formal financial system.

2. Layering

   2nd stage, money injected into the system is layered and moved or spread over various

   Transactions in different accounts and different countries.

   Thus, it becomes difficult to detect the origin of the money.

3. Integration

   3rd and final stage, money enters the financial system in such a way that original association with the crime is sought to be obliterated so that the money can then be used by the offender or person receiving it as clean money.

Proceeds of Crime (Section 2 (1) (u))

It means

1. Any property derived or obtained
2. Directly or indirectly
3. By any person
4. As a result of criminal activity
5. Relating to a scheduled offence or
6. The value of any such property.

Property (Section 2 (1) (v))

Property means any property or assets of every description

1. Whether corporeal or incorporeal
2. Movable or immovable
3. Tangible or intangible

And Includes

4. Deeds and instruments evidencing title to or interest in such property or assets, where ever located

Scheduled Offence (Section 2 (1) (y))

Scheduled Offences means –

1. The offences specified under Part A of the Schedule, or
2. The offences specified under Part B of the Schedule if the total value involved in such offences is Rs 1 crore or more or
3. The offences specified under Part C of the Schedule

Definition of Money Laundering

(Section 3)

Whosoever directly or indirectly

1. Attempts to indulge or
2. Knowingly assists or
3. Knowingly is a party or
4. Is actually involved

   In any process or activity connected with the proceeds of crime and

   1. Projecting it as untainted property or
   2. Claiming it as untainted property

   Shall be guilty of offence of money landering

Punishment for Money Laundering

(Section 4)

Whosoever commits the offence of money-laundering shall be punishable with rigorous imprisonment as well as fine as mentioned below :

1. Whosoever commits the offence of money laundering shall be punishable with rigorous imprisonment from 3 to 7 years and fine.
2. Where the proceeds of crime involved in money laundering relate to any offences pertaining to the (NDPS Act,1985) i.e.Narcotics and Psychotropic substance Act,1985, the , the offence shall be punishable with rigorous imprisonment for a term which shall not be less than 3 years but which may extend upto 10 years and shall also be liable to fine.

Attachment of Property involved in Money Laundering

(Section 5)

Order for Provisional Attachment

Power of Attachment is granted to a Director or any other person not below the rank of Deputy Director for attachment of property involved in money laundering.

It is important to note that to exercise the right of attachment, the concerned officer has to show that based on material in his possession, he has reason to believe (which has to be recorded in writing) that

1. Any person is in possession of any proceeds of crime, and
2. Such proceeds of crime are likely to be concealed, transferred or dealt with in any manner

Which may result in interfering any proceedings, investigations relating to confiscation of such proceeds linked with a crime.

He may in such a case order the prohibition of transfer, conversion, disposition or the movement of such proceeds or property.

The attachment is valid for 180 days from the date of order and following the attachment, the officer must forward the attachment order along with the material in his possession to the Adjudicating Authority of the matter.

Adjucating Authority (AA)

(Section 6)

As per Section 6, the Central Government by notification appoints an Adjudicating Authority to exercise jurisdiction, powers and authority conferred by or under this Act.

An Adjudicating Authority shall consist of Chairperson and 2 other members, provided that 1 member each shall be a person having experience in the field of law, administration, finance and accountancy.

(a) Composition of Adjudicating Authority

a) An AA shall consists of a Chairperson and 2 other members.

Of the 2 members, 1 member shall be a person having experience in the field of law and 1 member shall be a person having experience in the field of finance, accountancy or administration.

b) The Central Government shall appoint a member to be the Chairperson of the AA.

(b) Qualifications of 2 Members

a) To qualify for appointment as a member in the field of law

1. He should be qualified as appointment as District Judge or
2. He should be a member of Indian legal service and should have held a post in Grade I of that service.

b) To qualify for appointment as a member in the field of Finance, Accountancy or Administration , he should have such qualification as may be prescribed in the rules.

(c) Functioning of the AA

a) The jurisdiction of the AA may be exercised by the Benches

b) The Central Government shall, by notification, specify the areas in relation to which each bench of AA may exercise jurisdiction.

(d) Duration of office and Terms and Conditions

a) Chairperson and every member shall hold office for a term of 5 years from the date on which he enters upon his office.

Provided that no Chairperson or other Member shall hold office after he attains the age of 65 years.

b) The salary and allowances payable to and other terms and conditions of service of the Member shall not be varied to his disadvantage after appointment

Power of Survey (Section 16)

Section 16 of PMLA deals with the Power of Survey.

An officer under PMLA has the power to enter and survey a property or premises, if such officer believes that the survey will allow him the opportunity

1. to inspect necessary records which might be available on the premises in question,
2. help verify proceeds of a crime or
3. any transactions related to the proceeds which might be found on the premises or
4. might assist them with any other proceedings being conducted under the Act.

The officer is under an obligation to record the reasons for choosing to survey the premises as well as findings.

Power of Search and seizure (Section 17)

Section 17 of the PMLA deals with the power of search and seizure by the authority.

A Director or any other officer not below the rank of Deputy Director authorised by him for the purpose of this section, on the basis of information in his possession, has reason to believe (the reason for such belief to be recorded in writing) that any person –

1. has committed any act which constitutes money-laundering or
2. is in possession of any proceeds of crime involved in Money-Laundering or
3. is in possession of any records relating to Money-Laundering or
4. is in possession of any property related to crime

then subject to the rules made in this behalf, he may authorise any officer subordinate to him to –

1. enter and search any building, place , vessel, vehicle or aircraft where he has reason to suspect that such records or proceeds of crime are kept
2. break open the lock of any door, box, locker, safe, almirah or other receptacle for exercising the powers conferred by clause (a) where the key thereof are not available
3. seize any record or property found as a result of such search
4. place marks of identification of such record or property, if required or make or cause to be made extracts or copies therefrom
5. make a note or an inventory of such record or property
6. examine on oath any person, who is found to be in possession or control of any record or property, in respect of all matters relevant for the purpose of any investigation under this Act.

Section 18 of the PMLA deals with power to search a person

If an authority has reason to believe (the reason for such belief to be recorded in writing) that any person has

1. secreted about his person or
2. in anything under his possession, ownership, or control any record or proceeds of crime which may be useful for or relevant to any proceedings under this Act,

the authority may search that person and seize such record or property which may be useful for or relevant to any proceedings under this Act.

Arrest under PMLA (Section 19)

Under Section 19 of PMLA, the Deputy Director, Assistant Director, or any other officer authorised on this behalf by the Central Government by general or special order , has the power to arrest a person.

A person can be arrested by the concerned authority, if such authority, is based on material in his possession,

1. Has reason to believe that such a person has been guilty of an offence punishable under PMLA, and
2. The reason for such belief has been recorded in writing

After arresting such a person , the authority is bound to

1. Inform the arrested person about the ground for his arrest
2. Forward a copy of the arrest order along with the material in his possession to the Adjudication Authority
3. Produce such person,within 24 hours, before the Special Court or Judicial Megistrate or a Metropolitan Megistrate, as the case may be, having jurisdiction.

Section 21 of PMLA deals with Retention of Records

1. Where any records have been seized under section 17 or under section 18 or
2. Frozen under sub section (IA) of Section 17 and

   The Investigating officer or any other officer authorised by the Director in this behalf has reason to believe that such records are are required to be retained for any inquiry under this Act, may retain such records for a period not exceeding 180 days from the date on which such records were seized.

3. The person from whom records were seized or frozen, shall be entitled to obtain copies of records retained under sub section (1).
4. On the expiry of 180 days, the records, the records shall be returned to the person from whom such records were seized or whose records were ordered to be frozen unless the Adjudicating Authority permits retention or continuation of freezing of such records beyond the said period.
5. The AA, before authorising the retention or continuation of freezing of such records beyond the period of 180 days, shall satisfy himself that the records are prima facie involved in money laundering and the records are required for the purpose of adjudication under section 8.

Section 23 of PMLA deals with Inter-Connected Transactions

Where money laundering involves 2 or more transactions and 1 or more such transactions are proved to be involved in money laundering then for the purposes of

1. Adjudication or confiscation under section 8 or
2. For the trial of the money laundering offence,

It shall be presumed that the remaining transactions form part of such interconnected transactions,

Unless otherwise proved.

Section 24 of PMLA deals with Presumptions and Onus of Proof

Legal and Regulatory Framework in India

1. **Financial Intelligent Unit-India (FIU-IND)**

The Government of India vide O.M.Dated 18.11.2004 set up the Financial Intelligence Unit (FIU-IND) as the national agency responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions.

FIN-IND is also responsible for coordinating and strengthening efforts of

- National and international intelligence
- Investigation and enforcement agencies

In pursuing global efforts against money laundering and related crimes.

FIU-IND is an independent body that reports directly to the Economic Intelligence Council (EIC), headed by the Finance Minister of India.

Functions of FIU-IND

The main function of FIU-IND is to receive cash/suspicious transaction reports, analyse them and, as appropriate, disseminate valuable financial information to intelligence/enforcement agencies and regulatory authorities . The functions of FIU-IND are:

- **Collection of Information:** Act as the central reception point for receiving Cash Transaction reports (CTRs), Non-Profit Organisation Transaction Report (NTRs), Cross Border Wire Transfer Reports (CBWTRs), Reports on Purchase or Sale of Immovable Property (IPRs) and Suspicious Transaction Reports (STRs) from various reporting entities.
- **Analysis of Information:** Analyze received information in order to uncover patterns of transactions suggesting suspicion of money laundering and related crimes.

- **Sharing of Information:** Share information with national intelligence/law enforcement agencies, national regulatory authorities and foreign Financial Intelligence Units.
- **Act as Central Repository:** Establish and maintain national data base on the basis of reports received from reporting entities.
- **Coordination:** Coordinate and strengthen collection and sharing of financial intelligence through an effective national, regional and global network to combat money laundering and related crimes.
- **Research and Analysis:** Monitor and identify strategic key areas on money laundering trends, typologies and developments.

2. **Enforcement Directorate (ED)**

Responsibility

ED has been given the responsibility to enforce the provisions of the PMLA by conducting investigation to trace the assets derived from proceeds of crime, to provisionally attach the property to ensure prosecution of the offenders and confiscation of the property by the Special court.

Powers

1. ED has powers to impose penalty on reporting entities for non compliance with the PMLA,
2. It has the power of
   - Provisional attachment of property
   - Survey
   - Search and seizure
   - Search persons
   - Arrest
   - Retention of property
   - Retention of records
3. Reserve Bank Of India (RBI)

   RBI, as India's central banking institution, plays a key role in shaping and enforcing guidelines related to financial transactions, including those under the PMLA.

   RBI's guidelines cover aspects such as customer due diligence (CDD), Enhance Due Diligence (EDD), Transaction monitoring and reporting requirements.
4. Securities and Exchange Board of India (SEBI)

   SEBI regulates the securities market in India, and is involved in implementing PMLA guidelines related to securities transactions.
5. Other Regulatory Authorities

   Various other regulatory bodies, including insurance regulators, pension regulators, and sector – specific regulators, contribute to the implementation of PMLA guidelines in their respective domains.

International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation

18.1

Note: For detailed information on 18.1 and 18.2 Concepts, please go through the Documents on The FATF Recommendations (International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation) – Updated March 2022 and Guidance for a Risk-Based Approach (Accounting Profession) – Updated 2019 of Financial Action Task Force (FATF) - www.fatf-gafi.org

Acronyms:

AML/CFT: Anti-Money Laundering / Countering the Financing of Terrorism (also used for Combating the financing of terrorism)

BNI: Bearer-Negotiable Instrument

CDD: Customer Due Diligence

DNFBP: Designated Non-Financial Business or Profession

FATF: Financial Action Task Force

FIU: Financial Intelligence Unit

IN: Interpretive Note

ML: Money Laundering

MVTS: Money or Value Transfer Service(s) NPO: Non-Profit Organisation

Palermo Convention: The United Nations Convention against Transnational Organized Crime 2000

PEP: Politically Exposed Person

R.: Recommendation

RBA: Risk-Based Approach SR.: Special Recommendation SRB: Self-Regulatory Bodies

STR: Suspicious Transaction Report

TCSP: Trust and Company Service Provider

Terrorist Financing Convention: The International Convention for the Suppression of the Financing of Terrorism 1999

UN: United Nations

Vienna Convention: The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

The FATF Recommendations:

A. AML/CFT POLICIES AND COORDINATION

1. **Assessing risks and applying a risk-based approach:**

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation for the efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should also identify, assess, and understand the proliferation financing risks for the country. In the context of Recommendation 1, "proliferation financing risk" refers strictly and only to the potential breach, non-implementation, or evasion of the targeted financial sanctions obligations referred to in Recommendation 7. Countries should take commensurate action aimed at ensuring that these risks are mitigated effectively, including designating an authority or mechanism to coordinate actions to assess risks and allocate resources efficiently for this purpose. Where countries identify higher risks, they should ensure that they adequately address such risks. Where countries identify lower risks, they should ensure that the measures applied are commensurate with the level of proliferation financing risk, while still ensuring full implementation of the targeted financial sanctions as required in Recommendation 7.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering, terrorist financing, and proliferation financing risks.

2. National cooperation and coordination:

Countries should have national AML/CFT/CPF policies, informed by the risks (Proliferation financing risk refers strictly and only to the potential breach, non-implementation, or evasion of the targeted financial sanctions obligations referred to in Recommendation 7) identified, which should be regularly reviewed and should designate an authority or have the coordination or another mechanism that is responsible for such policies.

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors, and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. This should include cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT/CPF requirements with Data Protection and Privacy rules and other similar provisions (e.g., data security/localization).

B. MONEY LAUNDERING AND CONFISCATION

3. Money laundering offence:

Countries should criminalize money laundering based on the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, including the widest range of predicate offences.

4. Confiscation and provisional measures:

Countries should adopt measures similar to those outlined in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of bona fide third parties: (a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations, or (d) property of corresponding value.

Such measures should include the authority to (a) identity, trace, and evaluate the property that is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer, or disposal of such property; (c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries should consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction-based confiscation), or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

C. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5. Terrorist financing offence:

Countries should criminalize terrorist financing based on the Terrorist Financing Convention and should criminalize not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

6. Targeted financial sanctions related to terrorism and terrorist financing:

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including by resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country under resolution 1373 (2001).

7. Targeted financial sanctions related to proliferation:

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression, and disruption of the proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

8. Non-profit organisations:

Countries should review the adequacy of laws and regulations that relate to non-profit organisations that the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate

measures, in line with the risk-based approach, to such non-profit organisations to protect them from terrorist financing abuse, including:

(a) By terrorist organisations posing as legitimate entities;

(b) By exploiting legitimate entities as conduits for terrorist financing, including to escape asset-freezing measures; and

(c) By concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

D. PREVENTIVE MEASURES:

9. Financial institution secrecy laws:

Countries should ensure that financial institution secrecy laws do not inhibit the implementation of the FATF Recommendations.

CUSTOMER DUE DILIGENCE AND RECORD-KEEPING:

10. Customer due diligence:

Financial institutions should be prohibited from keeping anonymous accounts or accounts in fictitious names. Financial institutions should be required to undertake customer due diligence (CDD) measures when:

(i) Establishing business relations;

(ii) Carrying out occasional transactions: above the applicable designated threshold (USD/EUR 15,000); or

(ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

(iii) There is a suspicion of money laundering or terrorist financing; or

(iv) The financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data, or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions are undertaken throughout that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business, and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above but should determine the extent of such measures using a risk-based approach (RBA) by the Interpretive Notes to this Recommendation and Recommendation 1.

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed, and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report about the customer.

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers based on materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

11. Record-keeping:

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from competent authorities. Such records must be sufficient to permit the reconstruction of individual transactions (including the amounts and types of currency involved, if any) to provide, if necessary, evidence for the prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g., copies or records of official identification documents like passports, identity cards, driving licenses, or similar documents), account files, and business correspondence, including the results of any analysis undertaken (e.g., inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

ADDITIONAL MEASURES FOR SPECIFIC CUSTOMERS AND ACTIVITIES

12. Politically exposed persons:

Financial institutions should be required, about foreign politically exposed persons (PEPs) (whether a customer or beneficial owner), in addition to performing normal customer diligence measures, to:

(a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;

(b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;

(c) take reasonable measures to establish the source of wealth and source of funds; and conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher-risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs B, C and D.

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

13. Correspondent banking:

Financial institutions should be required, about cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

(a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

(b) Assess the respondent institution's AML/CFT controls;

(c) Obtain approval from senior management before establishing a news correspondent relationship;

(d) Clearly understand the respective responsibilities of each institution; and

(e) Concerning "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank and that it can provide relevant CDD information upon request to the correspondent bank.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

14. Money or value transfer services:

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use agents include them in their AML/CFT programs and monitor them for compliance with these programs.

15. New technologies:

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise about: (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place before the launch of new products, business practices, or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

16. Wire transfers:

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for detecting those that lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), relating to the prevention and suppression of terrorism and terrorist financing.

RELIANCE, CONTROLS, AND FINANCIAL GROUPS

17. Reliance on third parties:

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

(a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.

(b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(c) The financial institution should satisfy itself that the third party is regulated, supervised, or monitored, and has measures in place for compliance with, CDD and recordkeeping requirements in line with Recommendations 10 and 11.

(d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11, and 12, and programs against money laundering and terrorist financing, by Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programs are supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group program, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

18. Internal controls and foreign branches and subsidiaries:

Financial institutions should be required to implement programs against money laundering and terrorist financing. Financial groups should be required to implement group-wide programs against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country's requirements in implementing the FATF Recommendations through the financial groups' programs against money laundering and terrorist financing.

19. Higher-risk countries:

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

REPORTING OF SUSPICIOUS TRANSACTIONS

20. Reporting of suspicious transactions:

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

21. Tipping-off and confidentiality:

Financial institutions, their directors, officers, and employees should be:

(a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether the illegal activity occurred; and

(b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU. These provisions are not intended to inhibit information sharing under Recommendation 18.

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

22. DNFBPs: customer due diligence:

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

(a) Casinos- when customers engage in financial transactions equal to or above the applicable designated threshold.

(b) Real estate agents- when they are involved in transactions for their clients concerning the buying and selling of real estate.

(c) Dealers in precious metals and dealers in precious stones- when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

(d) Lawyers, notaries, other independent legal professionals, and accountants – when they prepare for or carry out transactions for their clients concerning the following activities:

- Buying and selling of real estate;
- Managing client money, securities, or other assets;
- Management of the bank, savings, or securities accounts;
- The organisation of contributions for the creation, operation, or management of companies;
- Creation, operation, or management of legal persons or arrangements, and buying and selling of business entities.

(e) Trust and company service providers – when they prepare for or carry out transactions for a client concerning the following activities:

- Acting as a formation agent of legal persons;
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position to other legal persons;
- Providing a registered office, business address, accommodation, correspondence, or administrative address for a company, a partnership, or any other legal person or arrangement;
- Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

23. DNFBPs: Other measures:

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

(a) Lawyers, notaries, other independent legal professionals, and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction about the activities described in paragraph (d) of recommendation 22. Countries are strongly encouraged to extend the reporting requirement for the rest of the professional activities of accountants, including auditing.

(b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

(c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction about the activities referred to in paragraph (e) of Recommendation 22.

E. TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24. Transparency and beneficial ownership of legal persons:

Countries should assess the risks of misuse of legal persons for money laundering or terrorist financing, and take measures to prevent their misuse. Countries should ensure that there is adequate, accurate, and up-to-date information on the beneficial ownership and control of legal persons that can be obtained or accessed rapidly and efficiently by competent authorities, through either a register of beneficial ownership or an alternative mechanism. Countries should not permit legal persons to issue new bearer shares or bearer share warrants and take measures to prevent the misuse of existing bearer shares and bearer share warrants. Countries should take effective measures to ensure that nominee shareholders and directors are not misused for money laundering or terrorist financing. Countries should consider facilitating access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

25. Transparency and beneficial ownership of legal arrangements:

Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. In particular, countries should ensure that it is adequate, accurate, and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities.

Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

F. POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES, AND OTHER INSTITUTIONAL MEASURES REGULATION AND SUPERVISION

26. Regulation and supervision of financial institutions:

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution. Countries should not approve the establishment, or continued operation, of shell banks.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply similarly for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes.

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

27. Powers of supervisors:

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorized to compel the production of any information from financial institutions that is relevant to monitoring such compliance and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

28. Regulation and supervision of DNFBPs:

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

(a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures. At a minimum:

- Casinos should be licensed;
- Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, holding a management function in, or being an operator of, a casino; and
- Competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements.

(b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by: (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also: (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, holding or being the beneficial owner of a significant or controlling interest, or holding a management function, e.g., through evaluating persons based on a "fit and proper" test; and (b) have

effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.

OPERATIONAL AND LAW ENFORCEMENT

29. Financial intelligence units:

Countries should establish a financial intelligence unit (FIU) that serves as a national center for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences, terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities and should have access on a timely basis to the financial, administrative, and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities:

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences, and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing, and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialized in financial or asset investigations. Countries should ensure that, when necessary, cooperative investigations with appropriate competent authorities in other countries take place.

31. Powers of law enforcement and investigative authorities:

When conducting investigations of money laundering, associated predicate offences, and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, prosecutions, and, related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs, and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations can use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences, and terrorist financing. These investigative techniques include undercover operations, intercepting communications, accessing computer systems, and controlled delivery. In addition, countries should have effective mechanisms in place to identify, promptly, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences, and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

32. Cash couriers:

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering, or predicate offences, or that are falsely declared or disclosed. Countries should ensure that effective, proportionate, and dissuasive sanctions are available to deal with persons who make a false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering, or predicate

offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

GENERAL REQUIREMENTS:

33. Statistics:

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions, and convictions; on property frozen, seized, and confiscated; and on mutual legal assistance or other international requests for cooperation.

34. Guidance and feedback:

The competent authorities, supervisors, and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

SANCTIONS:

35. Sanctions:

Countries should ensure that there is a range of effective, proportionate, and dissuasive sanctions, whether criminal, civil, or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should apply not only to financial institutions and DNFBPs but also, to their directors and senior management.

G. INTERNATIONAL COOPERATION:

36. International instruments:

Countries should take immediate steps to become a party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

37. Mutual legal assistance:

Countries should rapidly, constructively, and effectively provide the widest possible range of mutual legal assistance regarding money laundering, associated predicate offences, and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for assisting and, where appropriate, should have in place treaties, arrangements, or other mechanisms to enhance cooperation. In particular, countries should:

(a) Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance.

(b) Ensure that they have clear and efficient processes for the timely prioritization and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.

(c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offecse is also considered to involve fiscal matters. Do not refuse to execute a request for mutual legal assistance because laws require

financial institutions or DNFBPs to maintain secrecy or confidentiality (except where the relevant information that is sought is held in circumstances where legal, a professional privilege or legal professional secrecy applies).

(d) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, not withstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalize the conduct underlying the offence. Countries should ensure that the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

(a) All those relating to the production, search, and seizure of information, documents, or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and

(b) A broad range of other powers and investigative techniques;

are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Countries should, when making mutual legal assistance requests, make their best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means.

Countries should, before sending requests, make their best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human, and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

38. Mutual legal assistance: freezing and confiscation:

Countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences, and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of the corresponding value. This authority should include being able to respond to requests made based on non-conviction-based confiscation proceedings and related provisional measures unless this is inconsistent with fundamental principles of their domestic law. Countries should also have effective mechanisms for managing such property, instrumentalities, or a property of corresponding value, and arrangements for coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

39. Extradition:

Countries should constructively and effectively execute extradition requests in a relation to money laundering and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts, or terrorist organisations. In particular, countries should:

(a) Ensure money laundering and terrorist financing are extraditable offences;

(b) Ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritization where appropriate. To monitor the progress of requests a case management system should be maintained;

(c) Not place unreasonable or unduly restrictive conditions on the execution of requests; and

(d) Ensure they have an adequate legal framework for extradition.

Each country should either extradite its nationals or, where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case, without undue delay, to its competent authorities for prosecution of the offences outlined in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalize the conduct underlying the offence.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrest or judgments, or introducing simplified extradition of consenting persons who waive formal extradition proceedings. The authorities responsible for extradition should be provided with adequate financial, human, and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

40. Other forms of international cooperation:

Countries should ensure that their competent authorities can rapidly, constructively, and effectively provide the widest range of international cooperation about money laundering, associated predicate offences, and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation.

Countries should authorize their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts.

Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritization and timely execution of requests, and for safeguarding the information received.

Note: **Interpretive Notes** to the FATF Recommendations are mentioned in The FATF Recommendations on "International Standard on Combating Money Laundering and the Financing of Terrorism & Proliferation" updated March 2022 – Page No: 31 to 115).

The FATF Recommendations 10,11,12,15,17, 18 to 23 apply to all Designated Non-Financial Businesses and Professions (DNFBPs).

In the case of Accountants, these Recommendations apply in the following situation.

1. Buying and selling of real estate
2. Managing of client money, securities or other assests
3. Management of bank, savings or securities accounts
4. Organisation of contribution for the creation, operation or management of companies, and
5. Creation, operation or management of legal persons or arrangements and
6. Buying and selling of business entities
7. Financial Transactions for or on behalf of client concerning all the other activities

The objectives of the FATF Recommendations as they relate to Accounting Professionals is consistent with their ethical obligation as professionals to avoid assisting criminals or facilitating criminal activity.

Risk Based Approach for the Accounting Profession shall, inter alia, include the following :

1. Meaning of Risk Based Approach
2. Risk Identification & Assessment
3. Risk Mitigation
4. Additional Requirements of Accounting Professionals
5. Suspicious Transactions Reporting
6. Ongoing Monitoring
7. Internal Controls and Governance

All above mentioned 7 points are explained as under :

1. Meaning of Risk Based Approach

Risk is defined as the possibility of some adverse event occurring and the likely consequences of the event.

The Risk Based Approach (RBA) to Anti Money Laundering / Countering the Financing of Terrorism (AML/CFT) is fundamental to the effective implementation of the FATF Recommendations.

It requires countries, competent authorities and DNFBPs, including Accountants, to implement a RBA to:

1) Identify the existence of risks the profession is exposed to ,
2) Undertake an assessment of the risks, and
3) Develop strategies to manage and mitigate the identified risks

2. Risk Identification and Assessment

Before establishing a client relationship or accepting an engagement, the Accounting Professionals must have controls in place to adderss the risks arising from this relationship.

During the initial onboarding process and throughout the relationship with each client, Accounting Professionals are required to perform AML/CFT and Know Your Customer (KYC) risk assessment to determine the client's overall ML / TF risk.

Risk Factors

ML / TF risk can be organised into 3 main categories but are not limited to those listed below.

The main common risk criteria for Accounting Professionals are as follows :

1. Customer
   - Customer Back Ground
   - AML System Check
   - Politically Exposed Person
   - Beneficial Owner Information
2. Country / Geographical
   - Country of Residence
   - Country of Incorporation
   - Country subjected to sanctions / embargoes
   - Country Identified to support terrorist organisations
3. Transaction / Services and Associated Delivery Demand
   - Financial and Tax Advise
   - Buying and Selling of Properties
   - Company and Trust Formation

Identifying these risk factors will assist in prescribing an appropriate risk rating.

The weight assigned to each of the categories (individually or in combination) to ascertain the overall risk rating of each client is based on the risk factors highlighted above.

The applied rating will determine the appropriate level of Customer Due Diligence (CDD) [whether normal, simplified or Enhanced Due Diligence (EDD)] and mitigation process that the accounting professional can adopt to reduce the compliance risk.

3. Risk Mitigation

DNFBPs including Accounting Professionals are exposed to vulnerabilities of ML / TF and proliferation of weapons of mass destruction and consequently being sanctioned.

Therefore, it is of utmost importance to and necessary to adopt preventive measures that will ensure effective mitigation.

These preventive measures shall, inter alia, include the following :

1) Customer Due Diligence

CDD is a KYC process of doing background checks/investigations on a customer to assess the risk he/she poses, before engaging in a business relationship.

Criminals often seek to mask their true identity by using complex and non-transparent ownership structures.

2) Enhanced Due Diligence (EDD)

EDD is a KYC process that provides a greater level of scrutiny of potential business partnership and highlights risk that cannot be detected by normal / simplified CDD.

EDD is therefore applicable for clients who are classified as high risk.

The FATF regards Politically Exposed Persons (PEPs), their immediate family members and close associate as high risk clients because their positions and affiliations are susceptible to potential abuse for ML / TF and are therefore subjected to the EDD process.

Accounting Professionals should apply simplified CDD measures for Low Risk Customers / Services / Industries.

Normal / Standard CDD should be applied for Medium Risk Customers / Countries / Services / Industries.

EDD should be applied for High Risk Customers / Countries / Services / Industries.

3) The following events should prompt the Accounting Professional to update CDD information

- A change in the client's identity
- A change in the beneficial ownership of the client
- A change in the services provided to the client
- A change in the geographic location or physical address
- A change in the client's sources of wealth

Information that is inconsistent with the business of the client

Significant change in the client's business activity (includes new operations in a new country)

Client appears on watch / sanction lists and

Suspicion or cause for concern (where doubt arises with the veracity of information provided, etc)

The above list is illustrative and not exhaustive

4) Additional Requirements of Accounting Professionals

In addition to CDD, Accountants are also required to comply with the following requirements.

- Record Keeping
- Procedure for the assessment of new products, business practices and technologies
- Reliance on Third Parties for conducting CDD procedures
- Reporting of Suspicious Transactions
- Internal Control Systems (screening procedures for employee, ongoing training programme and independent audit function)
- Compliance Management Systems (including the appointment of Compliance Officer (CO) at a management level)
- Business relationships and transactions emanating from high risk countries

Education, training and awareness of staff with respect to AML/CFT.

5) Reporting of Suspicious Transactions

FATF Recommendation 20 requires Accontants to take appropriate steps to identify any activity that is deemed to be suspicious.

If suspicious arises, this suspicion must be reported as soon as possible to the FIU.

This recommendation 20 also requires the Accountant to appoint a CO or a Money Lundering Reporting Officer (MLRO) who is tasked with the responsibility of reporting all suspicious activities by filing a Suspicious Transaction Report (STR).

The following are examples of suspicious activities which should be monitored by the Accounting Professionals.

1. The client does not show concern in incurring losses or realising extremely low profits in comparison with persons / entities in the same business.

   The client remains persistent in pursuing his / her activities.

2. High volume of foreign transfers from / to the client's account or the sudden increase of revenue and cash which is inconsistent with his / her usual income, without any justification.

3. Client's receipt of cash or high value cheques which are not consistent with his / her profession or the nature of his / her activity / business.

The transactions come from persons who are not clearly or justifiably connected to the client.

4) Unjustified amounts or deposits in the client's account whose origin or cause is difficult to identify.

4) Ongoing Monitoring

These pertain to FATF Recommendations 10 & 22 (CDD & DNFBP CDD)

Ongoing monitoring procedures involve regular review and analysis of client activities (including enquiries into sources of funds , if necessary) to make sure they are consistent with the client's operation and initial risk rating.

Ongoing monitoring of an existing business relationship should be carried out on a risk related basis, to ensure that the Accountants are aware of any changes in the client's identity and risk profile established at the onboarding stage / client acceptance.

The ongoing monitoring progress ensures that documentation and information collected are kept up to date and relevant by undergoing reviews of existing records.

5) Internal Controls and Compliance

This is in accordance with FATF Recommendations 18 & 23

To have an effective risk based approach, the Accounting Professionals should embed the risk based process within their internal controls.

These should encompass :

1. Establishing and maintaining policies and procedures to guide the firm.

   These should be approved by Senior Management or Board of Directors

2. Developing, delivering and maintaining a training programme for employees

3. Provide regular review of the Risk Assessment and Management process and

4) Designate a Compliance Officer and implement a compliance programme.

Guidance for a Risk-based Approach for the Accounting Profession

18.2

(Note: Sl. No.60 to Sl. No.209 of Guidance for a Risk-Based Approach – Accounting Profession of FATF document (2019) deals with Guidance for a Risk-Based Approach for Accounting Profession – Refer FATF Document for detailed REGULATIONS).

Acronyms:

AML/CFT: Anti-money laundering/Countering the financing of terrorism

CDD: Client due diligence

DNFBP: Designated non-financial businesses and professions

FATF: Financial Action Task Force

FIU: Financial intelligence unit

INR: Interpretive Note to Recommendation

ML: Money laundering

NRA: National Risk Assessment

PEP: Politically Exposed Person

R: Recommendation

RBA: Risk-based approach

SRB: Self-regulatory body

STR: Suspicious transaction report

TCSP: Trust and company service providers

TF: Terrorist financing

Risk identification and assessment:

60. Accountants should take appropriate steps to identify and assess the risk firmwide, given their particular client base, that they could be used for ML/TF. This is usually performed as part of the overall client and engagement acceptance processes. They should document those assessments, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and supervisors. The nature and extent of any assessment of ML/TF risks should be appropriate to the type of business, nature of clients, and size of operations.

61. ML/TF risks can be organized into three categories: (a) country/geographic risk, (b) client risk, and (c) transaction/service and associated delivery channel risk. The risks and red flags listed in each category are not exhaustive but provide a starting point for accountants to use when designing their RBA.

62. When assessing risk, accountants should consider all the relevant risk factors before determining the level of overall risk and the appropriate level of mitigation to be applied. Such risk assessment may well be informed by findings of the NRA, the supranational risk assessments, sectoral reports conducted by competent authorities on ML/TF risks that are inherent in the accounting services/sector, risk reports in other jurisdictions where the accountant is based in, and any other information which may be relevant to assess the risk level particular to their practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions. Accountants may well also draw references to FATF Guidance on indicators and risk factors. During a client relationship, procedures for ongoing monitoring and review of the client's risk profile are also important. Competent authorities should consider how they can best alert accountants to the findings of any national risk assessments, supranational risk assessments, and any other information which may be relevant to assessing the risk level particular to accounting practice in the relevant country.

63. Due to the nature of services that an accountant generally provides, automated transaction monitoring systems of the type used by financial institutions will not be appropriate for most accountants. There may be some scope to use artificial intelligence and analytical tools in an audit context to spot unusual transactions. The accountant's knowledge of the client and its business will develop throughout a longer-term and interactive professional relationship (in some cases, such relationships may exist for short-term clients as well, e.g., for property transactions). However, although individual accountants are not expected to investigate their client's affairs, they may be well-positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of the business relationships. Accountants will also need to consider the nature of the risks presented by short-term client relationships that may inherently, but not necessarily be low risk (e.g., one-off client relationship). Accountants should also be mindful of the subject matter of the professional services (the engagement) being sought by an existing or potential client and the related risks.

64. Identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow accountants to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the accountant's role and involvement. Circumstances may vary considerably between professionals who represent clients on a single transaction and those involved in a long-term advisory relationship.

65. The amount and degree of ongoing monitoring and review will depend on the nature and frequency of the relationship, along with the comprehensive assessment of client/transactional risk. An accountant may also have to adjust the risk assessment of a particular client based upon information received from a designated competent authority, SRB, or other credible sources (including a referring accountant).

66. Accountants may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling accountants, where required, to subject each client to reasonable and proportionate risk assessment.

67. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature, and scope of services provided by the accountant and/or firm. These criteria, however, should be considered holistically and not in isolation. Accountants, based on their practices and reasonable judgments, will need to independently assess the weight to be given to each risk factor.

68. Although there is no universally accepted set of risk categories, the examples provided in this Guidance are the most commonly identified risk categories. There is no single methodology to apply these risk categories, and the application of these risk categories is intended to provide a suggested framework for approaching the assessment

and management of potential ML/TF risks. For smaller firms and sole practitioners, it is advisable to look at the services they offer (e.g., providing company management services may entail greater risk than other services).

69. Criminals use a range of techniques and mechanisms to obscure the beneficial ownership of assets and transactions. Many of the common mechanisms/techniques have been compiled by FATF in previous studies, including the 2014 FATF Guidance on Transparency and Beneficial Ownership and the 2018 Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership. Accountants may refer to the studies for more details on the use of obscuring techniques and relevant case studies.

70. A practical starting point for accounting firms (especially smaller firms) and accountants (especially sole practitioners) would be to take the following approach. Many of these elements are critical to satisfying other obligations owed to clients, such as fiduciary duties, and as part of their general regulatory obligations:

(a) Client acceptance and know your client policies: Identify the client (and its beneficial owners where appropriate) and the true "beneficiaries" of the transaction. Obtain an understanding of the source of funds and source of wealth (The source of funds and the source of wealth are relevant to determining a client's risk profile). The source of funds is the activity that generates the funds for a client (e.g., salary, trading revenues, or payments out of a trust), while the source of wealth describes the activities that have generated the total net worth of a client (e.g., ownership of a business, inheritance, or investments). While these may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption, or misuse of position. Under the RBA, accountants should satisfy themselves that adequate information is available to assess a client's source of funds and source of wealth as legitimate with a degree of certainty that is proportionate to the risk profile of the client, where required, its owners, and the purpose of the transaction.

(b) Engagement acceptance policies: Understand the nature of the work. Accountants should know the exact nature of the service that they are providing and have an understanding of how that work could facilitate the movement or obscure the proceeds of crime. Where an accountant does not have the requisite expertise, the accountant should not undertake the work.

(c) Understand the commercial or personal rationale for the work: Accountants need to be reasonably satisfied that there is a commercial or personal rationale for the work undertaken. Accountants however are not obliged to objectively assess the commercial or personal rationale if it appears reasonable and genuine.

(d) Be attentive to red-flag indicators: Exercise vigilance in identifying and then carefully reviewing aspects of the transaction if there are reasonable grounds to suspect that funds are the proceeds of criminal activity, or related to terrorist financing. These cases would trigger reporting obligations. Documenting the thought process by having an action plan may be a viable option to assist in interpreting/assessing red flags/indicators of suspicion.

(e) Then consider what action if any, needs to be taken.

(f) The outcomes of the above action (i.e., the comprehensive risk assessment of a particular client/transaction) will dictate the level and nature of the evidence/documentation collated under a firm's CDD/EDD procedures (including evidence of source of wealth or funds).

(g) Accountants should adequately document and record steps taken under (a) to (e).

Country/Geographic risk:

71. A client may be at higher risk when features of their business are connected to a higher risk country as regards:

(a) the origin or current location of the source of wealth or funds;

(b) where the services are provided;

(c) the client's country of incorporation or domicile;

(d) the location of the client's major operations;

(e) the beneficial owner's country of domicile; or

(f) target company's country of incorporation and location of major operations (for potential acquisitions).

72. There is no universally agreed definition of a higher risk country or geographic area but accountants should pay attention to those countries that are:

(a) Countries/areas identified by credible sources ("Credible sources" refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank, and the Egmont Group of Financial Intelligence Units.) as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

(b) Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking, smuggling, and illegal gambling.

(c) Countries subject to sanctions, embargoes, or similar measures issued by international organisations such as the United Nations.

(d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, about which financial institutions (as well as DNFBPs) should give special attention to business relationships and transactions.

(e) Countries identified by credible sources to be uncooperative in providing beneficial ownership information to competent authorities, a determination of which may be established from reviewing FATF mutual evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards.

Client Risk:

73. The key risk factors that accountants should consider are:

(a) The firm's client base includes industries or sectors where opportunities for ML/TF are particularly prevalent.

(b) The firm's clients include PEPs or persons closely associated with or related to PEPs, who are considered higher risk clients (Please refer to the FATF Guidance (2013) on politically-exposed persons for further guidance on how to identify PEPs).

Box 2

Particular considerations for PEPs and source of funds and wealth: If an accountant is advising a PEP client, or where a PEP is the beneficial owner of assets in a transaction, appropriate enhanced CDD is required if a specified activity under R.22 is involved. Such measures include obtaining senior management (e.g., senior partner, managing partner, or CEO) approval before establishing a business relationship, taking reasonable measures to establish the source of wealth and source of funds of clients and beneficial owners identified as PEPs, and conducting enhanced ongoing monitoring on that relationship.

The source of funds and the source of wealth are relevant to determining a client's risk profile. The source of funds is the activity that generates the funds for a client (e.g., salary, trading revenues, or payments out of a trust). The Source of funds relates directly to the literal origin of funds to be used in a transaction. This is likely to be a bank account. Generally, this would be evidenced by bank statements or similar. Source of

wealth describes the activities that have generated the total net worth of a client (e.g., ownership of a business, inheritance, or investments). The Source of wealth is the origin of the accrued body of wealth of an individual. Understanding the source of wealth is about taking reasonable steps to be satisfied that the funds to be used in a transaction are not the proceeds of crime.

While the source of funds and wealth may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption, or misuse of position. Under the RBA, accountants should satisfy themselves that adequate information is available to assess a client's source of funds and source of wealth as legitimate with a degree of certainty that is proportionate to the risk profile of the client.

Relevant factors that influence the extent and nature of CDD include the particular circumstances of a PEP, PEPs separate business interests and the time those interests prevailed about the public position, whether the PEP has access to official funds, makes decisions regarding the allocation of public funds or public procurement contracts, the PEP's home country, the type of activity that the PEP is instructing the accountant to perform, whether the PEP is domestic or international, particularly having regard to the services asked for, and the scrutiny to which the PEP is under in the PEP's home country.

(c) Clients conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated taking into account all the circumstances of the client's representation).

(d) Clients where the structure or nature of the entity or relationship makes it difficult to identify promptly the true beneficial owner or controlling interests or clients attempting to obscure understanding of their business, ownership, or the nature of their transactions, such as:

(i) Unexplained use of shell and/or shelf companies, front company, legal entities with ownership through nominee shares or bearer shares, control through nominee and corporate directors, legal persons or legal arrangements, splitting company incorporation and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason.

(ii) Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors.

(iii) Unusual complexity in control or ownership structures without a clear explanation, where certain circumstances, structures, geographical locations, international activities, or other factors are not consistent with the accountants' understanding of the client's business and economic purpose.

(e) Client companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose a higher geographic risk.

(f) Clients that are cash (and/or cash equivalent) intensive businesses. Where such clients are themselves subject to and regulated for a full range of AML/CFT requirements consistent with the FATF Recommendations, this will aid to mitigate the risks. These may include, for example:

(i) Money or Value Transfer Services (MVTS) businesses (e.g., remittance houses, currency exchange houses, Casas de Cambio, Centro's cambia Rios, remisores de Fondos, bureaux de change, money transfer agents and banknote traders, or other businesses offering money transfer facilities);

(ii) Operators, brokers, and others providing services in virtual assets;

(iii) Casinos, betting houses, and other gambling-related institutions and activities;

(iv) Dealers in precious metals and stones.

(g) Businesses that while not normally cash-intensive appear to have substantial amounts of cash.

(h) Non-profit or charitable organisations engaging in transactions for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

(i) Clients using financial intermediaries, financial institutions, or DNFBPs that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities or SRBs.

(j) Clients who appear to be acting on somebody else's instructions without disclosure.

(k) Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons and are otherwise evasive or very difficult to reach when this would not normally be expected.

(l) Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for the accountants to perform a proper risk assessment.

(m) Clients with previous convictions for crimes that generated proceeds, who instruct accountants (who in turn know such convictions) to undertake specified activities on their behalf.

(n) Clients who have no address, or multiple addresses without legitimate reasons.

(o) Clients who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g., their age, income, occupation, or wealth).

(p) Clients who change their settlement or execution instructions without appropriate explanation.

(q) Clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is an unexplained lack of information or transparency in the transaction. This risk extends to situations where last-minute changes are made to enable funds to be paid in from/out to a third party.

(r) Clients who insist, without adequate justification or explanation, that transactions be effected exclusively or mainly through the use of virtual assets to preserve their anonymity.

(s) Clients who offer to pay unusually high levels of fees for services that would not ordinarily warrant such a premium. However, bona fide and appropriate contingency fee arrangements, where accountants may receive a significant premium for a successful provision of their services, should not be considered a risk factor.

(t) Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such.

(u) Where there are certain transactions, structures, geographical location, international activities, or other factors that are not consistent with the accountants' understanding of the client's business or economic situation.

(v) The accountants' client base includes industries or sectors where opportunities for ML/TF are particularly prevalent.

(w) Clients who are suspected to be engaged in falsifying activities through the use of false loans, false invoices, and misleading naming conventions.

(x) The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination poses a risk of the creation of shell companies that might be used to obscure beneficial ownership.

(y) The relationship between employee numbers/structure and the nature of the business is divergent from the industry norm (e.g., the turnover of a company is unreasonably high considering the number of employees and assets used compared to similar businesses).

(z) Sudden activity from a previously dormant client without any clear explanation.

(aa) Clients that start or develop an enterprise with an unexpected profile of abnormal business cycles or clients that enter into new/emerging markets. Organized criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash-intensive.

(ab) Indicators that the client does not wish to obtain necessary governmental approvals/filings, etc.

(ac) Reason for the client choosing the accountant is unclear, given the firm's size, location, or specialization.

(ad) Frequent or unexplained change of client's professional adviser(s) or members of management.

(ae) Client is reluctant to provide all the relevant information or accountants have reasonable grounds to suspect that the information provided is incorrect or insufficient.

(af) Clients seeking to obtain residents' rights or citizenship in the country of establishment of the accountants in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities.

74. The clients referred to above may be individuals that are, for example, trying to obscure their business interests and assets or the clients may be representatives of a company's senior management who are, for example, trying to obscure the ownership structure.

Transaction/Service and associated delivery channel risk

75. Services that may be provided by accountants and which (in some circumstances) risk being used to assist money launderers may include:

(a) Use of pooled client accounts or safe custody of client money or assets without justification.

(b) Situations where advice on the setting up of legal arrangements may be misused to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seat, or establishing complex group structures). This might include advising about a discretionary trust that gives the trustee discretionary power to name a class of beneficiaries that does not include the real beneficiary (e.g. naming a charity as the sole discretionary beneficiary initially to add the real beneficiaries at a later stage). It might also include situations where a trust is set up to manage shares in a company to make it more difficult to determine the beneficiaries of assets managed by the trust.

(c) In the case of an express trust, and unexplained (where an explanation is warranted) nature of classes of beneficiaries and acting as trustees of such a trust.

(d) Services where accountants may in practice represent or assure the client's standing, reputation, and credibility to third parties, without a commensurate knowledge of the client's affairs.

(e) Services that are capable of concealing beneficial ownership from competent authorities.

(f) Services requested by the client for which the accountant does not have expertise except where the accountant is referring the request to an appropriately trained professional for advice.

(g) Non-cash wire transfers through the use of many inter-company transfers within the group to disguise the audit trail.

(h) Services that rely heavily on new technologies (e.g., initial coin offerings or virtual assets) that may have

inherent vulnerabilities to exploitation by criminals, especially those not regulated for AML/CFT.

(i) Transfer of real estate or other high-value goods or assets between parties in a period that is unusually short for similar transactions with no apparent legal, tax, business, economic, or other legitimate reason.

(j) Transactions where it is readily apparent to the accountant that there is inadequate consideration, where the client does not provide legitimate reasons for the transaction.

(k) Administrative arrangements concerning estates where the deceased was known to the accountant as being a person who had been convicted of proceeds generating crimes.

(l) Services that have deliberately provided or depend upon, more anonymity about the client's identity or regarding other participants than is normal under the circumstances and in the experience of the accountant.

(m) Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic, or other legitimate reason.

(n) Transactions using unusual means of payment (e.g., precious metals or stones).

(o) The postponement of a payment for an asset or service delivered immediately to date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made.

(p) Unexplained establishment of unusual conditions/clauses in credit arrangements that do not reflect the commercial position between the parties and may require accountants to be aware of risks. Arrangements that may be abused in this way might include unusually short/long amortization periods, interest rates materially above/below market rates, or unexplained repeated cancellations of promissory notes/mortgages or other security instruments substantially ahead of the maturity date initially agreed.

(q) Transfers of goods that are inherently difficult to value (e.g., jewels, precious stones, objects of art or antiques, virtual assets), where this is not common for the type of clients, transaction, or with accountant's normal course of business such as a transfer to a corporate entity, or generally without any appropriate explanation.

(r) Successive capital or other contributions in a short period to the same company with no apparent legal, tax, business, economic, or other legitimate reason.

(s) Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic, or other legitimate reason.

(t) Power of representation given in unusual conditions (e.g., when it is granted irrevocably or about specific assets) and the stated reasons for these conditions are unclear or illogical.

(u) Transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic, or other legitimate reasons.

(v) Situations where a nominee is being used (e.g., friend or family member is named as the owner of property/ assets where it is clear that the friend or family member is receiving instructions from the beneficial owner) with no apparent legal, tax, business, economic or other legitimate reason.

(w) Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

(x) Commercial, private, or real property transactions or services to be carried out by the client with no apparent legitimate business, economic, tax, family governance, or legal reasons.

(y) Existence of suspicions regarding fraudulent transactions, or transactions that are improperly accounted for.

These might include:

(i) Over or under-invoicing of goods/services.

(ii) Multiple invoicing of the same goods/services.

(iii) Falsely described goods/services – over or under shipments (e.g. false entries on bills of lading).

(iv) Multiple trading of goods/services.

76. About the areas of risk identified above, accountants may also consider the examples of fraud risk factors listed in International Standard of Auditing 240: The auditor's responsibilities relating to fraud in an audit of financial statements (ISA 240) and the examples of conditions and events that may indicate risks of material misstatement in International Standard of Auditing 315: Identifying and assessing risks of material misstatement through understanding the entity and its environment (ISA315). Even where the accountant is not performing an audit, ISA 240 and ISA 315 provide helpful lists of additional red flags.

Variables that may impact an RBA and risk

77. While all accountants should follow robust standards of due diligence to avoid regulator arbitrage, due regard should be accorded to differences in practices, size, scale, and expertise amongst accountants, as well as the nature of the clients they serve. As a result, consideration should be given to these factors when creating an RBA that complies with the existing obligations of accountants.

78. Consideration should also be given to the resources that can be reasonably allocated to implement and manage an appropriately developed RBA. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large firm; rather, the sole practitioner would be expected to develop appropriate systems and controls and an RBA proportionate to the scope and nature of the practitioner's practice and its clients. Small firms serving predominantly locally based and low-risk clients cannot generally be expected to devote a significant amount of senior personnel's time to conducting risk assessments. In such cases, it may be more reasonable for sole practitioners to rely on publicly available records and information supplied by a client for a risk assessment than it would be for a large firm having a diverse client base with different risk profiles. However, where the source is a public registry or the client, there is always a potential risk in the correctness of the information. Sole practitioners and small firms may be regarded by criminals as more of a target for money launderers than large law firms. Accountants in many jurisdictions and practices are required to conduct both a risk assessment of the general risks of their practice and all new clients and current clients engaged in one-off specific transactions. The emphasis must be on following an RBA.

79. A significant factor to consider is whether the client and proposed work would be unusual, risky, or suspicious for the particular accountant. This factor must always be considered in the context of the accountant's practice, as well as the legal, professional, and ethical obligations in the jurisdiction(s) of practice. An accountant's RBA methodology may thus take account of risk variables specific to a particular client or type of work. Consistent with the RBA and proportionality, the presence of one or more of these variables may cause an accountant to conclude that either enhanced CDD and monitoring are warranted, or conversely that standard CDD and monitoring can be reduced, modified, or simplified. When reducing, modifying, or simplifying CDD, accountants should always adhere to the minimum requirements as set out in national legislation. These variables may increase or decrease the perceived risk posed by a particular client or type of work. While the presence of the specific factors referred to in paragraphs 71-76 may tend to increase risk, more general client/ engagement-related variables may add to or mitigate that risk.

80. Examples of factors that may increase risk are:

(a) Unexplained urgency of assistance required.

(b) Unusual sophistication of client, including the complexity of control environment.

(c) Unusual sophistication of transaction/scheme.

(d) The irregularity or duration of the client relationship. One-off engagements involving limited client contact throughout the relationship may present a higher risk.

81. Examples of factors that may decrease risk are:

(a) Involvement of adequately regulated financial institutions or other DNFBP professionals.

(b) Similar country location of accountants and clients.

(c) Role or oversight of a regulator or multiple regulators.

(d) The regularity or duration of the client relationship. Long-standing relationships involving frequent client contact and easy flow of information throughout the relationship may present less risk.

(e) Private companies that are transparent and well-known in the public domain.

(f) Accountant's familiarity with a particular country, including knowledge of and compliance with local laws and regulations as well as the structure and extent of regulatory oversight.

Documentation of risk assessments:

82. Accountants must always understand their ML/TF risks (for clients, countries, geographic areas, services, transactions, or delivery channels). They should document those assessments to be able to demonstrate their basis and exercise due professional care and use compelling good judgment. However, competent authorities or SRBs may determine that individual documented risk assessments are not required if the specific risks inherent to the sector are identified and understood.

83. Accountants may fail to satisfy their AML/CFT obligations, for example by relying completely on a checklist risk assessment where there are other clear indicators of potential illicit activity. Completing risk assessments in a time-efficient yet comprehensive manner has become more important.

84. Each of these risks could be assessed using indicators such as low risk, medium risk, and/or high risk. A short explanation of the reasons for each attribution should be included and an overall assessment of risk determined. An action plan (if required) should then be outlined to accompany the assessment and dated. In assessing the risk profile of the client at this stage, reference must be made to the relevant targeted financial sanctions lists to confirm that neither the client nor the beneficial owner is designated and included in any of them.

85. A risk assessment of this kind should not only be carried out for each specific client and service on an individual basis, but also to assess and document the risks on a firm-wide basis, and to keep risk assessment up-to-date through monitoring of the client relationship. The written risk assessment should be made accessible to all professionals having to perform AML/CFT duties.

Risk mitigation:

86. Accountants should have policies, controls, and procedures that enable them to effectively manage and mitigate the risks that they have identified (or that have been identified by the country). They should monitor the implementation of those controls and enhance or improve them if they find the controls to be weak or ineffective. The policies, controls, and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with

guidance from competent authorities and supervisors. Measures and controls may include:

(a) General training on ML/TF methods and risks relevant to accountants.

(b) Targeted training for increased awareness by the accountants providing specified activities to higher risk clients or accountants undertaking higher risk work.

(c) Increased or more appropriately targeted CDD or enhanced CDD for higher risk clients/situations that concentrate on providing a better understanding of the potential source of risk and obtaining the necessary information to make informed decisions about how to proceed (if the transaction/ business relationship can be proceeded with). This could include training on when and how to ascertain, evidence, and record source of wealth and beneficial ownership information if required.

(d) Periodic review of the services offered by the accountant, and the periodic evaluation of the AML/CFT framework applicable to the accountant and the accountant's own AML/CFT procedures, to determine whether the ML/TF risk has increased.

(e) Review client relationships from time to time to determine whether the ML/TF risk has increased.

Initial and ongoing CDD (R.10 and 22):

87. Accountants should design CDD procedures to enable them to establish with reasonable certainty the true identity of each client and, with an appropriate degree of confidence, know the types of business and transactions the client is likely to undertake. Accountants should have procedures to:

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

(b) Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner, such that accountants are satisfied that they know who the beneficial owner is. This should include accountants' understanding of the ownership and control structure of the client. This is articulated in the following box.

Box 3. Beneficial ownership information obligations (see R.10, R.22, and INR.10)

R.10 sets out the instances where accountants will be required to take steps to identify and verify beneficial owners, including when there is a suspicion of ML/TF when establishing business relations, or where there are doubts about the veracity of previously provided information. INR.10 indicates that the purpose of this requirement is two-fold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess the potential ML/TF risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. Accountants should have regard to these purposes when assessing what steps are reasonable to take to verify beneficial ownership, commensurate with the level of risk. Accountants should also have regard to the AML/CFT 2013 Methodology Criteria 10.5 and 10.8-10.12.

At the outset of determining beneficial ownership, steps should be taken to identify how the immediate client can be identified. Accountants can verify the identity of a client by, for example meeting the client in person and then verifying their identity through the production of a passport/identity card and documentation confirming his/her address. Accountants can further verify the identity of a client based on documentation or information obtained from reliable, publicly available sources (which are independent of the client).

A more difficult situation arises where there is a beneficial owner who is not the immediate client (e.g., in the case of companies and other entities). In such a scenario reasonable steps must be taken so that the accountant is satisfied with the identity of the beneficial owner and takes reasonable measures to verify the beneficial owner's identity. This likely requires taking steps to understand the ownership and control of a separate legal

entity that is the client and may include conducting public searches as well as seeking information directly from the client.

Accountants will likely need to obtain the following information for a client that is a legal entity:

(a) the name of the company;

(b) the company registration number;

(c) the registered address and/ or principal place of business (if different);

(d) the identity of shareholders and their percentage ownership;

(e) names of the board of directors or senior individuals responsible for the company's operations;

(f) the law to which the company is subject and its constitution; and

(g) the types of activities and transactions in which the company engages.

To verify the information listed above, accountants may use sources such as the following:

(a) constitutional documents (such as a certificate of incorporation, memorandum, and articles of incorporation/ association);

(b) details from company registers;

(c) shareholder agreements or other agreements between shareholders concerning control of the legal person; and

(d) filed audited accounts.

Accountants should adopt an RBA to verify the beneficial owners of an entity. It is often necessary to use a combination of public sources and to seek further confirmation from the immediate client that information from public sources is correct and up-to-date or to ask for additional documentation that confirms the beneficial ownership and company structure. The obligation to identify beneficial ownership does not end with identifying the first level of ownership but requires reasonable steps to be taken to identify the beneficial ownership at each level of the corporate structure until an ultimate beneficial owner is identified.

(c) Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

(d) Conduct ongoing due diligence on the business relationship. Ongoing due diligence ensures that the documents, data, or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of clients. Undertaking appropriate CDD may also facilitate the accurate filing of suspicious transaction reports (STRs) to the financial intelligence unit (FIU), or to respond to requests for information from an FIU and law enforcement agencies.

88. Accountants should design their policies and procedures so that the level of client due diligence addresses the risk of being used for ML/TF by the client. By the national AML/CFT framework, accountants should design a 'standard' level of CDD for normal risk clients and a reduced or simplified CDD process for low-risk clients. Simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF or where specific higher-risk scenarios apply. Enhanced due diligence should be applied to those clients that are assessed as high risk. These activities may be carried out in conjunction with firms' normal client acceptance procedures and should take account of any specific jurisdictional requirements for CDD.

89. In the normal course of their work, accountants are likely to learn more about some aspects of their client, such as their client's business or occupation and/or their level and source of income, than other advisors. This

information is likely to help them reassess the ML/TF risk.

90. An RBA means that accountants should perform varying levels of work according to the risk level. For example, where the client or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, and that information is publicly available, fewer checks may be appropriate. In the case of trusts, foundations, or similar legal entities where the beneficiaries are distinct from the legal owners of the entity, it will be necessary to form a reasonable level of knowledge and understanding of the classes and nature of the beneficiaries; the identities of the settlor, trustees or natural persons exercising effective control; and an indication of the purpose of the trust. Accountants will need to obtain a reasonable level of comfort that the declared purpose of the trust is its true purpose.

91. Changes in ownership or control of clients should lead to review or repeat of client identification and verification procedures. This may be carried out in conjunction with any professional requirements for client continuation processes.

92. Public information sources may assist with this ongoing review (scrutinizing transactions undertaken throughout that relationship). The procedures that need to be carried out can vary, by the nature and purpose for which the entity exists, and the extent to which the underlying ownership differs from apparent ownership by the use of nominees and complex structures.

93. The following box provides a non-exhaustive list of examples of standard, enhanced, and simplified CDD:

Box 4. Examples of Standard/Simplified/Enhanced CDD measures (see also INR.10)

Standard CDD

- Identifying the client and verifying that client's identity using reliable, independent source documents, data, or information
- Identifying the beneficial owner, and taking reasonable measures on a risk-sensitive basis to verify the identity of the beneficial owner, such that the accountant is satisfied with the identity of the beneficial owner. For legal persons and arrangements, this should include understanding the ownership and control structure of the client and gaining an understanding of the client's source of wealth and source of funds, where required
- Understanding and obtaining information on the purpose and intended nature of the business relationship
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout that relationship to ensure that the transactions being conducted are consistent with the business and risk profile of the client, including, where necessary, the source of wealth and funds

Simplified CDD

- Limiting the extent, type, or timing of CDD measures
- Obtaining fewer elements of client identification data
- Altering the type of verification carried out on the client's identity
- Simplifying the verification carried out on the client's identity
- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established
- Verifying the identity of the client and the beneficial owner after the establishment of the business relationship

- Reducing the frequency of client identification updates in the case of a business relationship
- Reducing the degree and extent of ongoing monitoring and scrutiny of transactions

Enhanced CDD

- Obtaining additional information on the client (e.g., occupation, the volume of assets, information available through public databases, the internet, etc.), and updating more regularly the identification data of the client and beneficial owner
- Carrying out additional searches (e.g., internet searches using independent and open sources) to better inform the client risk profile (provided that the internal policies of accountants should enable them to disregard source documents, data, or information, which is perceived to be unreliable)
- Obtaining additional information and, as appropriate, substantiating documentation, on the intended nature of the business relationship
- Obtaining information on the source of funds and/or source of wealth of the client and evidencing this through appropriate documentation obtained
- Obtaining information on the reasons for intended or performed transactions
- Obtaining the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards
- Increasing awareness of higher risk clients and transactions, across all departments with a business relationship with the client, including the possibility of the enhanced briefing of engagement teams responsible for the client.
- Enhanced CDD may also include lowering the threshold of ownership (e.g., below 25%), to ensure a complete understanding of the control structure of the entity involved. It may also include looking further than simply holdings of equity shares, to understand the voting rights of each party who holds an interest in the entity.

Politically exposed persons (PEP) (R.12 and R.22):

94. Accountants should take reasonable measures to identify whether a client is a PEP or a family member or close associate of a PEP. Accountants should also refer to the 2013 FATF Guidance on politically-exposed persons for further guidance on how to identify PEPs.

95. If the client or the beneficial owner is a PEP or a family member or close associate of a PEP, accountants should perform the following additional procedures:

(a) obtain senior management approval for establishing (or continuing, for existing clients) such business relationships;

(b) take reasonable measures to establish the source of wealth and source of funds; and

(c) conduct enhanced ongoing monitoring of the business relationship.

96. Relevant factors that will influence the extent and nature of CDD include the particular circumstances of a PEP, the PEP's role in a particular government/ government agency, whether the PEP has access to official funds, the PEP's home country, the type of work the PEP is instructing the accountant to perform or carry out (i.e. the services that are being asked for), whether the PEP is domestically based or international, particularly having regard to the services asked for, and the scrutiny to which the PEP is under in the PEP's home country.

97. The nature of the risk should be considered in light of all relevant circumstances, such as:

(a) The nature of the relationship between the client and the PEP. If the client is a trust, company, or legal entity, even if the PEP is not a natural person exercising effective control or the PEP is merely a discretionary beneficiary who has not received any distributions, the PEP may nonetheless affect the risk assessment.

(b) The nature of the client (e.g., where it is a public listed company or regulated entity which is subject to and regulated for a full range of AML/CFT requirements consistent with FATF recommendations, the fact that it is subject to reporting obligations will be a relevant factor, albeit this should not automatically qualify the client for simplified CDD).

(c) The nature of the services sought. For example, lower risks may exist where a PEP is not the client but a director of a client that is a public listed company or regulated entity and the client is purchasing property for adequate consideration.

Ongoing monitoring of clients and specified activities (R.10 and 22):

98. Accountants are not expected to scrutinize every transaction that goes through their clients' books and some accounting services are provided only on a one-off basis, without a continuing relationship with the client and without the accountant having access to the client's books and/or bank records. However, many of the professional services provided by accountants put them in a relatively good position to encounter and recognize suspicious activities (or transactions) carried out by their clients through their inside knowledge of, and access, to the client's records and management processes, and operations, as well as through close working relationships with senior managers and owners. The continued administration and management of the legal persons and arrangements (e.g. account reporting, asset disbursements, and corporate filings) would also enable the relevant accountants to develop a better understanding of the activities of their clients.

99. Accountants need to be alert for events or situations which are indicative of a reason to be suspicious of ML/TF, employing their professional experience and judgment in the forming of suspicions where appropriate. An advantage in carrying out this function is professional scepticism which is a defining characteristic of many professional accountancy functions and relationships.

100. Ongoing monitoring of the business relationship should be carried out on a risk-related basis, to ensure that accountants are aware of any changes in the client's identity and risk profile established at client acceptance. This requires an appropriate level of scrutiny of activity during the relationship, including an inquiry into the source of funds where necessary, to judge consistency with expected behaviour based on accumulated CDD information. As discussed below, ongoing monitoring may also give rise to filing an STR.

101. Accountants should also consider reassessing CDD on an engagement/assignment basis for each client. Well-known, reputable, long-standing clients may suddenly request a new type of service that is not in line with the previous relationship between the client and accountant. Such an assignment may suggest a greater level of risk.

102. Accountants should not conduct investigations into suspected ML/TF on their own but instead file an STR or if the behaviour is egregious, they should contact the FIU or law enforcement or supervisors, as appropriate, for guidance. Within the scope of engagement, an accountant should be mindful of the prohibition of "tipping off" the client where suspicion has been formed. Carrying out additional investigations, which are not within the scope of the engagement should also be considered against the risk of alerting a money launderer.

103. When deciding whether or not an activity or transaction is suspicious, accountants may need to make additional inquiries (within the normal scope of the assignment or business relationship) of the client or their records this could typically be done as part of the accountant's CDD process. Normal commercial inquiries, being made to fulfil duties to clients, may assist in understanding an activity or transaction to determine whether or not it is suspicious.

Suspicious activity/transaction reporting, tipping-off, internal controls, and higher-risk countries (R.23)

104. R.23 sets out obligations for accountants on reporting and tipping-off, internal controls, and higher-risk countries as set out in R.20, R.21, R.18, and R.19.

Suspicious transaction reporting and tipping-off (R.20, 21, and 23) 105.

105. R.23 requires accountants to report suspicious transactions set out in R.20. Where a legal or regulatory requirement mandates the reporting of suspicious activity once suspicion has been formed, a report must always be made promptly. The requirement to file an STR is not subject to an RBA but must be made whenever required in the country concerned.

106. Accountants may be required to report suspicious activities, as well as specific suspicious transactions, and so may make reports on several scenarios including suspicious business structures or management profiles that have no legitimate economic rationale and suspicious transactions, such as the misappropriation of funds, false invoicing or company purchase of goods unrelated to the company's business. As specified under INR.23, where accountants seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

107. However, it should be noted that an RBA is appropriate for identifying a suspicious activity or transaction, by directing additional resources at those areas that have been identified as higher risk. The designated competent authorities or SRBs may provide information to accountants, which can inform their approach to identifying suspicious activity or transactions, as part of an RBA. The accountant should also periodically assess the adequacy of their system for identifying and reporting suspicious activity or transactions.

108. Accountants should review CDD if they have a suspicion of ML/TF.

Internal controls and compliance (R.18 and 23)

109. For accountants to have effective RBA, the risk-based process must be embedded within the internal controls of the firm and they must be appropriate for the size and complexity of the firm.

Internal controls and governance

110. Strong leadership and engagement by senior management and the Board of Directors (or equivalent body) in AML/CFT is an important aspect of the application of the RBA. Senior management must create a culture of compliance, ensuring that staff adheres to the firm's policies, procedures, and processes designed to limit and control risks.

111. The nature and extent of the AML/CFT controls, as well as meeting national legal requirements, need to be proportionate to the risk involved in the services being offered. In addition to other compliance internal controls, the nature and extent of AML/CFT controls will encompass several aspects, such as:

1. designating an individual or individuals, at the management level responsible for managing AML/CFT compliance;
2. designing policies and procedures that focus resources on the firm's higher risk, services, products, clients, and geographic locations in which their clients/they operate, and include risk-based CDD policies, procedures, and processes;
3. ensuring that adequate controls are in place before new services are offered; and
4. ensuring adequate controls for accepting higher-risk clients or providing higher-risk services, such as management approval.

112. These policies and procedures should be implemented across the firm and include:

(a) performing a regular review of the firm's policies and procedures to ensure that they remain fit for purpose;

(b) performing a regular compliance review to check that staff are properly implementing the firm's policies and procedures;

(c) providing senior management with a regular report of compliance initiatives, identifying compliance deficiencies, corrective action is taken, and STRs filed;

(d) planning for changes in management, staff, or firm structure so that there is compliance continuity;

(e) focusing on meeting all regulatory record-keeping and reporting requirements, recommendations for AML/CFT compliance, and providing timely updates in response to changes in regulations;

(f) enabling the timely identification of reportable transactions and ensuring accurate filing of required reports;

(g) incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel;

(h) providing for appropriate training to be given to all relevant staff;

(i) having appropriate risk management systems to determine whether a client, potential client or beneficial owner is a PEP or a person subject to applicable financial sanctions;

(j) providing for adequate controls for higher risk clients and services, as necessary (e.g. additional due diligence, evidencing the source of wealth and funds of a client and escalation to senior management, or additional review and/or consultation);

(k) providing increased focus on the accountant/accounting firm's operations (e.g. services, clients, and geographic locations) that are more vulnerable to abuse for ML/TF;

(l) providing for periodic review of the risk assessment and management processes, taking into account the environment within which the accountant/accounting firm operates and the services it provides; and

(m) providing for an AML/CFT compliance function and review program, as appropriate, given the scale of the organisation and the nature of the accountant's practice.

113. The firm should perform a firm-wide risk assessment that takes into account the size and nature of the practice; the existence of high-risk clients (if any); and the provision of high-risk services (if any). Once completed, the firm-wide risk assessment will assist the firm in designing its policies and procedures.

114. Accountants should consider using proven technology-driven solutions to minimize the risk of error and find efficiencies in their AML/CFT processes. As these solutions are likely to become more affordable, and more tailored to the needs of accountants as they continue to develop, this may be particularly important for smaller firms that may be less able to commit significant resources of time to these activities.

115. Depending on the size of the firm, the types of services provided, the risk profile of clients, and the overall assessed ML/TF risk, it may be possible to simplify internal procedures. For example, for sole practitioners, providing limited services to low-risk clients, client acceptance may be reserved for the sole owners/proprietors taking into account their business and client knowledge and experience. The involvement of the sole owner/proprietor may also be required in detecting and assessing possible suspicious activities. For larger firms, serving a diverse client base and providing multiple services across geographical locations, more sophisticated procedures are likely to be necessary.

Internal mechanisms to ensure compliance

116. Accountants (at the senior management level) should monitor the effectiveness of internal controls. If accountants identify any weaknesses in those internal controls, improved procedures should be designed.

117. The most effective tool to monitor the internal controls is a regular (typically at least annually) independent (internal or external) compliance review. If carried out internally, a staff member that has a good working knowledge

of the firm's AML/CFT internal control framework, policies, and procedures and is sufficiently senior to challenge them should perform the review. The person conducting an independent review should not be the same person who designed or implemented the controls being reviewed. The compliance review should include a review of CDD documentation to confirm that staff is properly applying the firm's procedures.

118. If the compliance review identifies areas of weakness and makes recommendations on how to improve the policies and procedures, then senior management should monitor how the firm is acting on those recommendations.

119. Accountants should review/update firm-wide risk assessments regularly and ensure that policies and procedures continue to target those areas where the ML/TF risks are highest.

Vetting and recruitment

120. Accountants should consider the skills, knowledge, and experience of staff both before they are appointed to their role and on an ongoing basis. The level of assessment should be proportionate to their role in the firm and the ML/TF risks they may encounter. Assessment may include criminal records checking and other forms of pre-employment screening such as credit reference checks and background verification (as permitted under national legislation) for key staff positions.

Education, training, and awareness

121. R.18 requires that accounting firms/ accountants provide their staff with AML/CFT training. For accountants, and those in smaller firms, in particular, such training may also assist with raising awareness of monitoring obligations. The accounting firm's commitment to having appropriate controls in place relies fundamentally on both training and awareness. This requires a firm-wide effort to provide all relevant staff with at least general information on AML/CFT laws, regulations, and internal policies.

122. Firms should provide targeted training for increased awareness by the accountant by providing specified activities to higher-risk clients and accountants undertaking higher-risk work. Case studies (both fact-based and hypotheticals) are a good way of bringing the regulations to life and making them more comprehensible. Training should also be targeted toward the role that the individual performs in the AML/CFT process. This could include false documentation training for those undertaking identification and verification duties or training regarding red flags for those undertaking client/transactional risk assessment.

123. In line with an RBA, particular attention should be given to risk factors or circumstances occurring in an accountant's practice. In addition, competent authorities, SRBs, and representative bodies should work with educational institutions to ensure that the relevant curricula address ML/TF risks. The same training should also be made available for students taking courses to train to become accountants.

124. Firms must provide their employees with appropriate AML/CFT training. In ensuring compliance with this requirement, accountants may take account of any AML/CFT training included in entry requirements and continuing professional development requirements for their professional staff. They must also ensure appropriate training for any relevant staff without professional qualification, at a level appropriate to the functions being undertaken by those staff, and the likelihood of their encountering suspicious activities.

125. The overall risk-based approach and the various methods available for training and education give accountants flexibility regarding the frequency, delivery mechanisms, and focus of such training. Accountants should review their staff and available resources and implement training programs that provide appropriate AML/CFT information that is:

(i) tailored to the relevant staff responsibility (e.g. client contact or administration);

(ii) at the appropriate level of detail (e.g. considering the nature of services provided by the accountants);

(iii) at a frequency suitable to the risk level of the type of work undertaken by the accountants; and

(iv) used to test to assess staff knowledge of the information provided.

Higher-risk countries (R.19 and 23)

126. Consistent with R.19, accountants should apply enhanced due diligence measures (also see paragraph 72 above), proportionate to the risks, to business relationships and transactions with clients from countries for which this is called for by the FATF.

Section IV – Guidance for supervisors

127. R.28 requires that accountants are subject to adequate AML/CFT regulation and supervision. Supervisors and SRBs must ensure that accountants are implementing their obligations under R.1.

A risk-based approach to supervision

128. A risk-based approach to AML/CFT means that measures taken to reduce ML/TF are proportionate to the risks. Supervisors and SRBs should supervise more effectively by allocating resources to areas of higher ML/TF risk. R.28 requires that accountants are subject to adequate AML/CFT regulation and supervision. While it is each country's responsibility to ensure there is an adequate national framework in place for the regulation and supervision of accountants, any relevant supervisors, and SRBs should have a clear understanding of the ML/TF risks present in the relevant jurisdiction.

Supervisors and SRBs' role in supervision and monitoring

129. According to R.28, countries can designate a competent authority or SRB to ensure that accountants are subject to effective oversight, provided that such an SRB can ensure that its members comply with their obligations to combat ML/TF.

130. An SRB is a body representing a profession (e.g. accountants, legal professionals, notaries, other independent legal professionals, or TCSPs) made up of member professionals, which has a role (either exclusive or in conjunction with other entities) in regulating the persons that are qualified to enter and who practice in the profession. An SRB also performs supervisory or monitoring functions (e.g. enforcing rules to ensure that high ethical and moral standards are maintained by those practicing the profession).

131. Supervisors and SRBs should have appropriate powers to perform their supervisory functions (including powers to monitor and impose effective, proportionate, and dissuasive sanctions), and adequate financial, human, and technical resources. Supervisors and SRBs should determine the frequency and intensity of their supervisory or monitoring actions on accountants based on their understanding of the ML/TF risks, and taking into consideration the characteristics of the accountants, in particular their diversity and number.

132. Countries should ensure that supervisors and SRBs are as equipped as competent authorities in identifying and sanctioning non-compliance by its members. Countries should also ensure that SRBs are well-informed about the importance of AML/CFT supervision, including enforcement actions as needed.

133. Countries should also address the risk that AML/CFT supervision by SRBs could be hampered by conflicting objectives about the SRB's role in representing their members, while also being obligated to supervise them. If an SRB contains members of the supervised population or represents those people, the relevant persons should not continue to take part in the monitoring/ supervision of their practice/firm to avoid conflicts of interest.

134. Supervisors and SRBs should allocate responsibility for managing AML/CFT related activity, where they are also responsible for other regulatory areas.

Understanding ML/TF risk

135. The extent to which a national framework allows accountants to apply an RBA should also reflect the nature, diversity, and maturity of the sector and its risk profile as well the ML/TF risks associated with individual accountants.

136. Access to information about ML/TF risks is essential for an effective risk-based approach. Countries are required to take appropriate steps to identify and assess ML/TF risks on an ongoing basis to (a) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations, and other measures; (b) assist in the allocation and prioritization of AML/CFT resources by competent authorities; and (c) make information available for AML/CFT risk assessments conducted by accountants and the jurisdictions' national risk assessment. Countries should keep the risk assessments up-to-date and should have mechanisms to provide appropriate information on the results to competent authorities, SRBs, and accountants. In situations where some accountants have limited capacity to identify ML/TF risks, countries should work with the sector to understand their risks.

137. Supervisors and SRBs should, as applicable, draw on a variety of sources to identify and assess ML/TF risks. These may include, but will not be limited to, the jurisdiction's national risk assessments, supranational risk assessments, domestic or international typologies, supervisory expertise, and FIU feedback. The necessary information can also be obtained through appropriate information-sharing and collaboration among AML/CFT supervisors when there are more than one for different sectors (legal professionals, accountants, and TCSPs).

138. These sources can also help determine the extent to which an accountant can effectively manage ML/TF risk. Information-sharing and collaboration should take place among AML/CFT supervisors across all sectors (legal professionals, accountants, and TCSPs).

139. Competent authorities may also consider undertaking a targeted sectoral risk assessment to get a better understanding of the specific environment in which accountants operate in the country and the nature of services provided by them.

140. Supervisors and SRBs should understand the level of inherent risk including the nature and complexity of services provided by the accountant. Supervisors and SRBs should also consider the type of services the accountant is providing as well as its size and business model (e.g., whether it is a sole practitioner), corporate governance arrangements, financial and accounting information, delivery channels, and client profiles, geographic location, and countries of operation. Supervisors and SRBs should also consider the controls accountants have in place (e.g., the quality of the risk management policy, the functioning of the internal oversight functions, and the quality of oversight of any outsourcing and subcontracting arrangements).

141. Supervisors and SRBs should seek to ensure their supervised populations are fully aware of and compliant with, measures to identify and verify a client, the client's source of wealth, and funds were required, along with measures designed to ensure transparency of beneficial ownership, as these are cross-cutting issues that affect several aspects of AML/CFT.

142. To further understand the vulnerabilities associated with beneficial ownership, with a particular focus on the involvement of professional intermediaries, supervisors should stay abreast of research papers and typologies published by international bodies. Useful references include the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership published in July 2018.

143. Supervisors and SRBs should review their assessment of accountants' ML/TF risk profiles periodically, including when circumstances change materially or relevant new threats emerge, and appropriately communicate this assessment to the profession.

Mitigating and managing ML/TF risk

144. Supervisors and SRBs should take proportionate measures to mitigate and manage ML/TF risk. Supervisors and SRBs should determine the frequency and intensity of these measures based on their understanding of the inherent ML/TF risks. Supervisors and SRBs should consider the characteristics of accountants, particularly where they act as professional intermediaries, in particular their diversity and number. It is essential to have a clear understanding of the ML/TF risks: (a) present in the country; and (b) associated with the type of accountant and their clients, products, and services.

145. Supervisors and SRBs should take account of the risk profile of accountants when assessing the adequacy of internal controls, policies, and procedures.

146. Supervisors and SRBs should develop a means of identifying which accountants are at the greatest risk of being used by criminals. This involves considering the probability and impact of ML/TF risk.

147. Probability means the likelihood of ML/TF taking place as a consequence of the activity undertaken by accountants and the environment in which they operate. The risk can also increase or decrease depending on other factors:

(i) service and product risk (the likelihood that services or products can be used for ML/TF);

(ii) client risk (the likelihood that clients' funds may have criminal origins);

(iii) the nature of transactions (e.g., frequency, volume, counterparties);

(iv) geographical risk (whether the accountant, its clients, or other offices trade in riskier locations); and

(v) other indicators of risk are based on a combination of objective factors and experience, such as the supervisor's wider work with the accountant as well as information on its compliance history, complaints about the accountant or the quality of its internal controls, and intelligence from law enforcement agencies on suspected involvement in financial crimes (including unwitting facilitation). Other such factors may include information from government/law enforcement sources, whistle-blowers, or negative news reports from credible media particularly those related to predicate offences for ML/TF or financial crimes.

148. In adopting an RBA to supervision, supervisors may consider allocating supervised entities sharing similar characteristics and risk profiles into groupings for supervision purposes. Examples of characteristics and risk profiles could include the size of the business, type of clients serviced, and geographic areas of activities. The setting up of such groupings could allow supervisors to take a comprehensive view of the sector, as opposed to an approach where the supervisors concentrate on the individual risks posed by the individual firms. If the risk profile of an accountant within a grouping changes, supervisors may reassess the supervisory approach, which may include removing the accountant from the grouping.

149. Supervisors and SRBs should also consider the impact, i.e. the potential harm caused if ML/TF is facilitated by the accountant or group of accountants. A small number of accountants may cause a high level of harm. This can depend on:

(a) size (i.e. turnover), number and type of clients, number of premises, the value of transactions, etc.); and

(b) links or involvement with other businesses (which could affect the susceptibility to being involved in 'layering' activity, e.g., concealing the origin of the transaction with the purpose to legalize the asset).

150. The risk assessment should be updated by supervisors and SRBs on an ongoing basis. The result from the assessment will help determine the resources the supervisor will allocate to the supervision of accountants.

151. Supervisors or SRBs should consider whether accountants meet the ongoing requirements for continued participation in the profession as well as assessments of competence and fitness and propriety. This will include whether the accountant meets expectations related to AML/CFT compliance. This will take place both when a supervised entity joins the profession, and on an ongoing basis thereafter.

152. If a jurisdiction chooses to classify an entire sector as higher risk, it should be possible to differentiate between categories of accountants based on factors such as their client base, countries they deal with, applicable AML/CFT controls, etc.

153. Supervisors and SRBs should acknowledge that in a risk-based regime, not all accountants will adopt identical AML/CFT controls and that an isolated incident where the accountant is part of an illegal transaction unwittingly

does not necessarily invalidate the integrity of the accountant's AML/CFT controls. At the same time, accountants should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

154. Supervisors and SRBs should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and the existing AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to accountants to enable them to enhance their RBA.

Supervision of the RBA Licensing or registration

155. R.28 requires a country to ensure that accountants are subject to regulatory and supervisory measures to ensure compliance by the profession with AML/CFT requirements.

156. R.28 requires the supervisor or SRB to take the necessary measures to prevent criminals or their associates from being professionally accredited or holding or being the beneficial owner of a significant or controlling interest or holding a management function in an accountancy practice. This can be achieved through the evaluation of these persons through a "fit and proper" test.

157. A licensing or registration mechanism is one of the means to identify accountants to whom the regulatory and supervisory measures, including the "fit and proper" test should be applied. It also enables the identification of the number of accountants to assess and understand the ML/TF risks for the country, and the action that should be taken to mitigate them by R.1.

158. Licensing or registration provides a supervisor or SRB with the means to fulfil a "gatekeeper" role over who can undertake the activities specified in R.22. Licensing or registration should ensure that upon qualification, accountants are subject to AML/CFT compliance monitoring.

159. The supervisor or SRB should actively identify individuals and businesses who should be supervised by using intelligence from other competent authorities (e.g., FIUs, company registry, or tax authority), information from financial institutions and DNFBPs, complaints by the public, open-source information from advertisements and business and commercial registries, or any other sources which indicate that unsupervised individuals or businesses are providing the activities specified in R.22.

160. Licensing or registration frameworks should define the activities that are subject to licensing or registration, prohibit unlicensed or unregistered individuals or businesses providing these activities and s, et out measures for both refusing licenses or registrations and for removing "bad actors".

161. The terms "licensing" or "registration" are not interchangeable. Licensing regimes generally tend to operate over financial institutions and impose mandatory minimum requirements based upon Core Principles on issues such as capital, governance, and resources to manage and mitigate prudential, conduct as well as ML/TF risks on an ongoing basis. Some jurisdictions have adopted similar licensing regimes for accountants, generally where accountants carry out trust and corporate services, to encompass aspects of prudential and conduct requirements in managing the higher level of ML/TF risks that have been identified in that sector.

162. A jurisdiction may have a registration framework over the entire DNFBP sector, including accountants, or have a specific registration framework for each constituent of a DNFBP. Generally, a supervisor or SRB carries out the registration function.

163. The supervisor or SRB should ensure that requirements for licensing or registration and the process for applying are clear, objective, publicly available, and consistently applied. Determination of the license or registration should be objective and timely. An SRB could be responsible for both supervision and for representing the interests of its members. If so, the SRB should ensure that registration decisions are taken separately and independently from its activities regarding member representation.

Fit and proper tests:

164. A fit and proper test provide a possible mechanism for a supervisor or SRB to take the necessary measures to prevent criminals or their associates from owning, controlling, or holding a management function in an accountancy practice.

165. By R.28, the supervisor or SRB should establish the integrity of every beneficial owner, controller, and individual holding a management function in an accountancy practice. However, the decisions on an individual's fitness and propriety may also be based upon a range of factors concerning the individual's competency, probity, and judgment as well as integrity.

166. In some jurisdictions, a "fit and proper test" forms a fundamental part of determining whether to license or register the applicant and whether on an ongoing basis the licensee or registrant (including its owners and controllers, where applicable) remains fit and proper to continue in that role. The initial assessment of an individual's fitness and propriety is a combination of obtaining information from the individual and corroborating elements of that information against independent credible sources to determine whether the individual is fit and proper to hold that position.

167. The process for determining fitness and propriety generally requires the applicant to complete a questionnaire. The questionnaire could gather personal identification information, and residential and employment history, and require disclosure by the applicant of any convictions or adverse judgments, including pending prosecutions and convictions relating to the applicant. Elements of this information should be corroborated to establish the bona fides of an individual. Such checks could include inquiries about the individual with law enforcement agencies and other supervisors or screening the individual against independent electronic search databases. The personal data collected should be kept confidential.

168. The supervisor or SRB should also ensure on an ongoing basis that those holding or being the beneficial owner of a significant or controlling interest and individuals holding management functions are fit and proper. A fit and proper test should apply to new owners, controllers, and individuals holding a management function. The supervisor or SRB should consider re-assessing the fitness and propriety of these individuals arising from any supervisory findings, receipt of information from other competent authorities; or open-source information indicating significant adverse developments.

Guarding against "brass-plate" operations

169. The supervisor or SRB should ensure that its licensing or registration requirements require the applicant to have a meaningful physical presence in the jurisdiction. This usually means that the applicant should have their place of business in the jurisdiction. Where an applicant is a legal person, those individuals who form its mind and management, should also be residents in the jurisdiction and be actively involved in the business. A business with only staff who do not possess the professional requirements of an accountant should not be licensed or registered.

170. A supervisor or SRB should consider the ownership and control structure of the applicant to determine that sufficient control over its operation will reside within the business, which it is considering licensing or registering.

Factors to take into account could include consideration where the beneficial owners and controllers reside, the number and type of management functions the applicant is proposing to have in the country, such as directors and managers, including compliance managers, and the caliber of the individuals who will be occupying those roles.

171. The supervisor or SRB should also consider whether the ownership and control structure of accountants unduly hinders its identification of the beneficial owners and controllers or presents obstacles to applying effective supervision.

Monitoring and supervision

172. Supervisors and SRBs should take measures to effectively monitor accountants through on-site and off-site supervision. The nature of this monitoring will depend on the risk profiles prepared by the supervisor or SRB and the connected risk-based approach. Supervisors and SRBs may choose to adjust:

(a) the level of checks required to perform their licensing/registration function: where the ML/TF risk associated with the sector is low, the opportunities for ML/TF associated with a particular business activity may be limited, and approvals may be made on a review of basic documentation. Where the ML/TF risk associated with the sector is high, supervisors and SRBs may ask for additional information.

(b) the type of on-site or off-site AML/CFT supervision: supervisors and SRBs may determine the correct mix of on-site and off-site supervision of accountants. Off-site supervision may involve analysis of annual independent audits and other mandatory reports, identifying risky intermediaries (i.e. based on the size of the firms, involvement in cross-border activities, or specific business sectors), automated scrutiny of registers to detect missing beneficial ownership information, and identification of persons responsible for the filing. It may also include undertaking thematic reviews of the sector, making compulsory the periodic information returns from firms. Off-site supervision alone may not be appropriate in higher-risk situations. On-site inspections may involve reviewing AML/CFT internal policies, controls, and procedures, interviewing members of senior management, compliance officers' other relevant staff, considering gatekeeper's risk assessments, spot-checking CDD documents and supporting evidence, looking at reporting ML/TF suspicions about clients and other matters, which may be observed in the course of an onsite visit and, where appropriate, sample testing of reporting obligations.

(c) the frequency and nature of ongoing AML/CFT supervision: supervisors and 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 as issues emerge (e.g. as a result of whistleblowing, information from law enforcement, or other supervisory findings resulting from accountants' inclusion in thematic review samples).

(d) the intensity of AML/CFT supervision: supervisors and SRBs should decide on the appropriate scope or level of assessment in line with the risks identified, to assess the adequacy of accountants' policies and procedures that are designed to prevent them from being abused. Examples of more intensive supervision could include; detailed testing of systems and files to verify the implementation and adequacy of the accountant's risk assessment, CDD, reporting, and record-keeping policies and processes, internal auditing, interviews with operational staff, senior management, and the Board of directors and AML/CFT assessment in particular lines of business.

173. Supervisors and SRBs should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and the existing AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to accountants to enable them to enhance their RBA.

174. Record keeping and quality assurance are important so that supervisors can document and test the reasons for significant decisions relating to AML/CFT supervision. Supervisors should have an appropriate information retention policy and be able to easily retrieve information while complying with the relevant data protection legislation. Record keeping is crucial and fundamental to the supervisors' work. Undertaking adequate quality assurance is also fundamental to the supervisory process to ensure decision-making/sanctioning is consistent across the supervised population.

Enforcement

175. R.28 requires supervisors or SRBs to have adequate powers to perform their functions, including powers to monitor compliance by accountants. R.35 requires countries to have the power to impose sanctions, whether criminal, civil or administrative, on DNFPBs, to include accountants when providing the services outlined in R.22(d). Sanctions should be available for the directors and senior management of the firm when an accountant fails to comply with requirements.

176. Supervisors and SRBs should use proportionate actions, including a range of supervisory interventions and corrective actions to ensure that any identified deficiencies are addressed promptly. Sanctions may range from an informal or written warning, reprimand, and censure to punitive measures (including disbarment and criminal prosecutions where appropriate) for more egregious non-compliance, as identified weaknesses can have wider consequences. Generally, systemic breakdowns or significantly inadequate controls will result in a more severe supervisory response.

177. Enforcement by supervisors and SRBs should be proportionate while having a deterrent effect. Supervisors and SRBs should have (or should delegate to those who have) sufficient resources to investigate and monitor non-compliance. Enforcement should aim to remove the benefits of non-compliance.

Guidance:

178. Supervisors and SRBs should communicate their regulatory expectations. This could be done through a consultative process after meaningful engagement with relevant stakeholders, including accountants. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based rules, and information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. Guidance issued to accountants should also discuss ML/TF risk within their sector and outline ML/TF indicators to help them identify suspicious transactions and activity. All such guidance should preferably be consulted on, where appropriate, and drafted in ways that are appropriate to the context of the role of supervisors and SRBs in the relevant jurisdiction.

179. Where supervisors' guidance remains high-level and principles-based, this may be supplemented by further guidance written by the accountancy profession, which may cover operational and practical issues, and be more detailed and explanatory. Where supervisors cooperate to produce combined guidance across sectors, supervisors should ensure this guidance adequately addresses the diversity of roles that come within the guidance's remit, and that such guidance provides practical direction to all its intended recipients. The private sector guidance should be consistent with national legislation and with any guidelines issued by competent authorities about the accountancy profession and be consistent with all other legal requirements and obligations.

180. Supervisors should consider communicating with other relevant domestic supervisory authorities to secure a coherent interpretation of the legal obligations and to minimize disparities across sectors (such as legal professionals, accountants, and TCSPs). Multiple guidance should not create opportunities for regulatory arbitrage. Relevant supervisory authorities should consider preparing joint guidance in consultation with the relevant sectors while recognizing that in many jurisdictions accountants will consider that separate guidance targeted at their profession will be the most appropriate and effective form.

181. Information and guidance should be provided by supervisors in an up-to-date and accessible format. It could include sectoral guidance material, newsletters, internet-based material, oral updates on supervisory visits, meetings, and annual reports.

Training

182. Training is important for supervisory staff, and other relevant employees, to understand the accountancy profession and the various business models that exist. In particular, supervisors should ensure that staff is trained

to assess the quality of ML/TF risk assessments and to consider the adequacy, proportionality, effectiveness, and efficiency of AML/CFT policies, procedures, and internal controls. It is recommended that the training has a practical basis/dimension.

183. Training should allow supervisory staff to form sound judgments about the quality of the risk assessments made by accountants and the adequacy and proportionality of AML/CFT controls of accountants. It should also aim at achieving consistency in the supervisory approach at a national level, in cases where there are multiple competent supervisory authorities, or when the national supervisory model is devolved or fragmented.

Endorsements

184. Supervisors should avoid mandating the use of AML systems, tools, or software of any third-party commercial providers to avoid conflicts of interest in the effective supervision of firms.

Information exchange

185. Information exchange between the public and private sectors and within the private sector (e.g., between financial institutions and accountants) is important to combat ML/TF. Information sharing and intelligence sharing arrangements between supervisors and public authorities (such as Financial Intelligence Units and law enforcement) should be robust, secure, and subject to compliance with national legal requirements.

186. The type of information that could be shared between the public and private sectors include:

(a) ML/TF risk assessments;

(b) Typologies (i.e., case studies) of how money launderers or terrorist financiers have misused accountants;

(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 accountants as a class or individually; and

(e) countries, persons, or organisations whose assets or transactions should be frozen under targeted financial sanctions as required by R.6.

187. Domestic co-operation and information exchange between FIU and supervisors of the accountancy profession and among competent authorities including law enforcement, intelligence, FIU, tax authorities, supervisors, and SRBs is also vital for effective monitoring/supervision of the sector. Such cooperation and coordination may help avoid gaps and overlaps in supervision and ensure sharing of good practices and findings. Intelligence about active misconduct investigations and completed cases between supervisors and law enforcement agencies should also be encouraged. When sharing information, protocols and safeguards should be implemented to protect personal data.

188. Cross-border information sharing of authorities and the private sector with their international counterparts is of importance in the accountancy profession, taking account of the multi-jurisdictional reach of many accounting firms.

Supervision of Beneficial Ownership requirements and source of funds/wealth requirements:

189. The FATF Recommendations require competent authorities to have access to adequate, accurate, and timely information on the beneficial ownership and control of legal persons (R.24). In addition, countries must take measures to prevent the misuse of legal arrangements for ML/TF, in particular ensuring that it is adequate, accurate, and timely information on express trusts (R.25). Implementation of the FATF Recommendations on beneficial ownership has proven challenging. As a result, the FATF developed a Guidance on Transparency and

Beneficial Ownership (2014) to assist countries in their implementation of R.24 and R.25, as well as R.1 as it relates to understanding the ML/TF risks of legal persons and legal arrangements. The FATF and Egmont Group also published the Report on Concealment of Beneficial Ownership in July 2018 which identified issues to help address the vulnerabilities associated with the concealment of beneficial ownership.

190. R.24 and R.25 require countries to have mechanisms to ensure that information provided to registries is accurate and updated on a timely basis and that beneficial ownership information is accurate and current. To determine the adequacy of a system for monitoring and ensuring compliance, countries should have regarded the risk of AML/CFT in given businesses (i.e. if there is a proven higher risk then higher monitoring measures should be taken). Accountants must, however, be cautious in blindly relying on the information contained in registries. It is important for there to be some form of ongoing monitoring during a relationship to detect unusual and potentially suspicious transactions as a result of a change in beneficial ownership as registries are unlikely to provide such information on a dynamic basis.

191. Those responsible for company formation and the creation of legal arrangements fulfill a key gatekeeper role to the wider financial community through the activities they undertake in the formation of legal persons and legal arrangements or their management and administration.

192. As DNFBPs, accountants are required to apply CDD measures to beneficial owners of legal persons and legal arrangements to whom they are providing advice or formation services. In several countries, an accountant may be required as part of the process of registering the legal person and will be responsible for providing basic and/or beneficial ownership information to the registry.

193. In their capacity as company directors, trustees, foundation officials, etc. of these legal persons and legal arrangements, accountants often represent these legal persons and legal arrangements in their dealings with other financial institutions and DNFBPs that are providing banking or audit services to these types of clients.

194. These financial institutions and other DNFBPs may request the CDD information collected and maintained by accountants, who because of their role as director or trustee, will be their principal point of contact with the legal person or legal arrangement. These financial institutions and other DNFBPs may never meet the beneficial owners of the legal person or legal arrangement.

195. Under R.28, countries are to ensure that accountants are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements, which includes identifying the beneficial owner/s and taking reasonable measures to verify them. R.24 and R.25, which deal with transparency of beneficial ownership of legal persons and legal arrangements, require countries to have mechanisms for ensuring that adequate, accurate, and up-to-date information on these legal entities is available on a timely basis.

196. By R.28, accountants should be subject to risk-based supervision by a supervisor or SRB covering the beneficial ownership and recordkeeping requirements of R.10 and R.11. The supervisor or SRB should have a supervisory framework, which can help in ascertaining that accurate and current basic and beneficial ownership information on legal persons and legal arrangements is maintained and will be available on a timely basis to competent authorities.

197. The supervisor or SRB should analyse the adequacy of the procedures and the controls, which accountants have established to identify and record the beneficial owner. In addition, they should undertake sample testing of client records on a representative basis to gauge the effectiveness of the application of those measures and the accessibility of accurate beneficial ownership information.

198. During onsite and offsite inspections, the supervisor or SRB should examine the policies, procedures, and controls that are in place for taking on new clients to establish what information and documentation are required where a client is a natural person or legal person or arrangement. The supervisor or SRB should verify the adequacy of these procedures and controls to identify beneficial owners understand the ownership and control structure of

these legal persons and arrangements and ascertain the business activity. For example, self-declaration on beneficial ownership provided by the client without any other mechanism to verify the information will not be adequate in all cases.

199. Sample testing of records will assist the supervisor or SRB in determining whether controls are effective for the accurate identification of beneficial ownership, accurate disclosure of that information to relevant parties, and for establishing if that information is readily available. The extent of testing will be dependent on risk but the records selected should reflect the profile of the client base and include both new and existing clients.

200. The supervisor or SRB should consider the measures the accountants have put in place for monitoring changes in the beneficial ownership of a legal person and legal arrangements to whom they provide services to ensure that beneficial ownership information is accurate and current and to determine how timely updated filings are made, where relevant to a registry.

201. During examinations, the supervisor or SRB should consider whether to verify the beneficial ownership information available on the records of accountants with that held by the relevant registry, if any. The supervisor or SRB may also consider information from other competent authorities such as FIUs, public reports, and information from other financial institutions or DNFBPs, to verify the efficacy of accountants' controls.

202. Accountants should be subject to risk-based supervision by a supervisor or SRB covering the requirements to identify and evidence the source of funds and source of wealth for higher-risk clients to whom they provide services. The supervisor or SRB should have a supervisory framework, which can help in ascertaining that accurate and current information on sources of funds and wealth is properly evidenced and available on a timely basis to competent authorities. The supervisor or SRB should analyse the adequacy of the procedures and controls that accountants have established to identify and record sources of wealth in arrangements.

Nominee arrangements:

203. A nominee director is a person who has been appointed to the Board of Directors of the legal person who represents the interests and acts by instructions issued by another person, usually the beneficial owner.

204. A nominee shareholder is a natural or legal person who is officially recorded in the register of members and shareholders of a company as the holder of a certain number of specified shares, which are held on behalf of another person who is the beneficial owner. The shares may be held in trust or through a custodial agreement.

205. In several countries, accountants act or arrange for other persons (either individuals or corporate) to act as directors. Accountants also act or arrange for other persons (either individuals or corporate) to act as nominee shareholders for another person as part of their professional services. By R.24, one of the mechanisms to ensure that nominee shareholders and directors are not misused is by subjecting these accountants to licensing and recording their status in company registries. Countries may rely on a combination of measures in this respect.

206. There are legitimate reasons for accountants to act as or provide directors to a legal person or act or provide nominee shareholders. These may include the settlement and safekeeping of shares in listed companies were post-traded specialists act as nominee shareholders. However, nominee director and nominee shareholder arrangements can be misused to hide the identity of the true beneficial owner of the legal person. There may be individuals prepared to lend their name as a director or shareholder of a legal person on behalf of another without disclosing the identity of the person from whom they will take instructions or whom they represent. They are sometimes referred to as "strawmen".

207. Nominee directors and nominee shareholders can create obstacles to identifying the true beneficial owner of a legal person, particularly where the status is not disclosed. This is because it will be the identity of the nominee that is disclosed in the corporate records of the legal person held by a registry and in the company records at its registered office. Company law in various countries does not recognize the status of a nominee director because in

law it is the directors of the company who are liable for its activities and the directors must act in the best interest of the company.

208. The supervisor or SRB should be aware that undisclosed nominee arrangements may exist. They should consider whether undisclosed nominee arrangements would be identified and addressed during their onsite and offsite inspections and examination of the policies, procedures, controls, and client records of the accountant, including the CDD process and ongoing monitoring by the accountant.

209. An undisclosed nominee arrangement may exist where there are the following (non-exhaustive) indicators:

(a) the profile of a director or shareholder is inconsistent with the activities of the company;

(b) the individual holds numerous appointments to unconnected companies;

(c) a director's or shareholder's source of wealth is inconsistent with the value and nature of the assets within the company;

(d) funds into and out of the company are sent to, or received from unidentified third party/ies;

(e) the directors or shareholders are accustomed to acting on the instruction of another person; and

(f) requests or instructions are subject to minimal or no scrutiny and/or responded to extremely quickly without challenge by the individual/s purporting to act as the director/s.

Sum up:

Money laundering is a common issue around the globe. In recent times, money laundering and terror financing have forced several governments and regulators globally to focus on stopping the illegitimate flow of funds. However, combating this problem remains a primary challenge for nations and financial institutions all over the world. The legalization of crime revenues has numerous damaging outcomes. Financial crimes result in the deterioration of the administrative order and economic stability. Governments have taken several measures from the past prevent money laundering. The objective of these measures is to prevent financial crimes and ensure that the administrative and economic stability of the nation is maintained.

Anti-Money Laundering (AML) in India is described as a set of regulations, laws, or procedures particularly designed to prevent the activity of generating money via illegal ways and methods. The Prevention of Money Laundering Act, 2002 (PMLA) along with the Prevention of Money Laundering (Maintenance of Records) Rules,

2005 (Rules) are the principal laws that are enforced to prohibit money laundering activities in India. There are specialised authorities that deal with the money laundering problems such as the Reserve Bank of India/ Securities and Exchange Board of India (SEBI)/ Insurance Regulatory and Development Authority of India, which lay down guidelines on anti-money laundering standards following PMLA and Rules.

Anti-Money Laundering Laws & Regulations: The Financial Action Task Force on Money Laundering (FATF), an intergovernmental body introduced by the G-7 Summit in Paris in 1989 and responsible for setting global standards on anti-money laundering and combating the financing of terrorism explains money laundering as the processing of criminal proceeds to disguise their illegitimate origin to legitimize the illegal gains of crime. In 2010, India became the 34th nation member of the Financial Action Task Force. India is one of the signatories to several United Nations Conventions which tackle anti-money laundering and countering the financing of terrorism.

India has prohibited money laundering under the Prevention of Money Laundering Act, 2002 (PMLA) and also in the Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act) (amended in 2001). The Prevention of Money Laundering Act, 2002 coupled with the rules issued under it and the rules and regulations formed by regulators such as the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) displays a broad framework for the anti-money laundering laws in India.

The Prevention of Money Laundering Act, 2002: In 1998, The Prevention of Money Laundering Bill was introduced in the Lok Sabha, passed in 2003, and came into force in 2005. It has gone through several amendments, with the last one being in 2019. Administration and enforcement authorities are chosen under PMLA to execute its provisions and rules. Certain powers are vested, which are very similar to those granted to the civil courts of the nation, to exercise the provisional attachment of properties that are involved in the offence under PMLA.

The PMLA attempts to combat acts related to money laundering in India and because of this, it has three main objectives i.e.

(i) to prevent and control money laundering

(ii) to confiscate and seize the property acquired from the laundered money

(iii) to deal with any other issue about money laundering in India.

Under the provisions of the PMLA, the Financial Intelligence Unit of India (FIU-IND) was formed in 2004 as the primary body for coordinating India's AML efforts. The primary function of FIU-IND is to receive, analyse, process and disseminate information relating to suspect financial transactions. FIU-IND also coordinates and strengthens efforts of national investigation, international intelligence, and enforcement agencies in pursuing the global efforts against money laundering and financing of terrorism. In 2005, the Enforcement Directorate (ED) was introduced by the Government of India to utilize exclusive powers related to the investigation and prosecution under PMLA.

The primary legislation other than the Prevention of Money Laundering Act, 2002, which directly or indirectly focuses to curb and fight money laundering activities are as follows:

1. **The Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974:** The act was passed in 1974 in furtherance of the government's attempt to retain foreign exchange within the nation. The Act is established on the concept of Preventive Detention which, apart from being a colonial legacy, is also given explicitly in our constitution as 'the necessary evil' and laws exist under Article 22 of the Indian Constitution for the same reasons related to the security of the state and maintenance of public order. According to the provisions of section 10, the stipulated period of detention is 1 to 2 years.

All decisions in furtherance of the Act may be taken by the state or central government. The relevant provisions in this regard which must be taken into consideration are Section 3 (power to make orders detaining certain persons), Section 4 (execution of detention orders), Section 5 (power to regulate place and conditions of detention), and Section 11 (revocation of detention orders).

2. The Benami Transactions (Prohibition) Act, 1988: A Benami transaction is a transaction in which property is transferred to one person for a value paid or provided by another person and often, the identity of the persons involved is concealed. This Act was passed in 1988. It is to constrain Benami transactions and the right to recover property held by Benami. Section 3 of the Act specifically debars anyone from getting into a Benami transaction. The Act further specifies those properties obtained under the Benami transaction which are liable to be acquired by the competent authorities without any need for compensation to be payable by such authority.

3. The Indian Penal Code, 1860 and Code of Criminal Procedure, 1973: The Indian Penal Code, 1860 is the primary substantive law that regulates several criminal activities and also prescribes penalties for them. The Code of Criminal Procedure, 1973 on the other hand is a part of procedural law that specify procedures to be followed in criminal cases. Several offences under the Indian Penal Code have been recognised as being scheduled offences within the meaning explained in the PMLA. Further, Section 65 of the PMLA also specifies that the provisions of the Code of Criminal Procedure are to be followed in respect of the several proceedings prescribed under the PMLA.

4. The Narcotic Drugs and Psychotropic Substances Act, 1985: This Act was passed in 1985 to consolidate and amendment of laws relating to narcotic drugs. Keeping in line with its objectives identifies, lists, and explains several forms and types of narcotic drugs and psychotropic substances.

The Act, in its essence, attempts to stop and restrict the transport and vending of narcotic and psychotropic substances and does not mention money laundering activities. It may, however, be taken into consideration that the trade of narcotic substances does generate a lot of cash for people involved in it. So much so that a noticeable portion of the money involved in drug trafficking is then mobilised to give it legitimacy or in simple words, the same money gets laundered. The NDPS Act, by working against practices involving drug trading and trafficking puts a direct restriction on the flow of money into illegitimate activities.

To Conclude, Money Laundering is a universal menace and cannot be resolved by a single nation alone. The activities related to money laundering have been spreading in Indian society, despite the best efforts of the Indian government to stop such practices. Through legislation and administrative bodies and efficient regulators who work tirelessly in this matter, the fight against money laundering activities continues to go on. Although such activities may be controlled at a domestic level, such practices are never restricted to the confines of a single jurisdiction. Restrictions at a specific jurisdiction motivate launderers to shift base to another jurisdiction which may give a hospitable environment for their activities to grow.

It may be noted that funds brought in by illegitimate ways for legitimisation, once legalised, be again utilised for the vested interests of the beneficiaries who may not always have good intentions in mind. Crime can only result in more crime and the vicious circle would only continue. Whereas checks are required to be maintained regularly on money laundering activities- one of the better methods to stop money laundering practices may be for governments to introduce such legitimate interests into confidence and provide them protection and certain benefits which may altogether restrict people from engaging in money laundering activities.

Solved Case

M/s XYZ Limited is a company engaged in the real estate and construction business. To build a land bank in various parts of India that were likely to see commercial development and anticipate a future upward trend in land prices in various parts of India. M/s XYZ Limited hired the services of Mr Mahesh to assist in the process of acquisition of lands.

M/s XYZ Limited issued a detailed offer letter to Mr Mahesh for the purchase of around 100 acres of land at the maximum price of ₹10, 00,000 per acre in different parts of India within a period not exceeding five years. The said offer was accepted by Mr Mahesh by a letter of acceptance. Upon exchange of offer and acceptance, a legally binding and valid contract came to be forced between M/s XYZ Limited and Mr Mahesh.

Mr Mahesh received from M/s XYZ Limited a sum of ₹1,000 Crore as a loan/advance for the purchase of lands as specified in the contract between the parties. Mr Mahesh purchased various movable and immovable properties with the funds received from M/s XYZ Limited. Since all the funds could not be directly invested in the land as required by the contract, investments were made by Mr Mahesh by himself or through his company in the purchase of immovable property, including land, built-up residential and commercial buildings, etc. and Investment in fixed deposits in name of Mr Mahesh and M/s PQR Limited (95% shareholding by Mr Mahesh) also investment in the movable property including bank balance and few vehicles.

In the meantime, the Directorate of Enforcement initiated Suo moto proceedings under the Prevention of Money Laundering Act, 2002 (PMLA) and registered a complaint under Sections 3 and 4 of the PMLA and attached the property of Mr Mahesh under the Prevention of Money Laundering Act, 2002.

Given the above, answer the following question:

(a) Discuss the attachment of property involved in money laundering under PMLA.

(b) Explain the extent of punishment prescribed under PMLA.

(c) Discuss Appellate Authority establish under PMLA and what is the time limit to file an appeal.

Suggested Solution:

(a) Section 5 of the Prevention of Money Laundering Act, 2002 (PMLA) deals with the provision of attachment of property involved in money laundering.

As per Section 5(1) of the PMLA, Where the Director or any other officer not below the rank of Deputy Director authorised by the Director, has reason to believe (the reason for such belief to be recorded in writing), based on material in his possession, that Section 5(2) states that the Director, or any other officer not below the rank of Deputy Director, shall, immediately after attachment under sub-section (1), forward a copy of the order, along with the material in his possession, to the Adjudicating Authority, in a sealed envelope, in the manner as may be prescribed and such Adjudicating Authority shall keep such order and material for such period as may be prescribed.

Section 5(3) provides that every order of attachment made under sub-section (1) shall cease to have effect after the expiry of the period specified in sub-section (1) or on the date of an order made under sub-section (3) of section 8, whichever is earlier.

As per Section 5(4) of PMLA, nothing in this section shall prevent the person interested in the enjoyment of the immovable property attached under sub-section (1) from such enjoyment.

It may be noted that the person interested, in any immovable property, includes all persons claiming or entitled to claim any interest in the property.

Section 5(5) states that the Director or any other officer who provisionally attaches any property under sub-section (1) shall, within thirty days from such attachment, file a complaint stating the facts of such attachment before the Adjudicating Authority.

(b) The offence of money Laundering and Punishment for money Laundering are specified under Sections

3 and 4 of the Prevention of Money Laundering Act, 2002 respectively.

Section 3 of the Prevention of Money Laundering Act, 2002 provides that whosoever directly or indirectly attempts to indulge or knowingly assists or is a party or is involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of the offence of money-laundering.

It may be further noted that proceeds of crime mean any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property.

According to Section 4 of the Prevention of Money Laundering Act, 2002, whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine.

It may be noted that where the proceeds of crime involved in money-laundering relate to any offence specified under paragraph 2 of Part A of the Schedule to the PMLA, shall be punishable with rigorous imprisonment for a term which shall not be

(a) any person has any proceeds of crime; and

(b) such proceeds of crime are likely to be concealed, transferred or dealt with in any manner which may result in frustrating any proceedings relating to the confiscation of such proceeds of crime, he may, by order in writing, provisionally attach such property for a period not exceeding one hundred and eighty days from the date of the order, in such manner as may be prescribed.

It may be noted that no such order of attachment shall be made unless, about the scheduled offence, a report has been forwarded to a Magistrate under section 173 of the Code of Criminal Procedure, 1973, or a complaint has been filed by a person authorised to investigate the offence mentioned in that Schedule, before a Magistrate or court for taking cognizance of the scheduled offence, as the case may be, or a similar report or complaint has been made or filed under the corresponding law of any other country.

Further, notwithstanding anything contained above, any property of any person may be attached, if the Director or any other officer not below the rank of Deputy Director authorised by him for Section of the PMLA has reason to believe (the reasons for such belief to be recorded in writing), based on material in his possession, that if such property involved in money-laundering is not attached immediately, the non-attachment of the property is likely to frustrate any proceeding under the Act.

To compute the period of one hundred and eighty days, the period during which the proceedings under Section 5 of PMLA are stayed by the High Court, shall be excluded and a further period not exceeding thirty days from the date of order of vacation of such stay order shall be counted.

Section 5(2) states that the Director, or any other officer not below the rank of Deputy Director, shall, immediately after attachment under sub-section (1), forward a copy of the order, along with the material in his possession, to the Adjudicating Authority, in a sealed envelope, in the manner as may be prescribed and such Adjudicating Authority shall keep such order and material for such period as may be prescribed.

Section 5(3) provides that every order of attachment made under sub-section (1) shall cease to have effect after the expiry of the period specified in sub-section (1) or on the date of an order made under sub-section (3) of section 8, whichever is earlier.

As per Section 5(4) of PMLA, nothing in this section shall prevent the person interested in the enjoyment of the immovable property attached under sub-section (1) from such enjoyment.

It may be noted that the person interested, in any immovable property, includes all persons claiming or entitled to claim any interest in the property.

Section 5(5) states that the Director or any other officer who provisionally attaches any property under sub-section (1) shall, within thirty days from such attachment, file a complaint stating the facts of such attachment before the Adjudicating Authority.

The offence of money Laundering and Punishment for money Laundering are specified under Sections 3 and 4 of the Prevention of Money Laundering Act, 2002 respectively.

Section 3 of the Prevention of Money Laundering Act, 2002 provides that whosoever directly or indirectly attempts to indulge or knowingly assists or is a party or is involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of the offence of money-laundering.

It may be further noted that proceeds of crime mean any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property.

According to Section 4 of the Prevention of Money Laundering Act, 2002, whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine.

It may be noted that where the proceeds of crime involved in money-laundering relate to any offence specified under paragraph 2 of Part A of the Schedule to the PMLA, shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to ten years and shall also be liable to fine.

(c) The Director or any person aggrieved by an order made by the Adjudicating Authority under this Act may prefer an appeal to the Appellate Tribunal. An appeal has to be filed within forty-five days from the date of receipt of a copy of the order made by the Adjudicating Authority. Appellate Tribunal may entertain an appeal after the expiry of the period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Appellate Tribunal to him on any question of law or fact arising out of such order. Thus, an appeal can be filed before High Court on any question of law or fact. High Court may if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

Solved Questions:

1. What are the key laws governing anti-money laundering activities in India?

Solution:

The Prevention of Money Laundering Act, 2002 ("PMLA") along with the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("Rules") are the principal laws enacted to prevent money laundering activities in India. Specialised authorities are dealing with money laundering issues such as the Reserve Bank of India / Securities and Exchange Board of India("SEBI") / Insurance Regulatory and Development Authority of India which also prescribe guidelines on anti-money laundering standards based on PMLA and Rules.

2. What do the SEBI / IRDAI guidelines cover?

Solution:

SEBI has introduced 'Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries' and IRDAI has introduced 'Guidelines on Anti Money Laundering programme for Insurers'. They are sector-specific based on the principles of PMLA and Rules.

3. What is the extent of applicability of PMLA and the Rules?

Solution:

The PMLA and rules apply to all persons which include individuals, a company, a firm, an association of persons, or a body of individuals (incorporated or otherwise), and any agency, office, or branch owned or controlled by any of the above persons.

4. What is money laundering?

Solution:

Money laundering is the processing of criminal proceeds i.e., profits generated from criminal acts, to disguise their illegal origin. For example, embezzlement, insider trading, bribery, computer fraud schemes, illegal arms sales, smuggling, and the activities of organized crime can produce large profits and create the incentive to legitimize the ill-gotten gains through money laundering.

5. What constitutes an offence of money laundering under the PMLA?

Solution:

Any person who directly or indirectly attempts to indulge or knowingly assists or is involved in any activity connected with the proceeds of crime is guilty of the offence of money laundering. Further, concealment, possession, acquisition or use, and projecting or claiming it as untainted property, of such proceeds of crime, in any manner is also an offence under the provisions of PMLA.

6. What are the proceeds of crime?

Solution:

Any property obtained directly or indirectly through a criminal activity relating to a scheduled offence constitutes proceeds of crime. The value of such property or its equivalent value held within the country or abroad are also considered to be proceeds of crime.

7. What does 'property' mean? Are intangible assets also included?

Solution:

Under PMLA, 'property' means any property/assets of every description, corporeal or incorporeal, movable or immovable, tangible or intangible, and includes deeds and instruments evidencing title/interest in the property/ assets wherever located and includes any kind of property used in the commission of an offence under PMLA.

8. What is a 'scheduled offence'?

Solution:

There is a list of offences provided under a schedule in the PMLA. These offences are called scheduled offences. The schedule consists of three parts specifying offences from thirty legislations. Some of the major legislations covered in the schedule include Indian Penal Code, 1860, Narcotic Drugs and Psychotropic Substances Act, 1985, Explosive Substances Act, 1908, Unlawful Activities (Prevention) Act, 1967, Arms Act, 1959, Wild Life (Protection) Act, 1972, Prevention of Corruption Act, 1988, the Companies Act, 2013 and the Customs Act, 1962.

9. What is the punishment for the offence of money laundering?

Solution:

The PMLA prescribes rigorous imprisonment for at least 3 (three) years which may extend up to 7 (seven) years and also a fine. In the event that the offence of money laundering is related to the Narcotic Drugs and Psychotropic Substances Act, 1985, the rigorous imprisonment may extend up to 10 (ten) years.

If an offence of money laundering is committed by a company, then every person in charge of and responsible for the conduct of the business of the company at the time of such contravention as well as the company will be deemed to be guilty and will be liable to be proceeded against and punished accordingly.

10. Which Authorities Regulate the PMLA?

Solution:

The Directorate of Enforcement in the Department of Revenue, Ministry of Finance is responsible for investigating offences of money laundering. The Financial Intelligence Unit - India ("FIU-IND") under the Department of Revenue, Ministry of Finance is the central national agency responsible for receiving, processing, analysing, and disseminating information relating to suspected financial transactions to enforcement agencies and foreign FIUs.

11. What are the compliances/obligations prescribed under PMLA and the Rules?

Solution:

Every banking company, financial institution, intermediary, or a person carrying on a designated business or profession ("Reporting Entity") is required to verify the identity of their clients and the beneficial owner, maintain records of all transactions and documents evidencing identity of its clients as well as beneficial owners and periodical furnishing of information related to certain transactions.

12. Who is covered under "persons carrying on a designated business or profession"?

Solution:

This expression includes : (a) a person carrying on activities for playing games of chance for cash or kind, and includes such activities associated with the casino; (b) inspector-general of registration appointed under the Registration Act, 1908; (c) real estate agent engaged in providing services about sale or purchase of real estate and having annual turnover of INR 2,000,000 or above; (d) dealer in precious metals, precious stones, and other high-value goods if they engage in any cash transactions with a customer equal to or above INR 1,000,000 carried out in a single operation or in several operations that appear to be linked; (e) a person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, as notified by the central government; or (f) a person carrying on such other activities as notified by the central government from time to time.

13. Is there a standard or a procedure required to be followed for verification of the client by the Reporting Entity?

Solution:

Every Reporting Entity is required to conduct an enhanced client due diligence to take steps to examine the client's ownership and financial positions including the source of funds and the intended nature of the relationship between the transaction parties. The Reporting Entity is required to:

(i) Identify and verify its clients and the beneficial owner (if applicable), obtain information on the purpose and intended nature of the business relationship in case of an account-based relationship. After the commencement of an account-based relationship, the Reporting Entity must file the electronic copy of the client's Know Your Client ("KYC") records with the central KYC records registry. The verification process may be done by relying on a third party as well.

(ii) Verify identity while carrying out the transaction of an amount of INR 50,000 or more or any international money transfer operations.

14. Who is considered a 'beneficial owner'?

Solution:

The beneficial owner for the verification process is as mentioned below:

S. No.	Nature of Client	Description (Beficial Owner)
(i)	Company	Natural person, who acting alone or together has a controlling ownership interest or who exercises control through other means. 'Controlling ownership interest' – ownership of or entitlement ot more than 25% of shares or capital or profits of the company. 'Control' – includes the right to appoint majority of the directors or to control the management or policy decisions such as by virtue of their shareholding or management rights or shareholders agreements or voting agreements.
(ii)	Partnership Firm	Natural person, who acting alone or together has ownership of or entitlement to more than 15% of the property or capital or profits of such association or body of individuals.
(iii)	Unincorporated association or body of individuals	Natural person, who acting alone or together has ownership of or entitlement to more than 15% of the property or capital or profits of such association or body of individuals.
(iv)	Trust	Includes identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

15. What are the records that are required to be maintained by the Reporting Entity? How long do these records have to be maintained?

Solution:

Every banking company, financial institution, intermediary, or a person carrying on a designated business or profession ("Reporting Entity") is required to verify the identity of their clients and the beneficial owner, maintain records of all transactions and documents evidencing identity of its clients as well as beneficial owners and periodical furnishing of information related to certain transactions. The records maintained must contain

information including: (a) the nature of the transactions; (b) the amount of the transaction and the currency in which it was denominated; (c) the date on which the transaction was conducted and (d) the parties to the transaction to enable the Reporting Entity to reconstruct individual transactions.

The information relating to the transaction must be maintained for five years from the date of the transaction between a client and the Reporting Entity. The records relating to the identity of clients and beneficial owners as well as account files and business correspondence must be maintained for five years after the business relationship between a client and the Reporting Entity has ended or the account has been closed, whichever is later.

16. What type of information is required to be furnished by the Reporting Entities and to whom?

Solution:

The information required to be furnished by the Reporting Entities is provided in the table below. This information is required to furnish information to the Director of FIU-IND.

Sr. No.	Description	Due Date
(i)	All cash transactions of the value or more than INR 1,00,000 or its equivalent in foreign currency.	15th day of the succeeding month
	All series. of cash transactions integrally connected to each other which have been valued below INR 1,00,000 or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of INR 1,00,000 or its equivalent in foreign currency	15th day of the succeeding month
(ii)	All cash transactions where forged or counterfeit currency notes of bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions	15th day of the succeeding month
(iii)	All transactions involving receipts by non- profit organisations of value more than INR 1,00,000 or, its equivalent in foreign currency	15th day of the succeeding month
(iv)	All cross-border "wire transfers of the value of more than INR 5,00,000 or its equivalent in foreign currency where erther the origin or destination of fund is in India.	15th day of the succeeding month
(v)	All purchase and sale by any person of immovable property valued at INR 5,00,000 or more that ts registered Py the reporting entity, as the case may be.	15th day of the month succeeding the quarter
(vi)	All suspicious transactions whether or not made in cash	Not later than 7 (seven) working days on being satisfied that the transaction is suspicious

17. What is the format in which the information is required to be furnished by the Reporting Entity?

Solution:

The reporting entity must register itself with FIU-IND using the portal https://finnet.gov.in/. Once the registration is complete, the Reporting Entity can furnish information to Director, FIU-IND online in a standard format prescribed for the purpose.

18. Who is responsible to furnish the information from the Reporting Entity?

Solution:

Every Reporting Entity is required to appoint two officers i.e., Designated Director and the Principal Officer. The Designated Director is required to ensure overall compliance with the obligations under PMLA and Rules. The Principal Officer is responsible for the overall compliance of the Reporting Entity. Accordingly, the Principal Officer is responsible to furnish the information promptly to the Director of FIU-IND.

19. What are the penalties for non-compliance with the client due diligence process, maintenance of records, and reporting obligations of the Reporting Entities?

Solution:

On failure to comply with the diligence, maintenance, or reporting obligations by the Reporting Entities, the Director of FIU-IND may:

1. Issue a warning in writing; or
2. Direct such Reporting Entity or it's Designated Director on the board or any of its employees, to comply with specific instructions; or
3. Direct such Reporting Entity or its Designated Director on the board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or
4. Impose a monetary penalty of not less than INR 10,000 but may extend up to INR 100,000 on such Reporting Entity or its Designated Director on the board or any of its employees for each failure.

20. What is the forum for appeal against the order of the Director of FIU-IND for noncompliance with diligence, maintenance, or reporting obligations?

Solution:

Any reporting entity aggrieved by any order of the Director of FIU-IND may appeal before the appellate tribunal constituted under the Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act, 1976. This appeal must be made within 45 days from the date on which a copy of the order made by the Director of FIU-IND is received.

21. What is a forum for appeal against the order of the appellate tribunal?

Solution:

A person aggrieved by the decision of the appellate tribunal may file an appeal to the High Court within 60 days from the date of communication of the decision of the appellate tribunal to it on any question of law or fact arising out of such decision. The High Court may accept an appeal within a further period of 60 days if sufficient cause for the delay is shown.

22. What is the court of the first instance to try and levy punishment for the offence of money laundering?

Solution:

The central government has designated special courts, in consultation with the Chief Justice of the High Court, for trial and punishment of the offence of money laundering. The list of special courts designated by the central government can be accessed.

23. What is the court of appeal against the order of the special court?

Solution:

An appeal or revision may be made to the High Court within the local limit of the jurisdiction of the special courts.

Exercise

A. Theoretical Questions

Multiple Choice Questions

1. Prevention of Money-Laundering Act, 2002 is?
   (a) Act No.15 of 2003
   (b) Act No.22 of 2003
   (c) Act No.11 of 2003
   (d) Act No.3 of 2003

2. Prevention of Money Laundering Act, 2002 came into force on?
   (a) 1st January 2002
   (b) 1st July 2005
   (c) 1st June 2004
   (d) 1st November 2002

3. "Financial institution" as defined under Section 2(l) of Prevention of Money Laundering Act, 2002 does NOT include? (i) a chit fund company, (ii) a housing finance institution, (iii) a payment system operator, (iv) a non- banking financial company, (v) Department of Posts in the Government of India.
   (a) (v) only
   (b) (iv) only
   (c) (ii), (iv) and (v) only
   (d) None of the above

4. "Payment system" as defined under PMLA Act, 2002 does include? (i) systems enabling credit card operations, debit card operations (ii) smart card operations (iii) money transfer operations
   (a) Only (i)
   (b) Only (iii)
   (c) Only (i) and (iii)
   (d) All the above

5. "Person" as defined under the Prevention of Money Laundering Act, 2002 includes?
   (a) A Hindu undivided family
   (b) Every artificial juridical person
   (c) An association of persons or a body of individuals, whether incorporated or not
   (d) All the above

6. "Precious metal" as defined by PMLA Act, 2002 does not include?
   (a) Gold
   (b) Palladium or rhodium
   (c) Diamond
   (d) Platinum

7. "Precious stone" as defined under PMLA Act, 2002 does not include?
   (a) Diamond
   (b) Graphite
   (c) Emerald
   (d) Sapphire

8. Offence of money laundering is defined in which section of PMLA Act, 2002?
   (a) Section 3
   (b) Section 2
   (c) Section 1
   (d) Section 11

9. "Punishment for money-laundering" is defined under which Section of PMLA Act 2002?
   (a) Section 3
   (b) Section 7
   (c) Section 4
   (d) Section 10

10. Which of the following is not prescribed in the provision of the Prevention of Money Laundering Act, 2002?
    (a) Seizure of property
    (b) Attachment of Property
    (c) Confiscation of Property
    (d) Life Imprisonment

11. Whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to?
    (a) Three Years
    (b) Five Years
    (c) Seven years
    (d) Ten years

12. Whoever commits the offence of money-laundering, which relates to any offence specified under paragraph 2 of Part A of the Schedule, shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to?

    (a) Three Years

    (b) Five Years

    (c) Seven years

    (d) Ten years

13. As per section 5 of PMLA Act, 2002, the property can be provisionally attached for a period not exceeding _____ from the date of the order?

    (a) 60 days

    (b) 90 days

    (c) 120 days

    (d) 180 days

14. Director or any other officer who provisionally attaches any property under PMLA Act, 2002, shall, within a period of days from such attachment, file a complaint stating the facts of such attachment before the Adjudicating Authority?

    (a) Thirty days

    (b) Sixty days

    (c) Forty-five days

    (d) Ninety days

15. Which among the following authority appointed by the Central Government shall exercise jurisdiction, powers, and authority conferred by or under the Prevention of Money Laundering Act, 2002?

    (a) Administrative Authority

    (b) Adjudicating Authority

    (c) Appellate Authority

    (d) Adjudicating Commission

16. By whom FATF was mendated ?

    (a) G4

    (b) G5

    (c) G6

    (d) G7

17. In which year FATF was mendated?
    (a) 1985
    (b) 1986
    (c) 1987
    (d) 1989

18. Till today FATF has come out with how many recommendations?
    (a) 30
    (b) 35
    (c) 40
    (d) 45

19. Which Recommendation of FATF pertains to Customer Due Diligence (CDD)?
    (a) 5
    (b) 7
    (c) 10
    (d) 12

20. Recommendation 20 of FATF states that Financial Institutions should report suspicious transactions to
    (a) RBI
    (b) Ministry of Finance
    (c) SEBI
    (d) FIU

Essay Type Questions

1. What do you mean by "money laundering"? What is the role of RBI in the Prevention of Money Laundering?
2. "Non-adherence of KYC norms can create opportunity for money laundering". Explain.
3. What is meant by pooled accounts?
4. What is meant by KYC Policy?
5. Describe the Customer Acceptance Policy in AML/KYC.
6. Explain the customer identification procedure in AML/KYC.
7. What can be a ground for a transaction to be a suspicious transaction?
8. What do you mean by Money Laundering?
9. What are the objectives of KYC?

10. What are the stages of money laundering?
11. Why is there a need to perform Anti-Money Laundering Checks?
12. What do you understand about money laundering and financial terrorism?

Answer:

⊙ **Multiple Choice Questions (MCQ)**

1.	(a) Act No.15 of 2003
2.	(b) 1st July 2005
3.	(d) None of the above
4.	(d) All the above
5.	(d) All the above
6.	(c) Diamond
7.	(b) Graphite
8.	(a) Section 3
9.	(c) Section 4
10.	(d) Life Imprisonment
11.	(c) Seven years
12.	(d) Ten years
13.	(d) 180 days
14.	(a) Thirty days
15.	(b) Adjudicating Authority
16.	(d) G7
17.	(d) 1989
18.	(c) 40
19.	(c) 10
20.	(d) FIU

Notes