Anti-Money Laundering and Counter Financing of Terrorism

– Guidelines for Cost and Management Accountants

Released in November 2019 by:
Institute of Cost and Management Accountants of Pakistan (ICMA Pakistan)

Contents

Disclaimer

While preparing this Guideline for Cost and Management Accountants, utmost care has been taken to ensure that only authenticated information in shape of acts, regulations and other legislation available from the State Bank of Pakistan (SBP), Financial Monitoring Unit (FMU), Securities and Exchange Commission of Pakistan (SECP) and other relevant organizations are included for purposes of general guidance only. The information provided in this Guideline should, not in any way, be construed as the main source of information on AMT and TF for which the concerned sources be referred. Further, the information provided herein should also not be construed as legal advice or legal interpretation.

ICMA Pakistan and/or its staff do not accept any liability to any party for any loss, damage or costs howsoever arising, whether directly or indirectly, whether in contract or otherwise from any action or decision taken (or not taken) as a result of any person relying on or otherwise using this Guideline or arising from any omission from it.

Executive Summary

The purpose of this Guideline on Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) is to provide guidance and assistance to the Cost and Management Accountants (CMAs) in order to assist their better understanding and effective performance of their statutory obligations under the legal and regulatory framework in force in Pakistan in addition to the international legislation on AML and CFT. The Anti-Money Laundering Act 2010 (the AML Act) is applicable to "Financial Institutions" and "Non-Financial Businesses and Professions" (NFBPs). Financial Institutions and NFBPs are specified as "Reporting Entity" in the AML Act.

In the AML Act "Accountants" are categorized as NFBPs. Further, in accordance with the provisions of the AML Act, every reporting entity shall file with Financial Monitoring Unit (FMU), which is established under the AML Act as an independent decision making authority for the purposes of carrying out responsibilities under the AML Act and housed in State Bank of Pakistan, to the extent and in the manner prescribed by the FMU, Report of Suspicious Transaction conducted or attempted by, at or through such reporting entity, if it knows, suspects or has reason to suspect that the transaction or a pattern of transactions of which the transaction is a part are arising out of proceeding of crime.

The applicability of the AML Act on Accountants outlines risk of money laundering faced by the accountancy profession. This risk originates from the possibility of Accountant's rendering of services to the persons who have proceeds of crime (from the predicate offenses or foreign serious offenses). In the case of money laundering, a predicate offense is an underlying crime that generates the funds to be laundered. The examples of predicate offenses include inter-alia corruption, bribery, fraud, forgery, counterfeiting, kidnapping, and corporate and fiscal offenses. The offenses listed in the Schedule to the AML Act have been declared as predicate offenses.

The implications of money laundering are significant as the AML Act and Anti-Terrorism Act 1997 (the Anti-Terrorism Act) criminalize the offense of money laundering and terrorism financing.

A National Risk Assessment (NRA) has been carried out with respect to money laundering and terrorist threats and vulnerabilities being faced by Pakistan, coordinated and compiled by FMU, which is responsible for coordination among all the stakeholders for facilitating implementation of the AML legislation. This NRA has evaluated amongst others, the vulnerability of accountancy profession and professionals towards money laundering and terrorist financing risks and found no money laundering and/or terrorist financing risks for the accountancy services sector (auditors, accountants or tax advisors) and this sector has been categorized as 'Low Risk'. The awareness building of money laundering and terrorist financing risks and related combating measures and development of guidance material have been noted as the area for action for the accountancy services sector.

Institute of Cost and Management Accountants of Pakistan [ICMA Pakistan], recognizing the significance and relevance of the country's accountancy profession in understanding the exposure to the risks of money laundering and terrorism financing and combating these risks effectively, has developed this Guideline for its members i.e. Cost and Management Accountants (CMAs).

It is noted that the AML Act uses the term "Accountant". However, "Accountant" encompasses professionals, including cost and management accountants (CMAs) and organizations that provide a range of accountancy services to a diverse range of clients. The services may include (but are not restricted to) audit and assurance services, book-keeping, tax compliance, tax advisory, business advisory, management consultancy, and transaction advisory. Due to non-provision of definition / explanation of term Accountant in AML legislation and varied use of term "Accountant" (in general), the explanation of "Accountant" provided in the Financial Action Task Force (FATF) Recommendations (which effectively serve as the global standards on Anti-Money Laundering and Counter Financing of Terrorism (AML and CFT) has been used for the development of this Guideline.

Based on the explanation provided in the FATF Recommendations, not all accountancy sector services are subject to the AML Act. For the purpose of this Guideline, a practicing firm (i.e. a practicing firm of cost and management accountants under the Cost and Management Accountants Act, 1966) and providing services specified/listed in the FATF Recommendations is an "Accountant". The Accountant's services, as specified in the FATF Recommendation include:

- Managing of client money, securities or other assets;
- Management of client's bank, savings or securities accounts;
- Organization 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

Further, in the FATF Recommendations, the activities of trust and company service provider are also listed under the Designated Non-Financial Business or Profession (DNFBP) category, and hence applicable to the practicing firms for AML/CFT compliance.

In this Guideline, the practicing firm of cost and management accountants, based on the above criteria is considered a reporting entity and obligated to fulfill existing requirements of AML legislation. Besides above-specified services, other services of the practicing firm such as auditing, tax consultancy, cost and management accounting services, regulatory compliance services, etc. are not directly subject to AML/CFT legislations. Accordingly, a CMA practicing firm engaged in rendering of these services would not be a reporting entity. The FATF Recommendations, however, strongly encourage countries to extend the reporting requirement to the rest of the professional activities of accountants, including auditing. However, the practicing firm and staff involved in rendering such other services are required to consider and comply the requirements under the respective engagement framework (e.g. International Standards on Auditing as applicable in Pakistan) and Code of Ethics.

The staff of the CMA practicing firm, including partners, are required to ensure compliance with the practicing firm's AML compliance program. They are obligated to report matters internally, whereas the practicing firm being a reporting entity is obligated to ensure compliance with the AML legislation.

The members of ICMA Pakistan employed with different business entities or who are individually carrying out businesses (other than practicing firms) could be subject to AML and CFT requirements. These members of the Institute in business are required to consider and comply with the AML/CFT requirements in the context of their employer (bank, insurance company, mutual funds, etc.), as these businesses are reporting entities under AML Act. These members should follow AML/CFT compliance program of their employers.

A CMA practicing firm can effectively comply with the AML and CFT legislations by formulating and implementing AML/CFT compliance program. The AML/CFT programs will vary for each practicing firm as it should be formulated on a risk-based approach involving professional judgments about how to best manage specific risks. It is critical that the practicing firm's senior management sets the right tone and demonstrates leadership on AML/CFT. The AML Act requires every reporting entity to conduct customer due diligence and maintain the record in accordance with the regulations issued by the regulator of such reporting entity.

The CMA practicing firm that is a reporting entity under AML Act, must submit Suspicious Transaction Reports (STR) to FMU. There is no materiality or de minimis exceptions to reporting under STR. Once an STR has been made, care must also be taken to avoid making any disclosures which could constitute tipping off, which is a criminal offense under the AML Act. Further, the Cash Transaction Reports (CTR) must be filed to FMU when cash-based transactions above PKR 2 million or equivalent foreign currency are carried out by the practicing firm during provision of the specified services.

The reporting provisions of the AML Act have effect notwithstanding any obligation as to secrecy or other restriction on the disclosure of information imposed by any other law or written document. Therefore, CMA practicing firms are obligated to file STR and CTR, irrespective of any other legal confidentiality requirement of other law or written non-disclosure agreement between the client and the practicing firm. The reporting of STR and CTR will not be treated as a breach of client confidentiality.

Under the AML Act, the FMU is mandated to receive and analyze the STRs and CTRs submitted by the reporting entities (including practicing firms). The FMU can further disseminate this information to the investigatory and supervisory authorities (such as Federal Investigation Authority, National Accountability Bureau, Anti-Narcotics Force, Directorate-General (Intelligence and Investigation Inland Revenue) Federal Board of Revenue, etc.) for investigation and legal action. FMU may also refer the matter of non-compliance of AML legislation on the part of Cost and Management Accountants (CMAs) to ICMA Pakistan for further action against such Accountants.

With regard to AML/CFT, a CMA practicing firm is not required to be registered with any agency/regulator, including Financial Monitory Unit (FMU).

Due to their role as gatekeepers and significant adverse implications of money laundering and terrorist financing, it is of utmost importance that CMA practicing firms and their staff are familiar with the risks of money laundering and terrorist financing originating from their services and take necessary measures to combat these risks.

It is hoped that this publication meets its objectives of assisting and facilitating all stakeholders, especially CMA practicing firms and their staff in understanding and complying the requirements of AML and CFT legislation

1. Preamble

1.1 Objectives

The primary objective of framing and implementing the AML/CFT legislations are to prevent, identify, report and investigate the Money laundering (ML) and Terrorism Financing (TF). Pakistan AML and CFT legislations are intended to raise the confidence level of global community on the country's financial systems.

In general, the roles and associated risks (including the risks of ML and TF of different sectors), professions and professionals are usually specific and separate. In consideration of these business/sector specific ML and TF risks, the globally recognized AML and CFT standards (i.e. Financial Action Task Force (FATF) Recommendations) outline activities-based AML/CFT scope and approach. This implies that certain identified businesses, professions, and professionals (when undertaking specified activities) are included in the scope of AML/CFT standards. To mitigate the AML/CFT risks arising from the nature of the products, activities or services of these businesses, professions, and professionals, they are obligated to take measures to combat the risk of ML and TF.

The accountancy profession is considered as one of the main professions in combating ML and TF, both locally and internationally. Effective systems and controls can help the professionals and organizations to detect, prevent and deter financial crime, including ML and TF.

The 'Accountants' [also including cost and management accountants] are one of the professional service providers that are covered in the scope of global AML and CFT standards. Further, the Pakistan AML/CFT regime (which scopes in certain businesses and professions, in accordance with the FATF Recommendations) also includes 'Accountants' as one of the professional service providers obligated with the AML requirements.

Institute of Cost and Management Accountants of Pakistan [ICMA Pakistan] in consideration of the significance of AML and CFT requirements for the Accountants has prepared this Guideline titled "Anti-Money Laundering and Counter Financing of Terrorism – Guideline for Cost and Management Accountants ("The Guideline").

The primary purpose of this Guideline is to facilitate ICMA Pakistan members, practicing firms of ICMA Pakistan and other related stakeholders to:

- Assist in understanding the accountant related scope and requirements of Pakistan's AML / CFT legislation and the FATF Recommendations;
- Outline the responsibilities of the accountants flowing from Pakistan's AML/CFT legislation and the FATF Recommendations and provide a high-level approach to fulfill these AML and CFT requirements effectively; and
- Summarize the suspicious reporting and currency reporting requirements under the AML legislation.

1.2 Scope

The AML Act is applicable to a number of different business sectors and professionals, including Accountants [including cost and management accountants]. These different business sectors and professionals are termed as 'Reporting Entity" under the AML Act. The AML Act classifies the Accountants in the "Non-Financial Business or Profession" (NFBP) category. NFBP being reporting entity have compliance obligations under the AML Act.

This Guideline is for the Accountants [including the Cost and Management Accountants] who are reporting entities and consequently have obligations under the AML Act.

Generally, the term 'Accountant' has a broader meaning and significantly varied usage. The AML Act and underlying rules and regulations neither provide a definition/explanation of the term 'Accountant' nor specify the activities/services which are subject to the compliance requirements of the AML legislation.

However, the FATF Recommendations (considered as global AML and CFT standards) contain an explanation of the term 'Accountant', as it lists the activities/services conducted by the Accountants that fall within the scope of AML/CFT compliance requirements. For purposes of this Guideline, the definition/ explanation of 'Accountant' and related in scope activities contained in the FATF standards (i.e. the FATF Recommendations and related glossary of terms) have been used.

In this Guideline, as a substitute to the term 'Accountant' following terms have been used:

- 'Practicing firm' to refer to the firm of cost and management accountants under the Cost and Management Accountants (CMA) Act, 1966; and

- 'Member' to refer to the member of ICMA Pakistan under the CMA Act, 1966.

The practicing firms and Institute's members conduct a range of professional services and activities.

Practicing firm

Under the AML legislation, the practicing firm would be the "Accountant" and thereby the reporting entity. However, not all practicing firms would be in the scope of AML legislation. The determining factor will be whether one or more of a number of specific activities (mentioned in the FATF Recommendations) are conducted by the practicing firm. These activities are described in the FATF Recommendation 22 Guideline "**Designated Non-Financial Business or Profession" (DNFBP)** and include:

- buying and selling of real estate for a client;
- managing of client money, securities or other assets;
- managing of client's bank, savings or securities accounts;
- organizing of contributions for the creation, operation or management of companies;
- creating, operating or managing legal persons or arrangements, and buying and selling business entities

Further, in the FATF Recommendations, the activities of trust and company service providers are also listed under the DNFBP category.

A practicing firm carrying out the above activities, including activities of trust and company service provider would be subject to AML and CFT compliance requirements. The Pakistan AML regulatory regime and the FATF Recommendations have been discussed in section 2 of this Guideline.

In the above backdrop, it is understood that AML Act and underlying rules and regulations are applicable to the practicing firms when conducting the above-mentioned activities, including that of trust and company service providers. These services/ activities, including that of trust and company service provider, are referred to in this Guideline as "specified services". The specified services have been further explained in section 3 of this Guideline.

For the purpose of this Guideline, specified services include any service provided under a contract for services (i.e. not a contract of employment).

Based on the above-specified services, outlined in the FATF Recommendations, the activities of practicing firm (other than the specified services) such as audit of financial statements carried out according to the International Standards on Auditing (ISAs) as applicable in Pakistan or tax consultancy services are not subject to AML Act and underlying rules and regulations.

Members of ICMA Pakistan in Business

As explained earlier, the AML scope and requirements are activities-based. Besides, Accountant's various other businesses and professions (such as financial institutions, insurance providers, lawyers, jewelers, etc.) are also subject to the requirements of AML legislation.

The members of ICMA Pakistan who are employed with different entities or who individually carry out businesses (other than practicing firms) could be subject to AML requirements. It is necessary that these members know about the scope of AML and CFT legislation and their responsibilities thereunder. ICMA Pakistan's members in their capacity as employees of other businesses are not reporting entities under the AML legislation. However, members should learn about the applicability of AML legislation on their business/employer, AML / CFT processes, systems and protocols (established by the employer and whether there is a designated AML compliance officer, and to whom to consult or what to do if coming across with ML / TF activities.

1.3 Contents of the Guideline

The Guideline has been organized in the following sections:

1. Preamble – Explains the objectives, scope, and content of the Guideline;

2. Regulatory Regime in Pakistan on AML / CFT – Provides an explanation of money laundering and terrorist financing, lists Pakistan's regulatory AML / CFT related laws, outlines the requirements for AML law related to accountants and overview of the FATF recommendations related to the DNFBP, including accountants;

3. AML / CFT requirements applicable on practicing firms – Describes the AML / CFT requirements applicable to the practicing firms engaged in the specified activities/services

4. Risk-Based Approach (RBA)– Explains the rationale and purpose of risk-based approach for AML / CFT system and procedures, lists responsibilities in relation to the risk-based approach, summarizes the categories of ML /TF risks and outlines the methodology for the accountants;

5. Customer Due Diligence (CDD) – Explains the rationale and purpose of CDD, the timing of CDD, the categories of CDD and its use of these in varied circumstances, sources of CDD and guidance on failure in performing CDD;

6. Reporting of suspicious activity to FMU – Outlines the practicing firms' responsibilities of reporting of suspicious activity to FMU, the possible events scenario triggering such reporting and procedure of reporting;

7. Record keeping – Describes the practicing firm's responsibility for the AML related record maintenance and retention; and

8. Awareness and training – Outlines the requirements related to the training and awareness creation of ML/TF risks and related measures/ controls for AML and CFT.

This Guideline does not provide a "how-to" Guideline or additional prescription to complement the AML Act and other pronouncements. It is recognized that a "one-size-fits-all approach" does not work well for most reporting entities. Instead, this Guideline will assist practicing firms, members of ICMA Pakistan and other stakeholders in creating awareness and enhancing understanding and of AML legislation, ML/TF risks, and in providing high-level guidance for managing the risks and complying with AML and CTF regulatory requirements.

In this Guideline where the terms "must" or "required" are used, this means that the information is referring directly to an obligation that is specified in the legislation. Where the term "should" have been used it is making a recommendation (which is reader/users choose to accept or not).

The FATF Recommendations use the term customer, in general. However, practicing firms typically refer to those benefiting from their services as "clients" rather than "customers", and so that term has generally been used in this Guideline.

This publication is prepared for guidance only and cannot be relied on as evidence of complying with the requirements of the AML legislation. It does not constitute legal advice from ICMA Pakistan and FMU and cannot be relied on as such.

This Guideline may be downloaded from the ICMA Pakistan website: www.icmap.com.pk

2. Regulatory Regime in Pakistan on AML / CFT

2.1 What is money laundering and terrorist financing?

Generally, money is the foremost reason for engaging in any type of criminal activity. ML is the method by which criminals disguise or attempt to disguise the illegal origins of their wealth and protect their asset bases, so as to avoid the suspicion of law enforcement agencies and prevent leaving a trail of incriminating evidence.

Terrorists and terrorist organizations also rely on money to sustain themselves and to carry out terrorist acts. Money for terrorists is derived from a wide variety of sources. Generally, terrorists are not greatly concerned with disguising the origin of money, they are concerned with concealing its destination and the purpose for which it has been collected. Terrorists and terrorist organizations, therefore, employ techniques similar to those used by money launderers to hide their money.

For the purpose of this Guideline, ML is also taken to encompass activities relating to TF, including handling or possessing funds to be used for terrorist purposes as well as proceeds from terrorism.

Appendix A of this document explains some common money laundering methods.

2.2 What is the AML regulatory regime in Pakistan?

Pakistan introduced the first standalone Anti Money Laundering law in September 2007 through promulgation of Anti-Money Laundering Ordinance 2007. This was followed by Anti-Money Laundering Ordinance 2009 and Anti-Money Laundering Act 2010.

Presently, the Pakistan AML/CFT regime is contained in the following legislations:

- The Anti-Money Laundering Act 2010 (AML Act)
- The Anti-Terrorism Act 1997
- The Anti-Money Laundering Regulations 2015
- The Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations 2018

The Securities and Exchange Commission of Pakistan (SECP) issued regulations which are applicable to the SECP regulated entities. Further, SECP has issued Guideline on Implementation of AML/CFT Framework under the AML/CFT Regulations 2018 and the AML/CFT Guideline for Non-Profit Organizations (NPOs). Moreover, the State Bank of Pakistan (SBP) has issued directives on AML/CFT for the banking sector.

In accordance with AML Act, ML includes all forms of using or possessing criminal property (as well as facilitating the concealment, use, possession or attempt to conceal, use or possess) such property.

Further, ML includes all forms of handling or possessing criminal property including facilitating any handling or possession of the criminal property. The AML law criminalizes money laundering and provides a wide range of predicate offenses.

Section 3 of the AML Act explains the offense of money laundering as follows:

*"A **person** shall be guilty of the **offence of money laundering** if the person:*
a) Acquires, converts, possesses, uses or transfers property, knowing or having reason to believe that such property is proceeds of crime;

b) Conceals or disguises the true nature, origin, location, disposition, movement or ownership of property, knowing or having reason to believe that such property is proceeds of crime;

c) holds or possesses on behalf of any other person any property knowing or having reason to believe that such property is proceeds of crime; or

d) Participates in, associates, conspires to commit, attempts to commit, aids, abets, facilitates, or counsels the commission of the acts specified in clauses (a), (b) and (c).

Explanation I- The knowledge, intent or purpose required as an element of an offense set forth in this section may be inferred from factual circumstances in accordance with the Qanoon-e-Shahadat Order, 1984 (P.O. 10 of 1984).

Explanation II- For the purposes of proving an offense under this section, the conviction of an accused of the respective predicate offense shall not be required."
Further, the related definitions of person, property, and proceeds of crime as contained in AML Act are as follows:

- *"**Person** means an individual, a firm, an entity, an association or a body of individuals, whether incorporated or not, a company and every other juridical person."*

- *"**Property** means property or assets of any description, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and includes deeds and instruments evidencing title to, or interest in, such property or assets, including cash and monetary instruments, wherever located."*

- *"**Proceeds of crime** means any property derived or obtained directly or indirectly by any person from the commission of a predicate offense or a foreign serious offense."*

With regard to ML, a predicate offense is an underlying crime that generates the funds to be laundered. The examples of predicate offenses include inter-alia corruption, bribery, fraud, forgery, counterfeiting, kidnapping, and corporate and fiscal offenses. The offenses listed in the Schedule to the AML Act have been declared as predicate offenses.

The Anti-Terrorism Act 1997 lays down the basic legal framework for counterterrorism prosecutions in Pakistan.

Some of the AML related sections of The Anti-Terrorism Act 1997 are reproduced below:

"11J. Funding Arrangements

(1) A person commits an offense if he-

(a) enters into or becomes concerned in an arrangement as a result of which money or other property is made available or is to make available to another; and
(b) has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

(2) Any person in Pakistan or a Pakistani national outside Pakistan shall commit an offense under this Act, if he knowingly or willfully makes money or other property or services available, directly or indirectly, wholly or jointly, for the benefit of a proscribed organization or proscribed person."

"11K. Money laundering

A person commits an offense if he enters into or becomes concerned in any arrangement which facilitates the retention or control, by or on behalf of another person, of terrorist property:
a) by concealment;
b) by removal from the jurisdiction;
c) by transfer to nominees; or
d) in any other way.

1) It is a defense for a person charged with an offense under sub-section (1) to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property."

2.3 What is the scope of AML Act and who is a "Reporting Entity"?

The AML Act 2010 (An Act to provide for the prevention of money laundering) extends to whole of Pakistan. The AML Act places compliance obligations on the following two categories:

1. Financial Institutions (FIs)

2. Non-financial businesses and professions (NFBPs)

The Accountants are included in NFBP category.

It is pertinent to note that the FATF in its Recommendations has also differentiated the AML/CFT requirements for the financial institutions and DNFBPs, and the Accountants fall under the DNFBP category.

The AML Act further specifies that the FIs and NFBPs are "Reporting Entities".

Under the AML Act the Reporting Entitles are obligated (including Accountants) to report STRs and CTRs to FMU. Further, reporting entities and their staff are prohibited from disclosing, directly or indirectly, any person involved in the transaction that the transaction has been reported. The record related to STR and CTR must be maintained by the reporting entity for a period of five years in accordance with the provisions of the AML Act.

Moreover, the reporting entities are to conduct customer due diligence (CDD), maintenance of record, account files and documents obtained through such diligence, in accordance with the regulations set out by the regulator of such reporting entities.

The reporting provisions of AML Act have effect notwithstanding any obligation as to secrecy or other restriction on the disclosure of information imposed by any other law or written document. Therefore, under AML Act practicing firms being reporting entities have been obligated to file STR and CTR, irrespective of any other legal confidentiality requirement of other law or written non-disclosure agreements between the client and the practicing firm.

For AML Act, members may visit the below link:

http://fmu.gov.pk/docs/laws/Anti-Money%20Laundering%20Act%202010-As%20amended%20upto%20May%202016.pdf

2.4 Which is the primary government authority responsible for AML/CFT in Pakistan?

In accordance with AML Act, the **Financial Monitoring Unit** (**FMU)** is the Financial Intelligence Unit of Pakistan. FMU is Pakistan's central agency mandated to receive and analyze the Suspicious Transaction Reports (STRs) and Cash Transaction Reports (CTRs), reported by the reporting entities (including practicing firms).

FMU is also responsible for further disseminate to the investigatory and supervisory authorities, disclosures of financial information concerning suspected proceeds of crime and alleged money laundering offenses and any activities or transactions related to financing of terrorism.

FMU has been established under section 6 (*Financial Monitoring Unit)* of the AML Act. The section is reproduced hereunder:

1) The Federal Government shall, by notification in the Official Gazette, establish a Financial Monitoring Unit which shall be housed in SBP or at any other place in Pakistan.

2) The FMU shall have independent decision-making authority on day-to-day matters coming within its areas of responsibility.

3) A Director General who shall be a financial sector specialist who shall be appointed by the Federal Government in consultation with SBP to head FMU and exercise all powers and functions of the FMU subject to the administrative oversight of the General Committee.

4) *The FMU shall exercise the following powers and perform the following functions, namely:*

a) *to receive Suspicious Transaction Reports and CTRs from financial institutions and such non-financial businesses and professions as may be necessary to accomplish the objects of this Act;*

b) *to analyze the Suspicious Transaction Reports and CTRs and in that respect, the FMU may call for record and information from any agency or person in Pakistan related to the transaction in question. All such agencies or persons shall be required to promptly provide the requested information;*

c) *to disseminate on a confidential basis, after analyzing the Suspicious Transaction Reports, and CTRs and other records, necessary information or materials to the concerned investigating or prosecuting agencies for inquiry or other action under this Act or any other applicable law;*

d) *to create and maintain a database of all Suspicious Transaction Reports and CTRs, related information and such other materials as the Director-General determines are relevant to the work of the FMU and in that respect, the FMU is authorized to establish necessary analytic software and computer equipment to effectively search the database, sort and retrieve information and perform real-time linkages with databases of other agencies both in and outside Pakistan as may be required from time to time;*

e) *to co-operate with financial intelligence units in other countries and to make reciprocal arrangements after the due administrative process to share, request and receive information relating to money laundering and financing of terrorism;*

f) *to represent Pakistan at all international and regional organizations and groupings of financial intelligence units and other international groups and forums which address the offense of money laundering and other related matters;*

g) *to submit to the General Committee and the National Executive Committee the reports including an annual report containing overall analysis of the Suspicious Transaction Reports and CTRs, statistics concerning the investigations and prosecutions conducted in relation to the offences of money laundering and financing of terrorism in Pakistan and recommendations on countermeasures to combat money laundering and financing of terrorism. In this behalf, FMU may call periodic reports from the investigating and prosecuting agencies in such manner as may be specified by FMU;*

h) *to frame regulations in consultation with SBP and SECP for ensuring receipt of Suspicious Transaction Reports and CTRs from the financial institutions and non-financial businesses and professions with the approval of the National Executive Committee;*

i) *to recommend to the regulatory authorities of reporting entities to issue regulations as considered necessary in the context of combating money laundering and financing of terrorism, including customer due diligence and ancillary record-keeping.*

j) *to enter into arrangements with domestic agencies and authorities or engage a financial institution or an intermediary or such other non-financial businesses and professions or any of its officers as may be necessary for facilitating the implementation of the provisions of this Act, the rules or regulations made thereunder; and*

k) *to perform all such functions and exercise all such powers as are necessary for, or ancillary to, the attainment of the objects of this Act.*

5) On considering suspicious transaction report or CTR the FMU may, if deems necessary, convey matters involving regulatory or administrative action to concerned regulatory or administrative body for appropriate action.

6) Subject to the regulations sanctioned by the National Executive Committee in this behalf, the Director-General may, if there appear to be reasonable grounds to believe that a property is a property involved in money laundering, order freezing of such property, for a maximum period of fifteen days, in any manner that he may deem fit in the circumstances.

The FMU website can be accessed at http://www.fmu.gov.pk/

Coordination, cooperation and use of the financial intelligence are strong points of an effective AML/CFT framework. The AML Act also defines investigating or prosecuting agency. In accordance with AML Act, the other major government law enforcement agencies (LEAs) with their distinct mandate/jurisdiction to conduct investigation and prosecution of money laundering / terrorist financing cases include:

1. Federal Investigation Authority (FIA);
2. National Accountability Bureau (NAB);
3. Anti-Narcotics Force (ANF);
4. Directorate General (Intelligence and Investigation Inland Revenue) Federal Board of Revenue; or
5. Any other law enforcement agency as may be notified by the Federal Government for the investigation or prosecution of an offense under the AML Act.

Further, different organizations and institutions are involved in the supervision of the entities in the supervision of the AML and CFT in Pakistan. For example, The State Bank of Pakistan (SBP) supervises financial institutions. SECP supervises the corporate entities, whereas ICMA Pakistan is mandated to regulate the cost and management accountancy profession in Pakistan i.e. practicing firms.

2.5 What is the Financial Action Task Force?

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by G-7 countries (Initially to examine and develop measures to combat ML. In 2001, FATF expanded its mandate to incorporate efforts to combat TF). FATF currently comprises 35 member jurisdictions and 2 regional organizations.

The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is a “policy-making body” which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

The FATF monitors the progress of its members and other jurisdictions in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures (termed as FATF Recommendations) globally. In collaboration with

other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

2.6 What are the FATF Recommendations?

The FATF has developed international standards on combating money laundering and the financing of terrorism & proliferation. These are termed as "The FATF Recommendations". The FATF Recommendations are implemented at the national level through legislation and other legally binding measures.

The FATF Recommendations were for the first time issued in 1990. Subsequently, the FATF Recommendations were revised in 1996, 2001, 2003 and most recently in 2012 to ensure that these remain up to date, globally relevant and applicable.

The FATF 40 Recommendations (along-with their Interpretive Notes and Glossary) provide a complete set of counter-measures against ML and TF covering the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation.

The FATF Recommendations set out the essential measures that countries should have in place to:

- identify the risks, and develop policies and domestic coordination;
- pursue money laundering, terrorist financing and the financing of proliferation;
- apply preventive measures for the financial sector and other designated sectors;
- establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures; enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and
- facilitate international cooperation.

Accordingly, these recommendations set out the principles for action and allow countries a measure of flexibility in implementing these principles according to their particular circumstances and constitutional frameworks.

2.7 What is Asia/Pacific Group on Money Laundering?

Asia/Pacific Group on Money Laundering (APG), a FATF Style Regional Body (FSRB), is an inter-governmental organization, consisting of 41 member jurisdictions. APG is an associate member of FATF.
Pakistan is a member of APG.

APG is focused on ensuring that its members effectively implement the FATF Recommendations against money laundering, terrorist financing and proliferation financing related to weapons of mass destruction.

2.8 What is the National Risk Assessment?

In accordance with the FATF Recommendations, the National Risk Assessment (NRA) is to be carried out by each country, and this is central to the FATF's analysis of the effectiveness of AML/CFT infrastructures.

NRA assists government departments, agencies, regulators and competent authorities to fulfil their mandate with respect to measures to combat ML/TF, as provided for in the legislation. It is a government-wide activity undertaken with the objective to identify, understand and assess the ML and TF risks faced by the country and allocate available resources to control, mitigate, and eliminate risks.

In Pakistan, the FMU is the central agency responsible to carry out the NRA in coordination and consultation with all the stakeholders. FMU initiated the Pakistan NRA in 2015 as per World Bank methodology. Based on the NRA, Pakistan's ML/TF risk profile is mainly impacted by the following risk factors:

- Corruption
- Drug trafficking
- Smuggling, including human smuggling
- Tax evasion

Further, being DNFBP, Accountants, Auditors and Tax Advisors have been evaluated and considered as to their vulnerability towards ML & TF risks.

The NRA has categorized "Accountants, Auditors and Tax Advisors" as '**Low Risk'** as no significant ML/TF risks have been noted in this sector. However, the NRA Report has identified certain challenges and recommended in certain areas of concern including but not limited to the following:

- There is a need to build awareness of AML/CFT requirements among the practitioners that also include the practicing firms of cost and management accountants. Regular training of the staff of accountancy and audit firms about the AML/CFT measures should be conducted to keep them abreast of the latest developments, global trends and regulatory changes pertaining to AML/CFT.

- Compliance with AML/CFT measures should be adopted as a matter of policy and undertaken by all the staff at the time of their appointment.

- Easy-to-use templates may be developed for compliance with reporting obligations under the AML Act for DNFBPs.

In this respect, ICMA Pakistan is in close liaison with the relevant authorities i.e. FMU and SECP to provide technical assistance to the cost and management accounting community in Pakistan so that they become fully compliant with international standards on AML and CFT.

3. AML / CFT requirements applicable on practicing firms

3.1 Why are Accountants obligated with AML / CFT requirements?

The FATF (which sets international standards to combat ML and counter TF) evaluated money laundering and terrorist financing risks and related vulnerable activities and identified that the services offered/provided by the Accountants involve ML and TF risks.

Generally, the practicing firms of accountants perform the services mentioned for Accountants under the FATF Recommendations. These firms are one of the first professional service providers consulted when businesses are set-up, expanded or diversified. The accountants are also consulted on the regulatory and compliance matters.

Arising from the financial and consultancy nature of work, the practicing firms may have a higher chance of crossing paths with money launders or dealing with illicit funds from money launders. Money launderers may obtain assistance from the practicing firms without practicing firms fully realizing it. (A client may ask an accountant to transfer to and from various bank accounts without giving any reasonable explanation).

In consideration of their role in the business world, it is recognized that the practicing firms and their staff can contribute to the AML cause in a big way. Accordingly, it is crucial for the practicing firms and their staff to be familiar with the risks and crime of ML and TF, and their role to report actual and suspected ML and TF activities.

3.2 Which services of the practicing firm fall in the scope of AML legislation?

Explained in the earlier sections, the AML Act has included "Accountants" in the NFBP category. Consequently, Accountants have compliance obligations with the requirements of AML legislation. In this context, the relevant provisions of AML Act contained in the section clauses (m) and (u) are reproduced hereunder:

2 (m)

"Non-financial businesses and professions" means real estate agents, jewelers, dealers in precious metals and precious stones, lawyers, notaries and other legal professionals, ***accountants****, trust and company service providers and such other non-financial businesses and professions as may be notified by the Federal Government."*

2 (u)

"Reporting entity" means an entity specified in clause (f) or clause (m) and includes any other entity designated as such by Federal Government by notification in the Official Gazette."

Generally, the term 'Accountant' encompasses professionals that provide a range of accountancy services, mainly including:

- Auditors;
- Tax advisors;
- Book-keepers / external accountants;
- Business consultants;
- Management Consultants; and
- Transaction advisory

The definition/explanation of the term 'Accountant' and the details of their specific activities/services falling under the scope of AML regime have not been defined/specified in the AML Act and related Regulations.

In the absence of this fundamental information in AML legislation, FATF Recommendations have been referred for the purpose of this Guideline. The FATF Recommendations require accountants to be regulated for AML/CTF purposes when they prepare for or carry out transactions or activities for their client(s) that have been identified by the FATF as posing high ML/TF risks.

FATF includes Accountants in DNFB category, and defines the DNFB as follows:

"The DNFBP means:

- Casinos
- Real estate agents
- Dealers in precious metals
- Dealers in precious stones
- *Lawyers, notaries, other independent legal professionals, and* ***accountants*** *– this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.*

- *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 in relation to other legal persons;*

  - *providing a registered office, business address or 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."*

Further, FATF Recommendation 22 specifies the following activities of the Accountants which are subject to the AML and CFT requirements:

"Lawyers, notaries, other independent legal professionals and **accountants** *when they prepare for or carry out transactions for their client concerning the following activities:*

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- *organization of contributions for the creation, operation or management of companies;*
- *creation, operation or management of legal persons or arrangements & buying and selling of business entities."*

Based on the above criteria, for the purposes of this Guideline the practicing firms (*sole practitioners, partners or employed professionals within* practicing *firms)* are considered to be subject to the compliance requirements of the AML legislation only when the practicing firm engages in any of the following activities on behalf of any individual or entity, or gives instructions in respect of those activities on behalf of any individual or entity:

- buying and selling of real estate;

- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organization 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
- 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 in relation to other legal persons;
- providing a registered office, business address or 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."

The practicing firm is subject to the requirements of AML Act when engages in the above-mentioned activities, regardless of whether or not any fee is charged to the client or a formal letter of engagement has been obtained. In other words, even if a practicing firm carries out these activities on a volunteer basis, it would be subject to the AML requirements.

The AML outlines an activity-based regime. The FATF Recommendations do not require regulation of activities undertaken by accountants that relate to recording historic transactions for the preparation of financial reports, compliance services provided to clients involving the reporting of historic financial information and the provision of assurance services in relation to financial reports. However, some of these activities, for example, auditing activity, may place accountants in a position to identify suspicious matters.

3.3 What are common examples of 'specified services'?

Some of the common examples of the specified services could be:

Managing client funds, accounts, securities, or other assets

The CMA practicing firm is engaged in managing payments to or from its clients' accounts as a specified service; and, with the exception of payments for professional fees, any instance where the practicing firm receives or holds client funds and controls the payment of those funds will also be specified service.

The key determining factor is whether the practicing firm has control over the flow of funds (if it has the control then the activity is specified service).

Managing client funds, accounts, securities, or other assets

Taking a payroll situation, for example, if a CMA practicing firm is preparing the vouchers or uploading the payments in the system that are then actioned by the client, in such a case the practicing firm is not controlling the funds, rather client is. However, if the practicing firm is authorizing salary payments from the client's account directly into client staff's personal accounts, then this is a specified service.

Examples of this kind of activity in practice

- The practicing firm has the authority to make payments on behalf of its client's business directly from the client's bank accounts.

- The practicing firm makes investments on behalf of a client in securities and/or other assets using funds from the client's bank accounts which practicing firm has the authority to transfer.

- The practicing firm manages the sale and/or purchase of trust assets for the client using funds from the client's bank accounts which practicing firm has the authority to transfer.

- The practicing firm disburses the funds generated from a company's winding up / liquidation to a creditor in line with the relevant administration requirements.

ML/TF risks associated with this activity

Some people will try to avoid accessing banking services typically used in transactions to obscure the trail of funds changing hands as a means to hide their criminal activities. One way to obscure this trail or to add an appearance of legitimacy is to use the trust accounts or other professional services of accountants.

Acting as a formation agent for legal persons or legal arrangements

This activity refers to forming a legal person (such as a company) or legal arrangement on behalf of a client; for example, registering a company with the SECP. The activity does not include instances where the CMA practicing firm simply provides advice about the formation of a legal person that is acted on by either the client themselves or a third party. In the case of forming a company, if client asks a lawyer to get the company registered in accordance with the practicing firm's advice, the specified service would be undertaken by the lawyer and they would have to apply their AML/CFT compliance program to that activity/ service.

Examples of this kind of activity in practice

- Incorporation / Registration of a company with the SECP on behalf of a client.
- Incorporation of an entity (partnership/firm/society/company etc.) on behalf of a client.

ML/TF risks associated with this activity

When a CMA practicing firm is engaged to register a company or partnership, the actual ownership of the company or partnership being formed may be concealed or obscured; for example, where shell companies, multiple layers of ownership, or other complex legal structures are used. Setting up a trust can also be a way to create a perception of distance between assets and their beneficial owners. Further, international evidence shows that criminals use charitable organizations (such as incorporated societies and charitable trusts) to launder their money or to finance terrorism.

Providing an office or address for a company or legal arrangement

A CMA practicing firm which, in ordinary course of business, provides a registered office or a business address, a correspondence address, or an administrative address for a company, or a partnership, or for any other legal persons or arrangement, is a specified service. The only exception to this is where the office or address is provided solely as an ancillary service to the provision of other services that are not otherwise specified services.

Examples of this kind of activity in practice

The CMA practicing firm allows a company or sole trader to use its business address as its registered office address but the practicing firm does not provide them with any other services.

ML/TF risks associated with this activity

For a person who is intent on laundering money or committing other crimes, the use of an address that is not their physical location is appealing. It allows them to keep anonymity and distance from the transactions and activities they are undertaking, and if it is the address of a practicing firm, it adds a perception of legitimacy to their activities. It also makes it more difficult for law enforcement to track them down in person.

Giving advice to a client, in the context of an accountant-client relationship, is not considered providing instructions, and therefore is not considered to be a specified service.

If, after considering the AML Act, the related rules and regulations, FATF Recommendations and this Guideline, a member of the Institute or practicing firm is unsure as to whether they are a reporting entity, they should contact FMU and/or seek independent professional advice.

3.4 Whether the AML Act captures the auditing and other assurance services?

The AML and CFT legislations do not provide a definition/ explanation of the term “Accountant”.

In the FATF Recommendations, the auditing and other assurance services are not amongst the specified services. Consequently, it is considered that the practicing firm carrying out such services will not be a reporting entity under the AML Act. It is not be required to apply the AML/CFT compliance measures under the AML Act to clients who are only requesting other than specified services. However, as part of audit client acceptance and retention process in accordance with Code of Ethics and ISAs, necessary information should be obtained and documented.

Further, in accordance with ISAs as applicable in Pakistan, the auditor is not required to detect or seek non-compliances and illegal activities.

In accordance with ISAs as applicable in Pakistan, the practicing firm has substantial responsibilities once a significant non-compliance with the Law including ML / TF activities has been identified. In this context, the practicing firm being an auditor may be required to perform additional procedures, discuss the matter with those charged with governance, consider communication/reporting mode of the matter (auditors report, etc.) and decide on continuing the engagement. Further, the practicing firm should consider its obligations to report that activity to the relevant regulator such as FIA, FBR, etc. However, no reporting obligation to FMU arises as the audit and assurance services are not specified services.

It is pertinent to note that the FATF under its Recommendation 23 strongly encourages countries to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

3.5 What are the AML / CFT requirements for the practicing firm?

The practicing firm has obligations under the AML Act if it is a 'reporting entity', i.e. if it is providing the earlier mentioned specified services.

Under the AML Act (*section 7(7)*) every reporting entity would be required to conduct CDD and maintain the record, in order to prevent activities related to ML and TF. The CDD and record maintenance shall be in accordance with the regulations prescribed by the regulator of the reporting entity.

Relevant sub-section of section 7 of AML Act is reproduced as under:

"Every reporting entity shall, in accordance with the regulations issued by the relevant regulatory authority of that reporting entity, conduct customer due diligence and maintain record of transactions, account files, and documents obtained through such diligence."

Further, section 7 of AML Act addresses the reporting of suspicious transactions by the reporting entity to FMU. Accordingly, a practicing firm that is subject to the AML Act is required to report actual or suspected transactions involving ML to FMU.

"Every reporting entity shall file with FMU, to the extent and in the manner prescribed by the FMU, Report of Suspicious Transaction conducted or attempted by, at or through such reporting entity, if it knows, suspects or has reason to suspect that the transaction or a pattern of transactions of which the transaction is a part-

a) involves funds derived from illegal activities or is intended or conducted in order to hide or disguise proceeds of crime;

b) is designed to evade any requirements of this section

c) has no apparent lawful purpose after examining the available facts, including the background and possible purpose of the transaction; or

d) involves financing of terrorism, including fund collected, provided, used or meant for, or otherwise linked or related to, terrorism, terrorist acts or organizations and individuals concerned with terrorism:

Provided that Suspicious Transaction Report shall be filed by the reporting entity with the FMU immediately, but not later than seven working days after forming that suspicion."

Moreover, section 7(1) of AML Act requires that "*All CTRs shall, to the extent and in the manner prescribed by the FMU, be filed by the reporting entities with the FMU immediately, but not later than seven working days, after the respective currency transaction."*

In case of failure to meet obligations under the AML Act, civil penalties or criminal sanctions can be imposed on the business and any individuals deemed responsible.

For the employee of a practicing firm, the requirements of CDD, record maintenance, reporting of suspicious and currency transactions mentioned in the AML Act are at the practicing firm level (as it is a reporting entity). The employee should ensure that he/she fulfills the obligations in accordance with the AML/CFT program and related policies, established by the practicing firm.

It is relevant to note that pursuant to section 453 of the Companies Act 2017 "Officers" (director, chief executive, chief financial officer, company secretary or another authorized officer) of all companies are bound to check commission of fraud and money laundering including predicated offenses under the AML Act.

3.6 How can practice firms comply with the AML/CFT obligations effectively?

The AML Act and related regulations (with regard to Accountants) do not contain specific requirements and guidance relating to the AML policies, procedures and controls.

However, the FATF Recommendations (through recommendation no. 22 *"DNFBPs: Customer Due Diligence"*) require inter-alia the customer (client) due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to the DNFBPs, which include the practicing firms.

The above-mentioned FATF Recommendations are listed below:

- **Recommendation 10 - *The Customer due diligence***
- **Recommendation 11 - *Record keeping***
- **Recommendation 12 - *Politically exposed persons***
- **Recommendation 15 – *New Technologies***
- **Recommendation 17 – *Reliance on third parties***

The practicing firm should also consider Recommendation 23 - ***DNFBPs: Other measures.*** Pursuant to which the requirements set out in Recommendations 18 to 21 apply to all DNFBPs, including practicing firm.

- **Recommendation 18 - *Internal controls and foreign branches and subsidiaries***
- **Recommendation 19 - *Higher-risk countries***
- **Recommendation 20 - *Reporting of suspicious transactions***
- **Recommendation 21 – *Tipping-off and confidentiality***

Further, the Cost and Management Accountants (CMAs) should also consider the implications of **Recommendation 6** ***(Targeted financial sanctions related to terrorism and terrorist financing)*** and **Recommendation 7** ***(Targeted financial sanctions related to proliferation)*** on their existing and future business relationships.

To address the ML and TF risks, comply with AML/CFT legislation and meet the requirements emanating from above-mentioned provisions of the FATF Recommendations, the practicing firm should develop a program to combat the risk of ML and TF.

The type and extent of the measures adopted by the practicing firm as part of its program should be appropriate having regard to the risks of ML and TF and the size, complexity, and nature of its business.

The AML program should contain systems and controls capable of:

1. Assessing the ML and TF risks that the practicing firm reasonably expects to face in the course of its business;

2. Developing, establishing and maintaining internal policies, procedures, systems, and controls to prevent and detect ML and TF. These should cover the following:

- CDD measures and ongoing monitoring;
- record-making and retention;
- the detection of suspicious transactions;
- the internal and external reporting obligations; and
- the communication of policies, procedures, systems, and controls to firm's officers and employees.

3. Training, covering the record maintenance protocols and an appropriate ongoing training program for its officers and employees

Risk assessment

The CMA practicing firm should assess the ML and TF risks that they may reasonably expect to face in the course of its business. In making this assessment, the practicing firm is to consider:

- the nature, size, and complexity of its business
- the services it offers
- the methods by which it delivers services to its clients
- the types of clients it deals with
- the countries it deals with
- any guidance material produced by FMU/FATF/ICMA Pakistan
- any other factors that are set out in AML legislation

The CMA practicing firm also needs to consider whether any of their services involve new or developing technologies that may favor client anonymity.

AML compliance program

An AML/CFT program sets out the internal policies, procedures, and controls to detect ML and TF and to manage and mitigate the risks of it occurring. The program should be in writing and be based on its risk assessment. In this context, establishing and implementing a comprehensive and effective compliance program is the basis for meeting the practicing firm's reporting, record-keeping, client identification, and CDD requirements. Accordingly, an approved and documented compliance program will serve as the basis of meeting all obligations under the AML/CFT Acts and associated regulations.

Risk-based systems and controls should be based on the nature, size and complexity of the practicing firm's business, along with any ML and TF risks it may face.

The risk-based approach means that the practicing firm should assess the risks it is exposed to from money launderers and terrorist financiers in relation to the activities/services being performed. *The risk-based approach is explained in detail in **Section 4** of this Guideline*.

Further, the CMA practicing firm should then apply suitable policies, procedures, and controls to effectively manage the risks identified for its business. Compliance resources can then be targeted primarily in high-risk areas, which should reduce the overall compliance cost.

The range of policies, procedures, and controls reporting entities on the following topics need to be considered:

- Customer due diligence;
- Reporting;
- Record keeping;
- Communication and training.

For a CMA practicing firm, it is important to demonstrate that the required documentation is in place and that employees are well trained and can effectively implement all the elements of the compliance program. As a best practice a senior partner should approve the compliance program and the designated compliance officer (if any) should have the necessary authority to carry out the requirements of the program.

3.7 Whether there is a standardized ('one-fit all') approach to AML/CFT?

There is no one fit all approach. The level of detail and sophistication of the compliance program should reflect the practicing firm's risk of exposure to ML and TF together with the firm's size and structure.

Risk-based systems and controls should be based on the nature, size and complexity of the practicing firm's business, along with any ML and TF risks it may face.

3.8 What is the role of senior management?

The senior management of CMA Practicing firm (by whatever name referred to in a particular firm i.e. senior board of partners, management committee, etc.) is responsible for managing all of the risks faced by the business, including ML and TF risks. Similarly, a sole proprietor is also responsible for managing all of the risks faced by the business, including ML and TF risks.

The level of seniority and degree of engagement that is appropriate will differ based on a variety of factors, including the management structure of the firm and the seriousness of the risk.

Senior management should set the right tone and demonstrate leadership on ML/TF. The senior management of a firm should be responsible for the effectiveness of firm's policies, procedures, systems and controls in preventing ML and TF.

The senior management of a practicing firm should ensure the following:

1) that the firm develops, establishes and maintains effective risk-sensitive AML/CFT policies, procedures, systems, and controls in accordance with the AML Act;

2) that regular and timely information is made available to senior management about the management of the firm's ML and TF risks;

3) that the firm's ML and TF risk management policies and methodology are appropriately documented, including the firm's application of them;

4) that the firm identifies, designs deliver and maintains an appropriate ongoing AML/CFT training program for its officers and employees;

5) that there is at all times a compliance officer or other authorized officer for the firm who has sufficient seniority, experience, and authority and is adequately resourced.

6) that appropriate measures are taken to ensure that ML and TF risks are taken into account in the day-to-day operation of the firm, including in relation to:

    - the development of new services; and
    - the taking on of new clients; and
    - changes in the firm's business profile

The CMA practicing firms should be able to demonstrate that senior management is actively engaged in risk management, for example through sufficient engagement by board and management committees (or any other committee), effective flows of good quality management information and appropriate challenge and escalation of issues as necessary.

Senior management should ensure that ML and TF risks are analyzed, and their nature and severity identified and assessed, in order so as to produce a risk profile. Senior management should then act to mitigate those risks in proportion to the severity of the threats they pose.

In this regard, the respective roles of the senior management in the oversight of risks should be clearly and explicitly defined. The risk analysis should be approved by senior management. This is likely to include formal ratification of the outcomes, including the resulting policies and procedures, but may also include close senior management involvement in some or all of the analysis itself.

In addition, whenever senior management sees that events have affected ML/TF risks, the risk analysis should also be refreshed by an event-driven review. A fresh analysis may require AML policies, controls, and procedures to be amended, with consequential impacts upon, for example, the training programs for relevant employees.

3.9 What is the role of a designated compliance officer?

The senior management can directly oversee the AML/CFT policies and procedures, or it may designate a senior resource as an AML/CFT compliance officer.

The Compliance officer shall be responsible for effectively implementing all of the elements policies and procedures; CDD, record keeping, ongoing training, risk assessment and monitoring the effectiveness, reporting to senior management and reporting to FMU.

In order to implement an effective AML/CFT program the compliance officer needs to:

a) have the necessary authority and access to resources in order to implement an effective compliance program and make any desired changes;
b) have knowledge of practicing firm's business's functions and structure;
c) have knowledge of ML/TF risks and vulnerabilities as well as ML/TF trends and typologies; and
d) understand the legal requirements under the AML legislation.

While the compliance officer is appointed, it is the CMA practicing firm's responsibility to meet its requirements under the AML legislation. Depending on the size of practicing firm, the compliance officer could be:

- a senior partner; or
- someone from a senior level who has direct access to senior management of the firm.

In the case of a sole proprietorship, the sole proprietor can be the compliance officer or may choose to appoint another individual to help implement the compliance program.

The particular responsibilities of the Compliance officer may include:

- receiving, investigating and assessing internal suspicious transaction reports for the firm;
- making suspicious transaction reports to the FMU, on behalf of the CMA practicing firm;
- reporting to the firm's senior management on AML and CFT issues;
- acting as a central point of contact between the firm, and the FMU, and other government authorities, in relation to AML and CFT issues;
- responding promptly to any request for information by the FMU, ICMA Pakistan and other government in relation to AML and CFT issues;
- receiving and acting on government, regulatory and international findings of AML and CFT issues;
- monitoring the appropriateness and effectiveness of the firm's AML/CFT training program;
- exercising any other functions given by senior management, whether under the AML/CFT Law or internal policies.

The role of compliance officer's (or any other officer authorized by the firm to report to FMU) is important in reporting of suspected and currency transactions to FMU. In this regard:

- Any member of staff reports to firm's nominated compliance officer, where they have grounds for knowledge or suspicion that a client or person is engaged in, or attempting, money laundering or terrorist financing;

- the compliance officer should consider each such information, and determine whether it gives grounds for knowledge or suspicion; and

- the compliance officer should report the information on the STR or CTR to FMU.

A compliance officer may choose to delegate certain duties to other employees. However, where such a delegation is made, the compliance officer remains responsible for the implementation of the compliance program.

As a best practice, the compliance officer should have the ability to report compliance-related issues too, and meet with the practicing firm's senior management on a regular basis.

3.10 Where can a practicing firm and member of the Institute can get support and guidance on AML?

Where employees of the CMA practicing firm have compliance questions, their first reference point should be the AML/CFT program. The program documentation should be able to provide answers to basic questions that are likely to arise in the specific business context.

Specific questions should be answered by the firm's designated compliance officer or senior management.

The members of ICMA Pakistan engaged in business should approach and consult their respective employers for consultation and guidance on AML and CFT program and measures. Further, they may consider their individual responsibilities under the AML and CFT legislation and other laws.

The members of ICMA Pakistan and the CMA practicing firms can access support from a range of sources:

- FMU as the AML supervisor
- SBP and SECP being the regulators of financial institutions and companies respectively
- ICMA Pakistan as the Professional Cost and Management Accounting body
- Independent professional advice from legal counsel
- Open-source information from relevant international bodies concerned with AML/CFT

This Guideline is not the only source of guidance and information on ML that can be referred to. The CMA practicing firms are reminded that other guidance issued by FATF, FMU, SECP, SBP, network of firm that may also be relevant and useful.

Appendix C to this Guideline contains a list of some useful and relevant web links.

4. Risk-Based Approach (RBA)

4.1 What is an RBA?

RBA is defined as allocation of resources in accordance with the priorities i.e. risks to the individual/business.

The general principle of a risk-based approach is that where there are higher risks, enhanced measures should be taken to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified and less extensive measures may be permitted.

4.2 Why risk-based approach is relevant in AML/CFT?

In accordance with FATF Recommendations, the risk-based approach is an effective way to combat money laundering and terrorist financing. Therefore, the risk-based approach is central to the effective and efficient implementation AML/CFT system and is essential to properly manage risk.

FATF recognizes that by adopting a risk-based approach, competent authorities, financial institutions and DNFBPs (including CMA practicing firms) should be able to ensure that measures to prevent or mitigate ML and TF are commensurate with the risks identified, and would enable them to make decisions on how to allocate their own resources in the most effective way.

The Expert Working Group advising the FATF on the risk-based approach and FATF Recommendations mentioned that:

"As a basic principle, financial institutions and DNFBPs should be required to take steps to identify and assess their money laundering/financing threat risks for customers, countries or geographic areas, and products/services/transactions/delivery channels. Additionally, they should have policies, controls, and procedures in place to effectively manage and mitigate their risks, which should be approved by senior management and be consistent with national requirements and guidance."

4.3 What is the purpose of a risk-based AML/CFT?

The FATF Recommendations permit to use a risk-based approach to discharging the AML and CFT obligations.

The risk-based approach will enable the CMA practicing firm to subject clients to proportionate controls and oversight by determining:

- the extent of the due diligence to be performed;
- the level of ongoing monitoring to be applied to the relationship, and
- measures to mitigate any risks identified.

Therefore, if applied effectively, the approach would allow the practicing firm to be more efficient and effective in their use of resources and minimize burdens on clients.

A risk-based AML/CFT regime should help ensure that honest clients can access the services provided by practicing firms, but creates barriers to those who seek to misuse those services.

The risk-based approach does not exempt low-risk clients, services, and situations from CDD, however the appropriate level of CDD is likely to be less onerous than for those thought to present a higher level of risk.

4.4 What are the expectations of the practicing firm under the risk-based approach?

It is expected that the CMA practicing firm would be able to identify, assess and understand the ML and TF risks and take commensurate measures in order to mitigate them. In this regard, the RBA approach is an effective way to combat ML and TF. An effective risk-based approach will allow the CMA practicing firms to exercise reasonable business and professional judgment with respect to clients.

Adopting a risk-based approach implies the adoption of a risk management process for dealing with ML and TF. This process encompasses recognizing the existence of the risk(s), undertaking an assessment of the risk(s) and developing strategies to manage and mitigate the identified risks.

Assessing risk

The CMA practicing firm should take appropriate steps to identify and assess its ML and risks (for clients, countries or geographic areas; and products, services, transactions or delivery channels). It should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to the FMU and other authorities. The nature and extent of any assessment of ML and TF risks should be appropriate to the nature and size of the business.

Risk management and mitigation

The CMA practicing firm should have policies, controls, and procedures that enable them to manage and mitigate effectively the risks that have been identified). It should monitor the implementation of those controls and to enhance them, if necessary. The policies, controls, and procedures should be approved by senior management, and the measures are taken to manage and mitigate the risks (whether higher or lower) should be consistent with the requirements and with guidance from the FMU.

Higher risk: Where higher risks are identified the CMA practicing firm should be required to take enhanced measures to manage and mitigate the risks.

Lower risk: Where lower risks are identified, the CMA practicing firm can take simplified measures to manage and mitigate those risks.

A risk-based approach does not prohibit the CMA practicing firms from continuing with legitimate business or from finding innovative ways to diversify their business.

A reasonably designed and effectively implemented risk-based approach will provide an appropriate and effective control structure to manage identifiable ML and TF risks. However, it is also recognized that any reasonably applied controls, including controls implemented as a result of a reasonably designed and effectively implemented risk-based approach, will not identify and detect all instances of ML and TF.

4.5 Why governance and risk culture is fundamental for the effective risk-based approach?

Robust institution-wide risk culture is one of the key elements for effective risk management. This demands a 'Tone at the Top' approach; accordingly, the CMA practicing firm's senior management is responsible for establishing sound business practices and strategic planning. It is therefore of the utmost importance that the senior management in carrying out both its management and supervisory functions has collectively a full understanding of the nature of the business and its associated risks, including ML and TF risks.

The CMA practicing firms should implement a consistent risk culture and establish sound risk governance supported by an appropriate communication policy. Every member of the practicing firm should be fully aware of his responsibilities relating to the identification and reporting of relevant risks (including ML and TF risks).

4.6 How should procedures take account of the risk-based approach?

Before establishing a client, relationship or accepting an engagement a business should have controls in place to address the risks arising from it.

The risk profile of the CMA practicing firm should show where particular risks are likely to arise, and so where certain procedures will be needed to tackle them.

Risk-based approach procedures should be easy to understand and easy to use for all relevant employees who will need them. Sufficient flexibility should be built to allow the procedures to identify, and adapt to, unusual situations. The nature and extent of AML policies, controls and procedures depend on:

- The nature, scale, complexity, and diversity of the business;

- The geographical spread of client operations, including any local AML regimes that apply; and

- The extent to which operations are linked to other organizations (e.g. networking businesses or agencies).

CMA Practicing firms should have different client risk categories (such as: low, normal, and high).

The procedures used for each category should be suitable for the risks typically found in that category. For example, if it is normal for a CMA practicing firm to deal with clients from a high-risk country, the business' procedures for what they regard as normal clients should be designed to address the risks associated with the high-risk country.

Regardless of the risk categorization, a CMA practicing firm is expected to undertake to monitor the client relationship. Such monitoring should be done on a risk-based approach, with levels of monitoring varying depending on the ML/TF risk associated with individual clients.

Taking into account key risk categories, a CMA practicing firm may be able to draw up a simple matrix in order to determine a client's risk profile. Such risk categories may include a client's legal form, the country in which the client is established or incorporated, and the industry sector in which the client operates. In addition, a CMA practicing firm should also consider the nature of the service being offered to a client and the channels through which the services/transactions are being delivered.

Elevated risks could be mitigated by:

- Conducting enhanced levels of due diligence – i.e., increasing the level of CDD that is gathered.

- Carrying out periodic CDD reviews on a more frequent basis.

- Putting additional controls around particular service offerings or clients.

4.7 What are the risk categories?

ML/TF risks can be organized into three categories:

- Geographic risk

- Client risk

- Service risk

4.8 What is a geographic risk?

A CMA practicing firm should consider the following question

"Are our clients established in countries that are known to be used by money launderers or terrorist financiers?"

Geographic risk, in conjunction with other risk factors, may provide useful information as to potential money laundering and terrorist financing risks, though it should be borne in mind that lower risk and legitimate commercial enterprises may be located in high-risk countries.

When determining geographic risk, factors to consider by CMA practicing firm may include:

- High risk and other monitored jurisdictions announced by the FATF from time to time.
- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations ("UN"). In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, maybe given credence by a financial institution because of standing of issuer and the nature of measures.
- Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them.
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

The "Credible sources' refers to information that is produced by well-known bodies that generally are regarded as reputable and 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 well as relevant national government bodies and non-governmental organizations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

Accordingly, in assessing geographic risk associated with a client, consideration may be given to information published by civil society organizations, data available from the UN, the International Monetary Fund, the World Bank, the FATF, the FMU etc. and the CMA practicing firm's experience or the experience of other group entities (where the practicing firms is part of a network) which may have indicated weaknesses in other jurisdictions.

4.9 What is client risk?

For a CMA practicing firm, it is important to consider who clients are, what they do, and any other information that may suggest the client is of higher risk. The following question should be considered,

"Does the client or its beneficial owners have attributes known to be frequently used by money launderers or terrorist financiers?"

Client risk is the overall ML/TF risk posed by a client based on the key risk categories, as determined by a business.

Some clients, by their nature or behavior might present a higher risk of ML/TF. Factors might include:

- The public profile of the customer indicating involvement with, or connection to PEP/s;
- Nature, scope and location of business activities generating the funds/assets (e.g. merchants), having regard to sensitive or high-risk activities. Examples could be:

  - Significant and unexplained geographic distance between the practicing firm and the location of the client.

  - Frequent and unexplained movement of funds between institutions in various geographic locations.

  - Charities and other "not for profit" organizations which are not subject to monitoring or supervision.
- Involvement in cash-intensive businesses;
- The origin of wealth (for high risk clients and PEPs) cannot be easily verified; and
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business and it cannot be easily verified.

Examples of potentially lower risk situations include the following:

- Financial institutions and DNFBPs – where they are subject to requirements to combat ML and TF consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- Public administrations or enterprises.
- A number of client types, industries, activities, professions and businesses, alongside other factors, such as the length of a client relationship, can increase or decrease ML and TF financing risks.

The client's risk profile may also inform the extent of the checks that need to be performed on other associated parties, such as the client's beneficial owners, corporate family tree.

Undue client secrecy and unnecessarily complex ownership structures can both point to heightened risk because company structures that disguise ownership and control are particularly attractive to people involved in ML /TF.

Risks may be inherent in the nature of the activities of the client and the possibility that the activity, transaction and/or related transaction may itself be criminal, or where the business/industrial sector to which a client has business connections is more vulnerable to corruption.

In cases where a client (an individual) or beneficial owner of a client is identified as a PEP, an enhanced level of due diligence should be performed on the PEP. Further details on the approach to be taken in such circumstances are set out in CDD section of this Guideline.

4.10 What is service risk?

An overall risk assessment should also include determining the potential risks presented by services offered by a practicing firm. A CMA practicing firm should consider the following question

"Do any of our services have attributes known to be used by money launderers or terrorist financiers?"

Service risk is the perceived risk that certain products or services present an increased level of vulnerability in being used for ML /TF purposes.

The CMA practicing firm should consider carrying out additional checks when providing a service that has an increased level of ML/TF vulnerability.

Before a practicing firm begins to offer a service significantly different from its existing range of services, it should assess the associated ML/TF risks and respond appropriately to any new or increased risks.

4.11 How can the practicing firm adopt the risk-based approach?

In developing a risk-based approach, the CMA practicing firms need to ensure the adopted approach is readily comprehensible and easy to use for all relevant staff. In cases of doubt or complexity, practicing firms may wish to consider putting in place procedures where queries may be referred to a senior and experienced person for a risk-based decision which may vary from standard procedures.

Adopting a risk-based approach implies the adoption of a risk management process for dealing with ML and TF. This process encompasses recognizing the existence of the risk(s), undertaking an assessment of the risk(s) and developing strategies to manage and mitigate the identified risks.

The CMA practicing firm should:

a) take appropriate steps to identify and assess their risks (for clients, countries or geographic areas; and products, services, transactions or delivery channels).

b) have adequate measures to verify the identity of beneficial owners so that they are satisfied that they know who the beneficial owner is and what the control structure is in respect of a client who is other than a natural person;

c) document the risk assessments in order to be able to demonstrate their basis;

d) keep these assessments up to date; and

e) have appropriate mechanisms to provide risk assessment information to relevant authorities. The nature and extent of any assessment of the risks should be appropriate to the nature and size of the business.

CMA Practicing firm should consider first the type of risk presented:

a) the risk that the client might be located in a country / jurisdiction with high risk of MLTF offences/ breaches

b) the risk that the firm might be used to launder money or provide the means to launder money? Examples might include handling client money, implementing company and trust structures etc.

c) the risk that the client or its counterparties might be involved in money laundering? Examples might include clients who are PEPs, or who are high profile and attract controversy or adverse comment in the public domain, or who are involved in higher risk sectors and jurisdictions (e.g., those where corruption is known to be a higher risk), or who are known to be potentially involved in illegal activities, such as tax evaders seeking advice to resolve their affairs, and certain forensic work connected with fraud or other crime etc.

Consideration of these risk types should enable the CMA practicing firm to draw up a simple matrix of characteristics of the client or service which are considered to present a higher than normal risk, and those which present a normal risk. Some may, by long acquaintance and detailed knowledge, or by their status (e.g. listed, regulated and government entities) be considered to present a lower than normal risk.

This matrix can then be incorporated into client acceptance procedures, and as step 1 of the CDD process.

It is important for the approach adopted to incorporate a provision for raising the risk rating from low or normal to high if any information comes to light in conducting the CDD that causes concern or suspicion.

In all cases, even where they are considered low risk, to assist in effective ongoing monitoring professional firms should gather knowledge about the client to allow understanding of:

- who the client is?
- where required, who owns it (including ultimate beneficial owners)
- who controls the client?
- the purpose and intended nature of the business relationship
- the nature of the client
- the client's source of funds
- the client's business and economic purpose.

However, CMA practicing firms may avail themselves of the opportunity to conduct verification of identity on a simplified basis where the accumulated knowledge of the client is considered sufficient to prove its identity on a risk-sensitive basis without collecting additional documents as might be necessary for a new client considered to present a normal risk.

CMA Practicing firms need to set out clear requirements for collecting Know Your Customer 'KYC' information i.e. CDD about the client and for conducting verification of identity, to a depth suitable to assessment of risk. This Guideline outlines some high-level measures as to how entities/professional firms might approach this.

When assessing risk, CMA practicing firms should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. CMA Practicing firm may differentiate the extent of measures, depending on the type and level of risk for the various risk factors (e.g. in a particular situation, normal CDD could be applied for client acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa). Enhanced CDD shall be applied to clients from higher risk countries for which this is called for by the FATF.

CMA Practicing firm should:

a) have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified;

b) monitor the implementation of those controls and enhance them, if necessary;

c) ensure that the policies, controls and procedures are approved by senior management; and

d) ensure that the measures taken to manage and mitigate the risks are consistent with relevant laws and regulations and this Guideline.

5. Customer Due Diligence (CDD)

5.1 What is CDD?

CDD information comprises the facts about a client that should enable an organization to assess the extent to which the customer exposes it to a range of risks.

It means identification measures taken by the CMA practicing firm of a customer, verifying identity, establishing if the customer is acting on behalf of another person, if the customer is a legal person, establishing the beneficial owner, obtaining information on the purpose and intended nature of business relationship etc. Simply put, a business i.e. a practicing firm should satisfy that it knows with whom it is dealing, and this is done on the basis of the best available information.

5.2 Why is CDD necessary?

FATF Recommendation 10 outlines that CDD measures should be taken and this principle should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or through enforceable means.

Accordingly, CDD measures are a key part of the AML / CFT requirements. Under the AML Act (*section 7(7)*) every reporting entity with regard to the specified service/s shall conduct CDD and maintain the record, in order to prevent activities related to ML and TF.

Relevant sub-section is reproduced as under:

"Every reporting entity shall, in accordance with the regulations issued by relevant regulatory authority of that reporting entity, ***conduct customer due diligence*** *and maintain record of transactions, account files and documents obtained through such diligence."*

The primary objective of CDD is to enable effective identification and reporting of suspicious activities. Accordingly, CDD information is an important element in recognizing whether there are grounds for knowledge or suspicion of ML/TF.

The CDD would enable the practicing firm to form a reasonable belief that they know the identity of each client and, with an appropriate degree of confidence, know the type of business and transactions that the client is likely to undertake and the source and intended use of funds.

5.3 What are stages of CDD?

The CDD stages are as follows:

1. Identifying the client - knowing who the client is and confirming that identity is valid by obtaining documents or other information from sources which are independent and reliable.

2. Identifying the beneficial owners of a client - there could be cases where a beneficial owner who is not the direct client. In these cases, the identification of the ultimate owners or controllers of business and understand the ownership and control is relevant. The focus on identifying and verifying (if they are higher risk) the identity of beneficial owners is not only an important element of CDD, but is also an important factor in an effective risk-based approach to client acceptance.

3. Gathering information on the purpose and intended nature of the business relationship -

In the majority of case for most compliance work undertaken by accountancy professional work, the nature and purpose of the proposed business relationship will be self-evident. However, when more complex or unusual work is involved, more thought needs to be given to this element.

4. Conducting ongoing due diligence on the business relationship and scrutiny of transactions –

Undertaken throughout the course of that relationship to ensure that transactions being conducted are consistent with the entities' knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

The extent of these measures should be determined by using a risk-based approach.

5.4 Who to conduct CDD on?

The CDD shall be conducted on:

- Client
- Any beneficial owner of a client
- Any person acting on behalf of a client

The term 'Beneficial owner' is not defined in the AML Act and related Regulations.

FATF defines it as follows:

"Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement."

Examples of the person acting on behalf of a client include:

- A person exercising a power of attorney for the client
- A legal guardian acting on behalf of a minor who is a client
- An employee who has the authority to act on behalf of a company that is the client

5.5 What are the outcomes of CDD?

The outcomes of CDD include:

- Client identification
- Decision on the acceptance / rejection of the engagement with the client
- Structured and documented CDD data

5.6 When should CDD be carried out?

In accordance with FATF recommendation 10, an accountant (i.e. practicing firm) should apply CDD measures:

- when establishing a business relationship;
- when carrying out occasional transactions:
- when money laundering or terrorist financing is suspected; and
- when there are doubts about a client's identification information obtained previously.

Generally, the CDD process, i.e., obtaining information on the client and beneficial owners, and about the purpose and intended nature of the business relationship, should be completed before establishing any client relationship and/or before carrying out occasional transactions or assignments for occasional clients.

Further, the CDD measures should also be carried out when there is doubt about their veracity or adequacy of previously obtained customer identification data or there is significant change in the client information (change in structure, ownership, activities etc.)

New clients

CDD should normally be completed before entering into a business relationship or undertaking an occasional transaction. In certain rare cases the complete verification under CDD may not be performed before the commencement of a business relationship, and would be completed after the establishment of business relationship, provided that:

- it is completed as soon as reasonably practicable;
- the ML/TF risks are effectively managed; and
- this does not interrupt the normal conduct of the business.

The CDD policies should mention the circumstances under which the completion of CDD verification after the establishment of business relationship is permitted, however, these noted instances should be rare/limited.

When establishing a new business relationship, the information should also be obtained about the:

- the purpose of the relationship; and
- the intended nature of relationship - for example where funds will come from, the purpose of transactions

Existing clients

The CDD on existing clients should be carried out if there has been a material change in the nature or purpose of the business relationship with that client, such as when there is a suspicion of ML/TF, or where there are doubts about the available identity information, following a change in ownership/control or through participation of a PEP. A service should not be provided until the CDD requirements of existing client are met.

Occasional clients

“Occasional activity” and “occasional transaction” are not defined in the AML Act and AML Regulations. However, under FATF Recommendation, the term “occasional” does not necessarily mean “single”; it also includes circumstances in which multiple transactions are so intermittent or infrequent that no business relationship is established.

5.7 Why ongoing monitoring of the client relationship is important?

The practicing firm should keep up-to-date information of its clients so that:

- the risk assessment of a particular client in case of change in circumstances can be updated; and
- further due diligence measures can be carried out, if necessary.

Accordingly, the established client relationships should be subject to CDD procedures throughout their duration. This ongoing monitoring involves the scrutiny of client activities (including enquiries into sources of funds, if necessary) to make sure they are consistent with the business’ knowledge and understanding of the client and its operations, and the associated risks.

Event-driven reviews

The events triggering a CDD information update may include:

- a change in the client's identity;
- a change in beneficial ownership of the client;
- a change in the service provided to the client;
- information that is inconsistent with the business' knowledge of the client; or
- a suspicion of ML / TF.

An event driven review may also be triggered by:

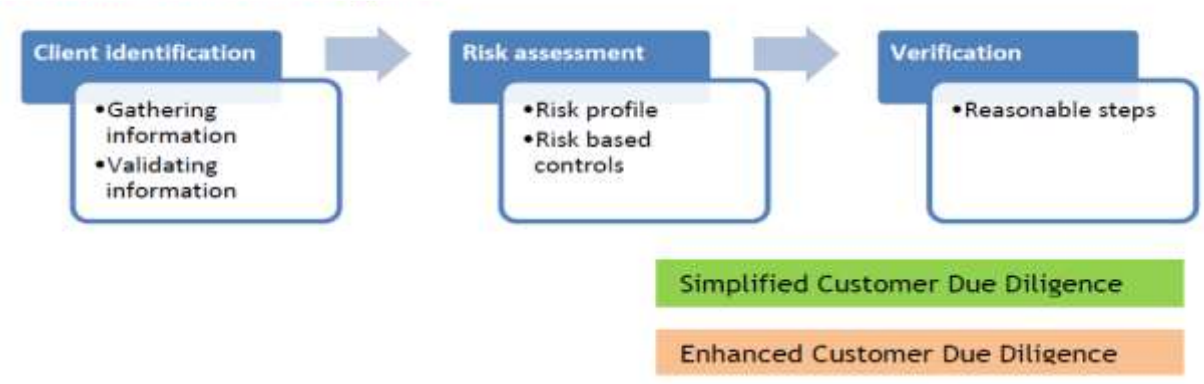
- the start of a new engagement;
- planning for recurring engagements;
- a previously stalled engagement restarting;
- a significant change to key office holders;
- the participation of a PEP
- a significant change in client's business activity (this would include new operations in new countries); an
- there is knowledge, suspicion or cause for concern (e.g. doubt on veracity of information provided). If a STR is made, care should be taken to avoid making any disclosures which could constitute tipping off.

Periodic reviews

The routine periodic reviews to update the CDD are also needed. The frequency of up-dating should be risk based, making use of the CMA practicing firm's risk assessment, and reflecting the business' knowledge of the client and any changes in its circumstances or the services it requires.

The CDD procedures necessary for either event-driven or periodic reviews may not be the same as when first establishing a new business relationship. Given how much existing information could already be held, ongoing CDD may require the collection of less new information than was necessary at the very outset.

5.8 How should CDD be applied?



The CDD should be designed to ensure that the CMA practicing firm understands who he is dealing with, understand client's activities and assess the risk of money laundering.

Client identification Process (CIP) – Gathering and identifying fundamental information and validating that information is the first step to CDD compliance and reducing risk. A CIP involves gathering information about the client, such as whether it's an individual or business, who controls, manages the client, what is normal and expected activity for that prospective client?

Risk assessment – Risk management procedures often differentiate based on a client's risk-profile. FATF suggests risk-based controls.

Based on the information gathered about a client, the CMA practicing firm using its risk assessment will determine the extent of verification required. This will help determining which kind of CDD to conduct before establishing the business relationship or conducting an occasional transaction or activity.

Application of a risk-based approach is of considerable importance in verification, both to ensure a good depth of knowledge in higher risk cases, but also to avoid superfluous effort in lower or normal risk cases.

Verification of information – CMA practicing firm should take reasonable steps to ensure that the information gathered is correct**.** In this regard the differentiated levels of CDD are:

- Simplified Due Diligence (SDD)
- Enhanced Due Diligence (EDD)

- **Simplified Due Diligence:** SDD is the lowest level of due diligence that can be completed on a client. This is appropriate where there is little opportunity or risk of practicing firm's specified services or client becoming involved in ML/TF.

- **Enhanced Due Diligence:** In situations that present a higher risk of money-laundering or terrorist financing CDD measures above and beyond normal measures i.e. EDD are performed.

5.9 When and how SDD should be performed?

The SDD should be carried out where the risks of ML/TF are lower. The low risk should be based on the adequate analysis of ML/ TF risk related to the client and adequate controls and checks exist in this regard.

The CMA practicing firm's internal procedures should set out clearly what constitutes reasonable grounds for a client to qualify for SDD and should take into account.

Sufficient information should be available about the client to satisfy that the client meets the criteria for SDD to be applied to it.

The SDD measures should be commensurate with the lower risk factors (e.g., a lower risk for identification and verification purpose at the client acceptance stage does not automatically mean that the same client is lower risk at the ongoing monitoring stage).

When assessing ML and TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

- Reliable information on the client is publicly available, such as public listed companies, Public administrations or enterprises.
- Familiarity with the client's AML/CFT controls due to previous dealings with the client.
- Clint is operating in countries which have been identified by credible sources as having a low level of corruption or other criminal activity.

Identity requirements

When simplified CDD is considered appropriate, the CMA practicing firm should document the full name of the entity and an explanation of how it falls in SDD category.

The information needs to be gathered about the identity of a person acting on behalf the client. This information would include, full name of the person, identification number, and the person's relationship to the client.

CMA practicing firm should obtain information about the nature and purpose of proposed business relationship with the client.

SBP and SECP Regulations on AML / CFT may also be referred to seek the types of documents from different categories of clients.

Verification requirements

The CMA practicing firm should verify the identity of a person acting on behalf of the client, and verification of that person's authority to act. Reasonable steps should be taken according to the level of risk involved. This verification should be undertaken before the business relationship is established or before the occasional transaction or activity is conducted.

In case of low assessed risk, the CDD measures are still needed but the extent and timing may be adjusted to reflect the assessment of low risk, for example in determining what constitutes reasonable verification measures.

Ongoing monitoring for unusual or suspicious transactions is also needed. Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

Simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing. Accordingly, in any case, when a client or potential client has been subjected to SDD, and a suspicion of ML/TF arises nonetheless, the SDD provisions should be set aside and the appropriate due diligence procedures applied instead (with due regard given to any risk of tipping off).

Example of SDD: Managing payroll for a small construction company

Client	Pioneer Construction (Private) Limited
Specified service	Managing client funds – making payroll payments to staff

Steps to complete simplified CDD	How this applies to the example
1. Obtain identity information for all relevant persons	Mr. Imtiaz (sole Director and shareholder of Pioneer Construction (Private) Limited) provides the CNIC details. The practicing firm checks the SECP records and notes that Mr. Imtiaz is listed as the sole director and shareholder of Pioneer Construction (Private) Limited, and the company address and incorporation number match those that have been provided by Mr. Imtiaz.
2. Obtain information about the nature and purpose of the proposed business relationship	Mr. Imtiaz explains that with the business growing, it is the right time to obtain professional accounting services for maintaining the payroll bank account and making payroll payments directly to staff.
3 Identify all relevant persons that need to be identified	Based on the information that Pioneer Construction (Private) Limited has provided and practicing firm's review of SECP records, it establishes that there are no other people with a beneficial interest in Pioneer Construction (Private) Limited.

4.	Make a determination of the level of ML/TF risk involved	The CMA practicing firm determines that the ML/TF risk is low, so it can continue with applying simplified CDD.
5.	According to that level of risk, verify the identity of relevant persons, including natural persons	The CMA practicing firm: - Obtains the certificate of incorporation / registration documents of Pioneer Construction (Private) Limited from Mr. Imtiaz. - Obtains a copy of the Pioneer Construction (Private) Limited records from SECP Registrar office and records the date of same. - Takes a clear copy of Mr. Imtiaz CNIC. - Records the date on which it sighted the CNIC and made the copy.
6.	If the identity information and verification requirements are satisfied, then practicing firm can proceed with the client's instructions	The CMA practicing firm on-boards Pioneer Construction (Private) Limited as a client and sets up systems to support the payroll disbursement operation directly to the staff.

5.10 When should EDD be carried out?

Where the risks of ML or TF are higher, practicing firm should conduct enhanced CDD measures, consistent with the risks identified. In particular, it should increase the degree and nature of monitoring of the business relationship, to determine whether those transactions or activities appear unusual or suspicious.

A risk-based approach to CDD will identify situations in which there is a higher risk of ML/TF. The 'enhanced' due diligence should be applied in the following situations:

- where there is a high risk of ML/TF;
- in any transaction or business relationship with a person/entity established in a high-risk country;
- if a business has determined that a client or potential client is a PEP, or a family member or known close associate of a PEP;
- in any case where a client has provided false or stolen identification documentation or information on establishing a business relationship;
- in any case where a transaction is complex and unusually large, there is an unusual pattern of transactions which have no apparent economic or legal purpose;
- in any other case which by its nature can present a higher risk of ML/TF.

Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- Obtaining additional client information (e.g. occupation, assets, information available through public databases, internet, etc.), and updating more regularly identification data of customer and beneficial owner.

- Obtaining additional information on the intended nature of the business relationship.

- Obtaining information on the source of funds or source of wealth of the customer.

- Obtaining information on the reasons for intended or performed transactions.

- Obtaining the approval of senior management to commence or continue the business relationship.

- Taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of 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

The extent of additional information sought, and of any monitoring carried out in respect of any particular client, will depend on the ML/TF risk that the customer is assessed to present to the designated person.

Example of CDD (high risk): Secretarial services for a tech start-up company

Client	Mr. Faraz who is launching a start-up company
Specified service	**Forming a company and providing a registered address** – The CMA practicing firm is requested to form a company for Mr. Faraz and provide a registered address for that company.

Steps to complete EDD	How this applies to the example
1. Identify which criteria the client customer meets to decide the level of CDD	Mr. Faraz proposed business would be part funded by an investor (his friend), who lives in a country that is a high-risk jurisdiction. The country risk is a red flag indicator so the CMA practicing firm decides to conduct enhanced CDD.
2. Obtain information about the nature and purpose of the proposed business relationship	Mr. Faraz explains that the purpose of his start-up business is to generate income from the smartphone applications. Users will make subscription payments via an online platform for using the applications. Mr. Faraz explains that he would like CMA practicing firm's advice on how best to set up this company and also require assistance to form it. He explains that he also requires practicing firm to offer a registered address for the company as he is a frequent traveler. Mr. Faraz explains that 50% of the seed funding is coming from his parents, with a further 50% from his friend who lives overseas.
3. Determine the initial level of ML/TF risk	The CMA practicing firm enquires Mr. Faraz about his friend. Mr. Faraz informs that his friend has various investments in new and developing technology businesses and has offered to top up the seed funding. Mr. Faraz's reference to using the online payment platform raises the perception of risk as these platforms can enable anonymous payments. The practicing firm decides that the level of ML/TF risk is such that enhanced CDD is necessary.
4. Identify all relevant persons that need to be identified	The CMA practicing firm asks Mr. Faraz to provide with the identity information about himself (including proof of his address), his parents and his investor friend and information about the sources of his seed funding.
5. Make a determination of the level of ML/TF risk involved	Mr. Faraz provides his original CNIC and the practicing firm views and takes a clear copy, and also notes date it sighted the CNIC and made the copy. Mr. Faraz also provides his bank statements that show his home address and lump sum payments from two sources: his parents and his friend (Friend's contribution originated by wire transfer from an overseas country. However, this does not fully enable identification of the actual source of the funds). Mr. Faraz parents live in Peshawar and he provides their CNICs and details of recent sale and purchase agreement that shows they have a profit from a property sale – some of which is being given to their son for the seed money. The practicing firm enquires whether the funds provided are a gift or a loan. Mr. Faraz inform it is a gift from parents, in lieu of future inheritance, and that appropriate paperwork has been filed via their lawyer. They have this paperwork with them. CMA practicing firm makes copies of all documents.

		The CMA practicing firm requests for further documents relating to the source of friend's funds and verifiable evidence of his identity. The practicing firm is provided with a copy of a five-year term deposit bank statement held at a bank in the overseas country, which has been certified by the banker and friend's lawyer. This shows that the term deposit concluded shortly before the date on which Mr. Faraz received funds in Pakistan. There are certified copies of accompanying bank records showing the instruction to send the balance by wire transfer to Mr. Faraz in Pakistan. The CMA practicing firm is also provided with a copy of the friend's Pakistan CNIC and passport which have been certified by a suitable professional in the overseas country.
6.	If the identity information and verification requirements are satisfied, then practicing firm can proceed with the client's instructions	The CMA practicing firm based on EDD steps concludes that this client and activity is not suspicious and does not require an STR to be filed. The practicing firm then set up the necessary arrangements to form the company for Mr. Faraz and keeps the record of the incorporated company

5.11 What does "High-risk countries" mean and what are its implications on the practicing firm?

The FATF identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT). The listing classifies countries into:

1. High-risk countries/jurisdictions
2. Other monitored jurisdictions

The high-risk countries and other monitored jurisdictions cover countries and territories that do not apply, or insufficiently apply, the FATF Recommendations. As of the FATF listing issued in July 2018, Democratic People's Republic of Korea and Iran have been designated as high-risk countries.

In accordance with FATF Recommendation 19, with regard to the high-risk countries, the CMA practicing firm should apply enhanced CDD measures to business relationships and transactions with natural and legal persons, resident or located in such jurisdictions. The enhanced CDD measures applied should be effective and proportionate to the risks.

The list of high risk and other monitored jurisdictions can be found at:
http://www.fatf-gafi.org/countries/#high-risk

5.12 Who is a Politically Exposed Person (PEP) and how CDD should be carried out?

Politically-exposed persons (PEPs) are individuals who, by virtue of their position in public life, may be vulnerable to corruption. The definition of PEP is not provided in the AML Act. However, the definition of PEP can be found in the FATF Recommendations. In accordance with the definition PEPs include foreign PEPs and domestic PEPs. The CMA Practicing firms should give specific consideration to the risks involved with PEPs and should:

- have procedures in place to determine whether a customer or a beneficial owner of a client, is a PEP or a close associate of a PEP
- obtain senior management approval for establishing or maintaining business relationships with PEPs
- take reasonable measures to establish the source of wealth and source of funds of PEPs conduct enhanced, ongoing monitoring of the business relationship.

Foreign PEP

FATF defines foreign PEP as follows:

"Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials."

The CMA practicing firms should have appropriate risk management systems in place to determine whether clients or beneficial owners are foreign PEPs, and if so, to take EDD measures to determine if and when they are doing business with them. The EDD measures, which are in addition to performing normal CDD measures should include:

- having appropriate risk-management systems to determine whether the client or the beneficial owner is a politically exposed person;
- obtaining senior management approval for establishing (or continuing, for existing clients) such business relationships;
- taking reasonable measures to establish the source of wealth and source of funds; and
- conduct enhanced ongoing monitoring of the business relationship

Domestic PEP and Persons who are or have been entrusted with a prominent function by an international organization

FATF defines domestic PEP as follows:

"Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials."

The CMA practicing firms should be taking reasonable measures to determine whether a client or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. As mentioned above FATF states that only directors, deputy directors and board members (or equivalent) of international organizations should be treated as PEPs. Middle-ranking and junior officials do not fall within the definition of a PEP.

The CMA practicing firm should determine risk of the business relationship with PEP. In cases of a higher risk business relationship with such persons, the practicing firm should apply the measures referred to in paragraphs (b), (c) and (d), above.

The factors that might point to potential higher risk, might include:

- known involvement in publicized scandals e.g., regarding expenses, misuse of authority;
- undeclared business interests;
- the acceptance of inducements to influence policy.

The enhanced CDD requirements for a PEP should also apply to family members and close associates of such a PEP.

The term 'international organization' is not defined in the FATF Recommendations. The CMA practicing firm should apply judgment to the type, reputation and constitution of a body before excluding its representatives from EDD. FATF refers persons who are or have been entrusted with a prominent function by an international

organization as members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

When considering whether to establish or continue a business relationship with a PEP, his/her family members and close associates, the focus shall be on the level of ML/TF risk, and whether CMA practicing firm has adequate controls in place to mitigate the risks so as to avoid the practicing firm from being abused for illicit purposes.

During the client relationship period, and to the extent that it is practical, efforts should be made to keep updated of developments that could transform an existing client into a PEP.

Existing clients may have become PEPs after they enter a business relationship, so it is essential that CMA practicing firm periodically monitors its existing client base for a change in the PEP status and update client information. Such ongoing monitoring shall be based on the level of risk.

5.13 What are the obligations of practicing firms under FATF Recommendation 6 and 7?

FATF Recommendation 6 requires each country to implement targeted financial sanctions to comply with the United Nations Security Council (UNSC / the Security Council) resolutions that require countries to freeze, without delay, the funds or other assets, and to ensure that no funds and other assets are made available to or for the benefit of:

(i) any person or entity designated by the Security Council under Chapter VII of the Charter of the United Nations, as required by Security Council resolution 1267 (1999) and its successor resolutions; or

(ii) any person or entity designated by that country pursuant to Security Council resolution 1373 (2001).

Further, FATF Recommendation 7 requires countries to implement targeted financial sanctions to comply with the Security Council resolutions that require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available to, and for the benefit of, any person or entity designated by the Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction

The Security Council sanction list can be accessed at:
https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list

Further, the above Recommendations are at the country (jurisdiction) level, requiring dissemination of sanctioned individuals / organizations to all stakeholders.

Accordingly, the Government of Pakistan under the United Nations (Security Council) Act 1948, gives effect to the decisions of the UNSC whenever the consolidated list maintained by the UN is updated. In this regard The Ministry of Foreign Affairs (MoFA) issues Statutory Regulatory Orders (S.R. Os) from time to time to provide legal cover for implementing sanction measures under the Security Council Resolutions. The S.R. Os issued by MoFA can be found at: http://www.mofa.gov.pk/contentsro.php

Further, the Government of Pakistan under section 11B of Anti-Terrorism Act, 1997 can declare an organization believed to be concerned with terrorism as a “Proscribed Organization” or put it under surveillance. In this regard, Ministry of Interior issues the formal notification of proscription of an organization. The listing of ‘prescribed organizations’ can be found at: https://nacta.gov.pk/proscribed-organizations/

Moreover, any individual about whom either there is a credible intelligence-information or who has a history of being linked to a Proscribed Organization can be proscribed by Home Department of a Province and can be subjected to restrictions on travel, speech and business, under the ATA, 1997. After issuance notification by the Home Department, name of such proscribed person is included in the 4th Schedule through Ministry of Interior,

Government of Pakistan under section 11EE of the Anti-Terrorism Act, 1997. Therefore, such proscribed persons are also referred to in local Police/ LEAs parlance as 4th Schedulers.

The CMA practicing firm is advised to check these lists while carrying out CDD and are accordingly obligated to ensure that no business relationship is established/maintained with the individuals/entities exposed and notified under the Recommendations 6 and 7. Further, STR reporting to FMU is required in case of suspicion of any individual / entity on the sanctioned list.

5.14 Can the CDD be carried out by Intermediaries?

The CDD measures/steps can be carried out by third parties on behalf of CMA practicing firm. Accordingly, the practicing firm is permitted to rely on certain other parties (subject to their agreement) to complete all or part of CDD.

The CMA practicing firm may rely upon an intermediary to perform any part of the CDD measures specified above, subject to confirming that the intermediary has adequate AML/ CFT controls in place and the other considerations set out in this section. However, the ultimate responsibility for ensuring that CDD level and requirements are met remains with the practicing firm.

Reliance on third parties may occur through, e.g., introductions made by another member of the same network or referrals from other practices or other professionals.

The CMA practicing firm should have written confirmation from the intermediary that:

- it agrees to perform the role; and
- it will provide without delay a copy of any document or record obtained in the course of carrying out the CDD measures on behalf of the practice, upon request.

Parties seeking reliance

The CMA practicing firm relying on a third party in this way is not obligated to apply standard CDD. However, it should still carry out a risk assessment and perform ongoing monitoring. That means it should still obtain a sufficient quantity and quality of CDD information to enable it to meet its monitoring obligations.

Further, the CMA practicing firm seeking to rely on a third party remains liable for any CDD failings irrespective of the terms of the CDD agreement. If relying on a third party, the CMA practicing firm should enter into a written arrangement and obtain copies of all relevant information to satisfy CDD requirements.

Parties granting reliance

The business (including the practicing firm) should consider whether it wishes to be relied upon to perform CDD for another party. Before granting consent, the business that is relied upon should ensure that its client (and any other third party whose information would be disclosed) is aware that the disclosure may be made to the other party and has no objection to the disclosure. It should make sure that:

- it has adequate systems for keeping proper CDD records;
- it can make available immediately on request:
- any information about the client/BO gathered during CDD; and/or
- copies of information/document provided during client/BO identity/verification or obtained during CDD.

It can keep those CDD records securely for legal/ statutory specified period after the end of business relationship.

5.15 Are there any specific CDD requirements for start-ups and SMEs?

The AML requirements are generic to all corporates and comparatively high level in order to provide flexibility to businesses to apply them to different types of customers / clients.

There are no specific or special requirements for, or mention of, start-ups or SMEs. However, as explained earlier the CMA practicing firms should not adopt a one-size-fit-all approach in the application of CDD requirements.

The CMA practicing firm should also ensure that design and implementation of its CDD requirements reflect both the operation and profile of these entities, the risk level as assessed and any other relevant considerations.

5.16 Which sources could be relied upon in CDD verification?

The purpose of verification of identity is to confirm and prove the information collected in so far as it relates to the identity of the client. Recourse to documents from independent sources is important. The amount of reliance that can be placed upon, and thus the strength of, particular forms of evidence varies.

Client verification means to verify on the basis of documents or information obtained from a reliable source which is independent of the person whose identity is being verified.

Documents issued or made available by an official body can be regarded as being independent. The following are illustrative of a different strength of various forms of documentary evidence:

- documents issued by a government department or agency or a Court (including documents filed with SECP, SBP or overseas equivalent).
- documents issued by other public sector bodies or local authorities.
- documents issued by professionals regulated for anti-money laundering purposes by the bodies listed in AML Regulations or overseas equivalents.

In the case of individuals, documents from highly rated sources that contain photo identification as well as written details are a particularly strong source of verification of identity.

Electronic identification

Globally, there are now a number of subscription services that give access to databases of information on identity. Many of these services can be accessed on-line and are often used by businesses to replace or supplement paper verification checks. This means that CMA practicing firm may use on-line verification as a substitute for paper verification checks for clients considered normal risk, supplemented by additional paper verification checks for higher risk clients, or vice versa.

Before using electronic databases, however, CMA practicing firm should question whether the information supplied is sufficiently reliable, comprehensive and accurate. The following points should be considered before deciding to use an electronic source (either as part of a wider process or, where appropriate, on its own):

- **Does the system draw on multiple sources?** A single source, e.g., Electoral Roll, is usually not sufficient. A system which uses both negative and positive data sources is generally more robust than one that does not.

- **Are the sources checked across a period of time?** Systems that do not regularly update their data are generally prone to more inaccuracies than those that do.

- **Are there control mechanisms to ensure the quality and reliability of data?** Systems should have built-in checks that ensure the integrity of data and should ideally be transparent enough to show the results of these checks and their bearing on the integrity of data.

- **Is the information accessible?** Systems need to allow a business either to download and store the results of searches in appropriate electronic form, or to print off a hardcopy record containing all necessary details as to name of provider, source, date etc.

5.17 What happens if CDD cannot be performed?

CDD measures should normally be undertaken before entering into a business relationship with a client. When delays occur, the business should still gather enough information to form a general understanding of the client's identity so that it remains possible to assess the risk of ML / TF.

The CDD will sometimes need to be completed while the business relationship is established, rather than before. But delays of this kind are only permissible when there is little risk of ML/TF and it is necessary to avoid interrupting the normal conduct of business. Such exceptions will be rare.

When most of the information needed has been collected before the business relationship has begun, it may be acceptable to have a short extension (to allow for information collection to be completed) provided the cause of the delay is administrative or logistical, not the client's reluctance to cooperate. To ensure the reasons are valid, and should not give rise to suspicions of ML/TF, it is recommended that each extension be considered individually and agreed with the senior management.

Extensions to the CDD schedule should be specific, well-defined and time-limited. There should be no granting of general extensions (such as for particular client types).

No client engagement (including transfers of client money or assets) should be completed until CDD has been completed in accordance with the business' own procedures.

Provided that CDD is completed as soon as practicable, verification procedures may be completed during the establishment of a business relationship if it is necessary not to interrupt the normal course of business and there is little risk of ML/TF. It is advised that such categories are considered carefully and defined by the Compliance officer to ensure that the reasons for any extension are appropriate.

Cessation of work and suspicious activity reporting

If a prospective client refuses to provide evidence of identity or other information properly requested as part of CDD, the business relationship or occasional transaction should not proceed any further and any existing relationship with the client should be terminated. Further, consideration should be given by the CMA practicing firm as to whether any reporting needs to be done to FMU.

6. Reporting of Suspicious Activity to FMU

6.1 What are the reporting obligations under the AML Act?

A purpose of the AML legislation is to help detect and report suspicious ML and TF activity. Businesses and professions regulated by the AML Act should report activity that may be linked to ML and TF.

FATF Recommendation 20 outlines that if a DNFBP suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the FIU.

Further, the FATF Recommendation 23 explains that an Accountant should report suspicious transactions when:

- On behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22; and

- Trust and company service providers, on behalf of or for a client, engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

Based on FATF Recommendation 20, the AML Act requires reporting of suspicious transactions.

Section 7 of the AML Act specifies that every reporting entity (including practicing firms for the purpose of this Guideline) should report the ML and TF related actual or suspected information to FMU. This reporting is termed as 'Suspicious transaction report'.

There is no materiality or de minimis exceptions to ML/TF reporting under STRs.

Additionally, section 7 of the AML Act also obligates the reporting entity (including practicing firms) to file 'Currency Transaction Report (CTR)' regarding the cash-based transactions above a set monetary limit.

6.2 What are the types of reports under the AML Act?

Under AML Act the two types of reports are:

1. Suspicious transaction report (STR)
2. Currency transaction report (CTR)

STR: In accordance with AML Act (under section 7) the STR is submitted to FMU whenever there is an actual incidence or suspicion of ML/TF (The AML Act defines STR as "the report on suspicious transaction specified under section 7")

CTR: The AML Act defines CTR as a report on cash/currency transactions exceeding such amount as may be specified by the National Executive Committee by notification in the official Gazette. Presently, all cash-based transactions above PKR 2.0 million or equivalent foreign currency require to be reported to FMU.
These standardized formats of these reports are provided in AML Regulation:

- Appendix I of AML Regulation contains the format of STR
- Appendix II of AML Regulation contains the format of CTR

6.3 What are responsibilities of a member of ICMA Pakistan and/or practicing firm in relation to AML reporting?

The CMA practicing firm and/or its employees may encounter or be made aware of ML or TF in the course of providing professional service to a client.

It is the responsibility of the CMA practicing firm to report the suspected transaction to FMU. Further, a CMA practicing firm is also mandated to submit CTR to FMU. To discharge its reporting obligations the CMA practicing firm should have internal reporting procedures that enable its employees to disclose their knowledge or suspicions of ML/TF.

CMA Practicing firm being the reporting entity under AML Act should consider the provisions in the AML Act and the underlying regulations and rules that provide for the reporting of suspicious transactions and implement appropriate internal policies, procedures and controls for meeting its obligations under the law.

With regard to the obligations of employees of CMA practicing firm, being reporting entity it should submit the STR to FMU. The employee of the practicing firm should report internally within the practicing firm in accordance with the AML program and related policies. The standardized format of STR (provided in AML Regulations) require signature by a person authorized by a reporting entity i.e. the CMA practicing firm to sign the STR. This implies that the STRs should be sent to the FMU through the authorized officer i.e. compliance or AML officer or any other authorized officer in this regard rather than directly from the person generating the STR. To do so the CMA practicing firm should establish a single reference point /compliance officer within the organization to which all employees are instructed to promptly refer all transactions suspected of being connected with ML or TF, for possible reporting to the FMU.

Individuals should exercise a healthy level of professional skepticism in accordance with their firm's AML procedures and engagement specific procedures. If in doubt, individuals should err on the side of caution and make a report to the compliance officer.

The CMA practicing firm's internal process to evaluate whether a matter should be referred to the FMU should be completed without delay, unless the circumstances are exceptional or extraordinary.

The CMA practicing firm should also take into account that they may not be able to identify the source of the funds, and therefore may not be able to ascertain whether the funds are proceeds of crime (including terrorist financing). In case of doubt, the CMA practicing firm may consider obtaining expert / legal advice.

Existence of higher than normal risk factors require increased attention to gathering and evaluation of client identification information, and heightened awareness of the risk of ML/TF in performing professional work, but does not itself require a report of suspicion to be made.

A sole proprietor, who knows or suspects, or where there are reasonable grounds to know or suspect, that a client or the person on whose behalf the client is acting, is or has been engaged in, or attempting, ML or TF, should submit STR to the FMU.

When preparing to file an STR the CMA practicing firm should consider whether it would commit a ML offence if it continued to act as it intends (usually as instructed by the client).

The provisions of reporting under the AML Act shall have effect notwithstanding any obligation as to secrecy or other restriction on disclosure of information imposed by any other law or written document.

As explained in earlier sections, the AML legislation read together with FATF Recommendations is not applicable to the practicing firm's audit and assurance services. Audit and Assurance services are not included in the specified services, therefore a CMA practicing firm carrying out these activities is not obligated with the AML Act requirements. However, such a practicing firm should have regard to their other obligations, such as reporting responsibilities under the ISAs as applicable in Pakistan or responsibilities under Code of Ethics (such as NOCLAR).

For clarification and determining the regulator that should be approached for any suspicious ML/TF activity of audit client, the member of ICMA Pakistan and/or practicing firm may contact FMU for clarification or else seek independent legal advice.

Under the AML legislation, there is no requirement to report and disclose information to FMU about the client's committed or intended fraud. This is owing to the fact that the client's attempt was to commit fraud, rather than to commit an offence under the AML legislation.

Further members of ICMA Pakistan engaged in business should consider their reporting obligations under their business activities or employment with a business. It is reminded that the only reporting entities are required to comply with the requirements of AML legislation, including STR and CTR submission to FMU.

6.4 What must be reported?

Section 7 of AML Act sets out the reporting obligations as under:

"Every reporting entity shall file with FMU, to the extent and in the manner prescribed by the FMU, Report of Suspicious Transaction conducted or attempted by, at or through such reporting entity, ***if it knows, suspects or has reason to suspect*** *that the transaction or a pattern of transactions of which the transaction is a part;*

a) *involves funds derived from illegal activities or is intended or conducted in order to hide or disguise proceeds of crime;*

b) *is designed to evade any requirements of this section;*

c) *has no apparent lawful purpose after examining the available facts, including the background and possible purpose of the transaction; or*

d) *involves financing of terrorism, including fund collected, provided, used or meant for, or otherwise linked or related to, terrorism, terrorist acts or organizations and individuals concerned with terrorism:*

Provided that Suspicious Transaction Report shall be filed by the reporting entity with the FMU immediately, but not later than seven working days after forming that suspicion.
.....".

STR

In accordance with above referred section 7, if a CMA firm knows, suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should report promptly its suspicions to the FMU.

The STR must be made by CMA practicing firm in following scenarios/ circumstances / events of ML or TF:

- known
- suspected; or
- reasonably suspected

Known ML or TF

Known or knowledge means actually knowing something to be true. The knowledge must have come to the practicing firm (or to its staff) in the course of business.

Suspected ML or TF

On the other hand, the suspicion or not is a subjective test. Being suspicious of a transaction does not require knowledge of the exact nature of the criminal offence or that the funds are definitely those arising from a crime.

Reasonably suspected ML or TF

Though the reasonable grounds are judgmental but should not be speculative. For 'reasonable grounds' to come into existence, there needs to be adequate information to proceed beyond speculation that it is merely possible someone is laundering money.

STR must be made where there is knowledge or suspicion of money laundering, but there is no requirement to make speculative STRs. The purchase of a new bungalow in UAE by a Pakistan based client's director is not, in itself, suspicious activity. However, inconsistencies in the affairs of company for which the director is responsible could raise speculation to the level of suspicion.

6.5 What are the timelines for STR and CTR reporting?

Under section 7 of the AML Act:

- The STR must be filed by the reporting entity with the FMU immediately, but not later than seven working days after forming that suspicion.

- The CTR must be filed by the reporting entities with the FMU immediately, but not later than seven working days, after the respective currency transaction.

6.6 What should be the approach when encountering or suspecting ML/TF?

The CMA practicing firm should have internal reporting procedures that enable its employees to disclose their knowledge or suspicions of ML/TF. As explained earlier, a designated compliance officer should be appointed to receive these disclosures.

Where an employee of CMA practicing firm (partner/other employee, who could be a member of ICMA Pakistan) and consequently the practicing firm becomes aware of an actual or suspected ML or TF, the steps that the employee or practicing firm take to comply with the reporting requirements under AML legislation should be taken on a timely basis, having regard to their respective understanding of nature of matter.

The following approach should be followed:

- Obtaining an understanding of the matter
- Internal reporting
- Reporting to FMU

Obtaining an understanding of the matter

There is no standardized approach or rules for recognizing ML/TF. In a CMA practicing firm, it is important for everyone to remain alert to the risks and to apply their professional judgment, experience and skepticism.

If a member of the Institute (or any other employee) employed in a practicing firm (the relevant employee), while establishing client engagement or providing the specified services for a client becomes aware of information (known, suspected or reasonably suspected) of ML/TF, such a relevant employee shall obtain an understanding of the matter, including the nature of the act and the circumstances in which it has occurred or may occur.

An illustrative list of indicators (Red flags) which may give rise to suspicious transaction is set out in AML Regulations. Further, FATF has also issued red flags related to ML and TF. (*These are included as Appendix B to this Guideline)*

The indicators should be assessed in the context in which the transaction occurs. Each indicator may contribute to a conclusion that there are reasonable grounds to suspect that the transaction is related to ML or TF. On the other hand, they may offer no indication of no ML or TF in view of factors such as the client's occupation, business, financial history and past investment pattern.

Depending on the nature and significance of the matter, the relevant employee of the practicing firm may consult on a confidential basis with the firm's senior management, compliance officer or with the legal counsel.

Internal reporting

The relevant employee of CMA practicing firm should report the matter to the designated compliance officer or any other person designated to receive information (or STR reporting authorized officer) of the practicing firm.

The CMA practicing firm's designated compliance officer or STR reporting authorized officer should be duty bound to consider all such internal reporting.

If the designated compliance officer or STR reporting authorized officer also suspects ML/TF then after consultation with the CMA firm's senior management an external STR should be filed with the FMU.

Deciding whether or not something is suspicious may require further enquiries to be made with the client or their records (all within the normal scope of the assignment or business relationship). However, prior to making further enquiries the risk of tipping-off should be considered. Accordingly, before disclosing any matter to the client or third parties it is fundamental to analyze and consider whether to do so is likely to constitute an offence of tipping off or prejudicing an investigation.

Further, if an employee of CMA practicing firm is in doubt, he/she shall always report concerns to the firm's internal designated person and/or senior management. It could be concluded as an offence for someone who knows or suspects that ML/TF has taken place (or has reasonable grounds) not to report their concerns to their authorized officer / compliance officer.

Reporting to FMU

As explained earlier, the CMA practicing firm is responsible to submit the STR to FMU. In the practicing firm it should be the responsibility of designated authorized officer/compliance officer to decide in consultation with the firm's senior management whether information reported internally needs to be reported to FMU as an STR.

In consideration of the significance of the above matters the compliance officer shall consult on a confidential basis with the practicing firm's senior management or legal counsel.

Section 7 of AML Act gives the timeline for furnishing information about suspicious transactions. The STR should be filed by the reporting entity with the FMU immediately, but not later than seven working days after forming that suspicion.

The CMA practicing firm should file with FMU the STR along with brief reason for the suspicion and the available supporting documents. Further, the practicing firm should keep and maintain all record related to STR and CTR filed by it for a period of at least five years after reporting of transaction.

In case where the internal STR reported by a relevant employee is not reported to FMU by CMA practicing firm the authorized officer / compliance officer, the relevant employee may consult senior management of the firm or seek advice from the legal counsel.

6.7 Whether a practicing firm is obligated to inform the client that an STR is submitted?

The practicing firm is required to ensure that a client is not informed of the STR submission to FMU. Disclosure of such information to a client is generally termed as tipping-off, and unlawful disclosure of such information is an offence under AML Act.

The FATF Recommendation 21 requires prohibition by law from disclosing ("tipping-off") the fact that a STR or related information is being filed with the FIU.

Accordingly, section 34 of the AML Act specifies that:

1) The directors, officers, employees and agents of any reporting entity, financial institution, non-financial business or profession or intermediary which report a suspicious transaction or CTR pursuant to this law or any other authority, are prohibited from disclosing, directly or indirectly, any person involved in the transaction that the transaction has been reported.

2) A violation of the sub-section (1) is a criminal offence and shall be punishable by a maximum term of three years imprisonment or a fine which may extend to five hundred thousand rupees or both.

Therefore, the practicing firm, its partners and persons employed with the practicing firm are prohibited to make a disclosure of submitted STR.

Further, section 34(3) provides that

3) Any confidential information furnished by a financial institution, non-financial business and profession, or any other person under or pursuant to the provisions of this Act, shall be kept confidential by the FMU, investigation agency or officer as the case may be.

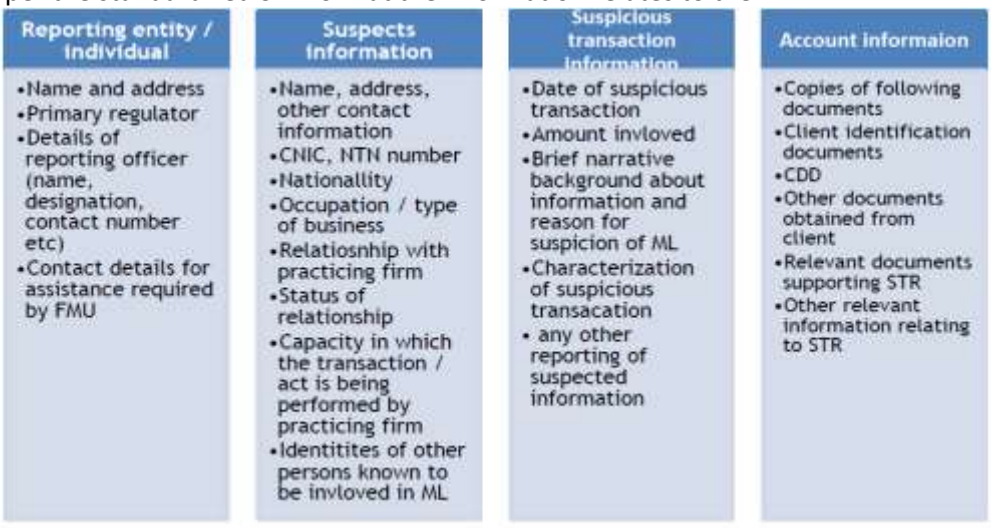
6.8 What are the contents of STR?

The reports to FMU under AML Act can be STR and CTR. These standardized formats of these reports are provided in AML Regulation:

- Appendix I of AML Regulation contains the format of STR
- Appendix II of AML Regulation contains the format of CTR

Contents of STR

As per the standardized STR format the information relates to the:



The STR should be signed and stamped by reporting entity, in this case CMA practicing firm's authorized person.

The STR should be free of jargon and written in plain English.

The reporters should also consider to:

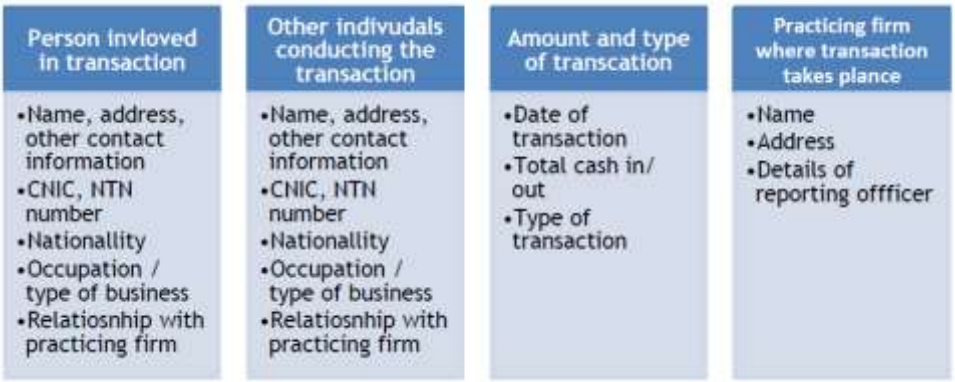
- Do not include information that is not required by AML law;
- Show the name of the business, individual or designated person/compliance officer submitting the report;
- Do not include the names of the relevant employees who made the internal report to the designated person;
- Include other parties only when the information is necessary for an understanding of the STR or to meet required disclosure standards; and
- Highlight clearly any particular concerns (whether physical, reputational or other). This information could be included in the 'reasons for suspicion/disclosure' field.

The STR form is available at: http://www.fmu.gov.pk/docs/Suspicious_Transaction_Report_Form.pdf

The guidance about filling the STR form can be found at:
http://www.fmu.gov.pk/docs/Guidance_notes_to_Reporting_Entities_(Non_Bank).pdf

6.9 What are the contents of CTR?

As per the standardized CTR format the information relates to the:



The CTR has to be signed and stamped by the CMA practicing firm's reporting officer.

The STR form is available at:
http://www.fmu.gov.pk/docs/Currency_Transaction_Report_Form.pdf

The guidance about filling the CTR form can be found at:
http://www.fmu.gov.pk/docs/CTR_Guidance_Notes.pdf

6.10 What should happen after an STR has been filed?

Where an STR involves a client as a suspect, practicing firms may wish to consider whether the behaviour observed is such that for professional reasons the business no longer wishes to act.

Generally, if following a report of suspicion, a practicing firm desires for its own commercial or ethical reasons to exit a relationship, there is nothing to prevent this provided the way the exit is communicated does not constitute tipping off. This also applies to the prejudicing an investigation offence.

If a decision is made to terminate a client relationship, a practicing firm should follow its normal procedures in this regard, whilst always bearing in mind the need to avoid tipping off.

6.11 What is the liability of not filing an STR?

The CMA practicing firm is liable to file the STR with FMU in accordance with the AML Act.

Section 33 of AML Act specifies the liability for failure to file STR and for providing false information, reproduced as under:

1) "Whoever willfully fails to comply with the suspicious transaction reporting requirement as provided in section 7 or give false information shall be liable for imprisonment for a term which may extend to three years or with fine which may extend to one hundred thousand rupees or both.

2) In the case of the conviction of a reporting entity, the concerned regulatory authority may also revoke its license or registration or take such other administrative action, as it may deem appropriate."

6.12 When should independent advice be sought?

There will be occasions where the CMA practicing firm needs to seek independent advice to ensure compliance with the AML Act. It is understood that FMU cannot provide legal advice to the reporting entities, including the practicing firm.

When a specific compliance questions about unique circumstances that the FMU cannot reasonably answer, the CMA practicing firm may need to seek independent legal advice or advice from an otherwise suitable professional. However, the consultation should be done carefully to ensure that there is no tipping-off of the suspected ML to the suspected client.

7. Record keeping

7.1 What are the record retention requirements?

The AML Act defines record as follows:

"Record includes the records maintained in the form of books or stored in a computer or any electronic device, or such other form as may be prescribed."

The AML Act section 7(7) related to the procedure and manner of furnishing information by reporting entity outlines that:

"Every reporting entity shall, in accordance with the regulations issued by relevant regulatory authority of that reporting entity, conduct customer due diligence and maintain record of transactions, account files and documents obtained through such diligence."

Further, section 7(4) requires the **record to be maintained for a period of five years after reporting of the transaction**. The relevant provision is reproduced hereunder:

"Every reporting entity shall keep and maintain all record related to Suspicious Transaction Reports and CTRs filed by it for a period of at least five years after reporting of transaction under sub-sections (1), (2) and (3)."

Similarly, the FATF recommendation 11 requires that the records relating to CDD, the business relationship and occasional transactions should be kept for five years after the business relationship is ended, or after the date of the occasional transaction.

7.2 What considerations apply to STRs?

In accordance with section 7 (4) of AML Act, the record relating to STRs must be retained for a period of at least five years after reporting of transaction. This record will generally include:

- internal reports;
- the practicing firm's consideration of internal reports;
- any subsequent reporting decisions;
- issues connected to consent, production of documents and similar matters;
- suspicious activity reports and consent requests sent to the FMU, or its responses.

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

7.3 Where should reporting records be located?

Records related to internal and external STRs and CTRs are not part of the working papers relating to client assignments. They should be stored separately and securely as a safeguard against tipping off and inadvertent disclosure to someone making routine use of client working papers.

7.4 What needs to done regarding third-party arrangements?

The practicing firm may arrange for another organization to perform some of its AML related activities – CDD or training, for example. In which case, it should also ensure that the other party's record keeping procedures are sufficient to demonstrate compliance with the ML/TF obligations, or else it should obtain and store copies of the records for itself. It should also consider how it would obtain its records from other party should they be needed, as well as what would happen to them if other party ceased trading.

8. Training and awareness

8.1 Why is training important?

Staff training is an important element of an effective system to prevent and detect ML/TF activities. The effective implementation of even a well-designed internal control system can be compromised if staff members using the system are not adequately trained.

8.2 Who should be trained?

A CMA practicing firm should identify, design, deliver and maintain an appropriate ongoing AML/CFT training program for its senior management, other partners and employees.

The practicing firms who may engage in 'specified services' should describe in their AML/CFT compliance program how they will conduct training on AML/CFT matters for senior management, the AML/CFT compliance officer, and any other staff engaged in AML/CFT related duties.

The CMA practicing firm should provide appropriate AML/CFT training to their staff and should have a clear and well-articulated policy for ensuring that relevant members of staff receive adequate AML/CFT training.

All partners and staff (especially those who interact with clients, handle funds or otherwise assist with compliance) should be made aware of AML/CTF laws and are trained regularly to recognize and deal with transactions/events/ circumstances, which may be related to ML/TF, as well as to identify and report anything that gives grounds for suspicion.

In case someone is accused of a failure-to-disclose offence a defense could be if:

- they did not know or suspect that someone was engaged in money laundering or terrorist financing even though they should have; but
- their employer had failed to provide them with the appropriate training.

This defense – that the employee did not receive the necessary AML training – may put the practicing firm at risk of prosecution for a regulatory breach.

8.3 What could be included in the training?

Training can be delivered in several different ways: face-to-face, self-study, e-learning, video presentations, or a combination of all of them.

The training should enable the CMA practicing firm's senior management, other partners and employees to seek and assess the information that is necessary for them to decide whether a transaction is suspicious.
The program itself should include:

- an explanation of the law within the context of the business's own commercial activities;
- so-called 'red flags' of which relevant employees should be aware when conducting business, which would cover all aspects of the ML/TF procedures, including CDD (for example those that might prompt doubts over the veracity of evidence provided) and STRs (for example what might prompt suspicion); and
- how to deal with transactions that might be related to ML/TF (including how to use internal reporting systems), the business's expectations of confidentiality, and how to avoid tipping off (see Section 6 of this Guideline);
- When to do customer due diligence (CDD), i.e., is the firm applying CDD to all clients on inception, or only when they instruct on a specified activity?
- How to identify and verify a client's identity (i.e., CDD)?

- What to say when a client does not want to produce identity documents?
- What the systems are to identify suspicious activity?
- What to do when an employee / organization encounters potentially suspicious activity?
- What records need to be kept?
- What are the firm's internal policies on AML/CFT?
- What penalties/ consequences might apply to the employees and the firm if they don't comply with the AML Act?

Training programs should be tailored to each service area and cover the procedures so that relevant employees understand the ML/TF risks posed by the specific services they provide and types of client they deal with, and so are able to appreciate, on a case-by-case basis, the approach they should be taking.

Furthermore, CMA practicing firms should aim to cultivate an AML culture in which employees are always alert to the risks of ML/TF and consistently adopt a risk-based approach to CDD. However, the overall objective of training is not for relevant employees to develop specialist knowledge of criminal law.

Records should be kept showing who has received training, the training received and when training took place. These records should be used so as to inform when additional training is needed – e.g. when the ML/TF risk of a specific business area changes, or when the role of a relevant employee changes.

A system of tests, or some other way of confirming the effectiveness of training, may also be considered.

The records of training should be maintained to show the training that was imparted, the dates on which it was given, which individuals received the training and the results from any assessments.

8.4 When should training be completed?

The CMA practicing firm may adopt timing and content of training for different groups of staff for their own needs, with due consideration given to the size and complexity of their business and the type and level of ML/TF risks. The frequency of training should be sufficient to ensure that members of staff maintain up-to-date AML/CFT knowledge and competence. Staff should be trained in what they need to do to carry out their particular role with respect to AML/CFT. This is especially important before new staff commence work.

CMA Practicing firms should also ensure that the new employees are trained promptly. Further, for new employees the confirmation of their understanding of AML / CFT requirements related to their particular role and affirmation of ensuring compliance with these requirements should be obtained.

In context of new staff hiring, background screening of employees plays an important role in the creation of an employee assessment system to help manage risk exposure. Accordingly, there shall be a policy in the CMA practicing firm to screen new staff hiring to determine the integrity and credibility of all employees.

8.5 What should be the frequency of the training?

The CMA practicing firm should, at regular and appropriate intervals, carry out reviews of the AML/CFT training needs of senior management and employees and ensure that the needs are met.

The frequency of training events can be influenced by changes in legislation, regulation, professional guidance, case law and judicial findings (both domestic and international), the business' risk profile, procedures, and service lines.

It may not be necessary to repeat a complete training program regularly, but it may be appropriate to provide senior management and employees with concise updates to help refresh and expand their knowledge and to remind them the importance and significance of effective AML/CFT system.

Appendix A - Common money laundering methods

Few common money-laundering methods include:

- **Nominees**

  This is one of the most common methods of laundering and hiding assets. A launderer uses family members, friends or associates who are trusted within the community, and who will not attract attention, to conduct transactions on their behalf. The use of nominees facilitates the concealment of the source and ownership of the funds involved.

- **Currency smuggling**

  Funds are moved across borders to disguise their source and ownership, and to avoid being exposed to the law and systems that record money entering into the financial system. Funds are smuggled in various ways (for example, by mail, courier and body-packing) often to countries with strict bank secrecy laws.

- **Structuring or "smurfing"**

  Many inconspicuous individuals deposit cash or buy bank drafts at various institutions, or one individual carries out transactions for amounts less than the amount that should be reported to the government, and the cash is subsequently transferred to a central account. These individuals, commonly referred to as "smurfs," normally do not attract attention as they deal in funds that are below reporting thresholds and they appear to be conducting ordinary transactions.

- **Asset purchases with bulk cash and use of shell companies**

  Individuals purchase big-ticket items such as cars, boats and real estate. Buying goods such as jewelry, boats, real estate, artwork, antiques, precious metals and stones is a common money laundering method, particularly for the placement (introducing illegal funds into the formal financial system) and integration (reinvesting funds) stages of money laundering. Many of these high-value goods are attractive to money launderers because they are easy to conceal and transport across borders and convert back into legitimate funds. In many cases, launderers use the assets but distance themselves by having the assets registered in the name of a friend, relative or employee or a trust / shell company. Further, the assets may also be resold to further launder the proceeds. Exchange transactions Individuals often use the proceeds of crime to buy foreign currency that can then be transferred to offshore bank accounts anywhere in the world.

Appendix B – Red Flags

The list below features some common money laundering indicators. This list should be treated as a non-exhaustive Guideline:

To help identify suspicious transactions, the CMA practicing firms should consider the following indicators:

- Client appears to be living beyond his or her means.
- Client has a history of changing bookkeepers or accountants yearly/frequently.
- Client is requiring assistance with unexplained urgency.
- Client is paying unusual consultant fees to offshore companies.
- Client has business activity inconsistent with industry averages or financial ratios.
- Client has bank deposits/cheques inconsistent with sales (i.e., unusual payments from unlikely sources).
- Client is uncertain about location of company records.
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.
- Funds transfer activity occurs to or from a financial institution located in a higher risk jurisdiction distant from the client's operations.
- Funds transfers contain limited content and lack related party information.
- Company carries non-existent or satisfied debt that is continually shown as current on financial statements.
- Company has no employees, which is unusual for the type of business.
- Company's currency transaction patterns show a sudden change inconsistent with normal activities.
- Company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues without reasonable explanation of the continued loss.
- Company shareholder loans are not consistent with business activity.
- Examination of source documents shows misstatements of business activity that cannot be readily traced through the company books.
- Company makes large payments to subsidiaries or similarly controlled companies that are not within the normal course of business.
- Company acquires large personal and consumer assets (i.e., boats, luxury automobiles, personal residences and cottages) when this type of transaction is inconsistent with the ordinary business practice of the client or the practice of that particular industry.
- Company is invoiced by organizations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.

- Formation of subsidiaries or branches in countries where these do not appear necessary to the business, and/or the manipulation of transfer prices with such subsidiaries or branches.

- Company conducting business mainly in cash, e.g. restaurants.

- Company financial statements are finalized with long delays.

Other Red flags

This appendix also provides more detail on the "red flags" to be on the lookout for when conducting specified services for clients. The red flags described below have been taken from a range of open source publications and professional judgments of subject matter experts.

They can be categorized in the following manner:

1. Country/Geographic risk
2. Client risk
3. Product, service or delivery method risk
4. Other risk factors

Country/Geographic risk

Moving money from country to country is a key typology for obscuring the criminal origins of funds and/or the true intended destination for funds. There are particular countries that represent higher ML/TF risks and these will change over time in the dynamic AML/CFT environment. When considering the risks associated with dealing with customers or transactions that relate to other countries or geographic regions, have regard to whether the countries are:

- identified by credible sources as not having effective systems to counter money laundering and terrorist financing

- Identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering, and the production and supply of illicit drugs

- subject to sanctions, embargos or similar measures issued by, for example, the United Nations or the European Union

- identified by credible sources to have provided funding or support for terrorism

- There are a wide variety of credible sources and it is up to the users' judgment what information to access and how to perceive the credibility of that information. Generally, sources with expertise in AML/CFT are deemed to be credible, such as the FATF, the Asia/Pacific Group (the FATF-style regional body), and other international organizations such as the United Nations, International Monetary Fund, and the Financial Intelligence Units of countries with strong AML/CFT systems in place.

Client risk

Reduced transparency
Factors that may indicate a higher than normal ML/TF risk include:

- Lack of face-to-face introduction of client.

- Subsequent lack of contact, when this would normally be expected.

- Beneficial ownership is unclear.
- Position of intermediaries is unclear.
- Inexplicable changes in ownership.
- Company activities are unclear.
- Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
- Management appear to be acting according to instructions of unknown or inappropriate person(s). Unnecessarily complex client structure.
- Reason for client choosing the firm is unclear, given the firm's size, location or specialization.
- Frequent or unexplained change of professional adviser(s) or members of management.
- The client is reluctant to provide all the relevant information or the accountant has reasonable doubt that the provided information is correct or sufficient

Transactions or Structures out of line with Business Profile

Factors that may indicate a higher than normal ML/TF risk include the following:

- Client instructions or funds outside of their personal or business sector profile.
- Individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear.
- Employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used).
- Sudden activity from a previously dormant client.
- Client starts or develops an enterprise with unexpected profile or early results.
- Indicators that client does not wish to obtain necessary governmental approvals/filings, etc.
- Clients offer to pay extraordinary fees for services which would not ordinarily warrant such a premium.
- 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.

Higher risk sectors and operational structures

Some client sectors and operational structures present a higher than normal ML/TF risk. Such risk factors may include:

- Entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.
- Politically exposed persons.

- Investment in real estate at a higher/lower price than expected.
- Large international payments with no business rationale.
- Unusual financial transactions with unknown source. Clients with multijurisdictional operations that do not have adequate centralized corporate oversight.
- Clients incorporated in countries that permit bearer shares.

Service risk

Particular products or services or transaction delivery methods can be vulnerable to misuse by those wishing to launder money or finance terrorism. When considering the risks associated with a product or service or transaction delivery method, have regard to whether:

- The product involves private banking.
- The product, service or transaction delivery channel might favour anonymity.
- The situation prevents face-to-face business relationships or transactions without certain safeguards, such as electronic signatures.
- Payments will be received from unknown or un-associated third parties.
- New products and new business practices are involved, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products.
- The service involves the provision of nominee directors, nominee shareholders, or shadow directors, or the formation of companies in third countries.
- The service is open to misuse of pooled client (or trust) accounts or provides safe custody of customer money or assets.
- The service requested is for introductions to other financial institutions, where this is not otherwise necessary or ordinary.
- The service requested is for advice on setting up legal arrangements that may be used to obscure ownership or real economic purpose (including setting up trusts, companies, or change of name/corporate seat or other complex group structures).

Other risk factors

These are some factors to consider that can either increase or decrease the perception of risk:

- Involvement of financial institutions or other DNFBPs.
- Unexplained urgency of assistance required.
- Sophistication of the customer, including the complexity of the control environment (ie, the overall attitude, awareness and actions of directors and management regarding the internal control system and its importance to the entity).
- Sophistication of transaction/scheme.

- Country location of accountant.
- Working environment/structure of the accountant (e.g., sole practitioner or large firm).
- Role or oversight of another regulator.
- The regularity or duration of a business relationship (long-standing relationships involving frequent customer contact throughout the relationship present less risk).
- The purpose of the business relationship and the need for an accountant to provide services.
- The reputation of customers in the local community.
- Whether private companies are transparent and well known in the public domain.
- The familiarity of the accountant with a country, including knowledge of local laws and regulations as well as the structure and extent of regulatory oversight.

Appendix C - Useful Web links to other publications / documents

Sr. #	Document	Weblink
1	**AML Act 2010**	http://www.fmu.gov.pk/docs/laws/Anti-Money%20Laundering%20Act%202010-As%20amended%20upto%20May%202016.pdf
2	**Anti-Terrorism Act 1997**	http://www.molaw.gov.pk/molaw/userfiles1/file/Anti-Terrorism%20Act.pdf
3	**AML Regulations 2015**	http://www.fmu.gov.pk/docs/AMLRegulations2015.pdf
4	**FATF Recommendations**	http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html
5	**FATF Guidance on the Risk-Based Approach for Accountants**	http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfguidanceontherisk-basedapproachforaccountants.html
6	**Typologies / Case Studies**	http://www.fmu.gov.pk/typologies.html
7	**Link of MOFA's website having designated individuals and entities under the UNSC Resolutions 1267**	http://www.mofa.gov.pk/contentsro.php
8	**List of 'prescribed organizations' issued by Ministry of Interior**	https://nacta.gov.pk/proscribed-organizations/
9	**CTR Form**	http://www.fmu.gov.pk/docs/Currency_Transaction_Report_Form.pdf
10	**CTR Form Filing Guidance Notes**	http://www.fmu.gov.pk/docs/CTR_Guidance_Notes.pdf
11	**STR Form**	http://www.fmu.gov.pk/docs/Suspicious_Transaction_Report_Form.pdf
12	**STR Form Filing Guidance Notes**	http://www.fmu.gov.pk/docs/Guidance_notes_to_Reporting_Entities_(Non_Bank).pdf
13	**Red Flag Indicators**	http://fmu.gov.pk/reporting-form.html

Appendix D - Glossary for Acronyms

AML Act	Anti-Money Laundering Act 2010
AML Regulations	Anti-Money Laundering Regulations 2015
AML legislation	Anti-Money Laundering Act 2010, The Anti-Money Laundering Regulations 2015 and FMU pronouncements
AML	Anti-Money Laundering
ANF	Anti-Narcotics Force
The Anti-Terrorism Act	Anti-Terrorism Act 1997
APG	Asia/Pacific Group on Money Laundering
BO	Beneficial Ownership
CDD	Customer Due Diligence
CFT	Counter Financing of Terrorism
CTR	Currency Transaction Report
DNFBP	Designated Non-Financial Business or Profession
EDD	Enhanced Due Diligence
FIA	Federal Investigation Agency
FATF	Financial Action Task Force
The FATF Recommendations	International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation issued by the Financial Action Task Force
FIU	Financial Intelligence Unit
FMU	Financial Monitoring Unit
ICMA Pakistan/ the Institute	Institute of Cost and Management Accountants of Pakistan
ISA	International Standard on Auditing
KYC	Know Your Customer
ML	Money Laundering
NAB	National Accountability Bureau
NACTA	National Counter Terrorism Authority
NPO	Non-Profit Organization
NFBP	Non-Financial Business or Profession
PEP	Politically Exposed Person
RBA	Risk-Based Approach
SBP	State Bank of Pakistan
SECP	Securities and Exchange Commission of Pakistan
SECP AML Regulations	Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations 2018
SDD	Simplified Due Diligence
STR	Suspicious Transaction Report
TF	Terrorist Financing
UN	United Nations
The Security Council	United Nations Security Council